EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY STOCKTAKING IN THE CAM

Stakeholder mapping and stocktaking of connected and automated mobility (CAM) cybersecurity

NOVEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS

We would like to acknowledge the following experts who have contributed to the study (in no particular order): Umar Zakir Abdul Hamid (Sensible 4 Oy), Mouhannad Alattar (Renault), David Arnold (Michelin), Roland Atoui (Red Alert Labs), Sadio Bâ (ANSSI), Markus Bartsch (TUVIT), Sandro Berndt-Tolzmann (Federal Highway Research Institute (Bundesanstalt für Straßenwesen - BASt)), Anastasia Bolovinou (ICCS), Slava Bronfman (Cybellum), Scott Cadzow (C3L), Jocelyn Delatre (ACEA), Markus Dreher (Robert Bosch Automotive Steering GmbH), Thierry Ernst (YoGoKo), Michael Feiri (ZF), Claire Fioretti (Michelin), Guido Gielen (FIA Region I), Sylvia Gotzen (FIGIEFA), Sami Harmoinen (EUROPOL), Dimitri Havel (McLaren Applied), Christophe Jouvray (VALEO), Josef Kaltwasser (Open Traffic Systems City Association e.V.), AJ Khan (APMA Institute of Automotive Cybersecurity), Horst Klene (Volkswagen AG), Lina Konstantinopoulou (EuroRAP), Mika Kulmala (City of Tampere), Jacques Kunegel (ACTIA Automotive), Eddie Lazebnik (Cybellum), Cédric Levy-Bencheton (Cetome), Sami Luoma (Finnish Transport and Communications Agency (Traficom)), Anthony Magnan (Verizon Wireless), Victor Marginean (Continental Automotive GmbH), Stefan Marksteiner (AVL List GmbH), Eduardo Meyer (Volkswagen AG), Idan Nadav (GuardKnox), Daniel O'Connell (Blackberry QNX), Lorenzo Perrozzi (Garrett Motion), Carlos Rosales (CTAG), Hari Sankar Ramakrishnan (FIGIEFA), Guillaume Stecowiat (UTAC CERAM), Jasja Tijink (Kapsch TrafficCom AG), Markus Tschersich (Continental AG), Virpi Tuulaniemi (Finnish Transport and Communications Agency (Traficom)), Eléonore van Haute (FIGIEFA), Timo van Roermund (NXP Semiconductors), Erik Vandervreken (CLEPA - European Association of Automotive Suppliers), Saša Vulinović (Volkswagen AG), Paul Wooderson (HORIBA MIRA).

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-407-7

DOI: 10.2824/24902

TABLE OF CONTENTS

1. INTRODUCTION

The Connected and Automated Mobility (CAM)[1] sector is an entire ecosystem of services, operations and infrastructures comprised of a variety of actors and stakeholders. The ecosystem brings about transformation in the industries as well as in the demands of citizens who look for safer, cleaner, more sustainable, and easier transportation. CAM has the potential to change the way society views transportation, benefit from digitalisation to connect vehicles with their surroundings and with the drivers, as well as contribute to solving congestion, reducing pollution, diminish road accidents, and improve access to mobility.

There are, therefore, two varying but complementing aspects in the ecosystem: connectivity and automation. A connected vehicle relies on the technologies installed in cars, buses, other vehicles and the infrastructure surrounding it, as well as people. A connected vehicle can also wirelessly (e.g. 4g/5g and/or WIFI) exchange data and information with the vehicle manufacturer and third-party service providers. The notion of V2X (i.e. vehicle-to-everything) therefore includes[2]:

- Vehicle-to-vehicle (V2V)
- Vehicle-to-infrastructure and vice-versa (V2I and I2V)
- Vehicle-to-mobile network (V2N) and infrastructure-to-mobile network (I2N)
- Vehicle-to-devices (V2D)
- Vehicle-to-persons (V2P)
- Vehicle-to-grid (V2G)

The automated aspect concerns the vehicles, where safety-critical control functions are carried out without driver input. Several years ago, Advanced Driver-Assistance Systems (ADAS) where only found in very few vehicles. Today, the mass market also includes, among others, (adaptive) cruise control, cameras, self-parking, blind spot detection and vehicle emergency braking. Drivers are quickly starting to rely on automation in various situations. There are five levels of automation[3] that range from driver assistance systems supporting the driver to the vehicle assuming all driving functions, therefore all persons becoming passengers in the vehicle without interaction with the car to drive it. Most manufacturers are currently aiming to reach Level 2 and 3: Partly Automated Driving and Highly Automated Driving (incl. Tesla[4], BMW[5], Mercedes-Benz[6]).

Cybersecurity is crucial in the evolution of the CAM ecosystem. The increasing connectivity and automation of vehicles and surrounding infrastructure brings about novel cybersecurity challenges, threats, and risks. The CAM ecosystem requires cybersecurity standards and cybersecurity measures by the stakeholders that provide for a safe infrastructure and services delivery. All stakeholders in CAM must ensure that data and technical structures have the necessary protection, safety and security measures for protection of the systems. Furthermore, cybersecurity is becoming more defined in this area through the adoption of both national and international standards and regulations in Europe and throughout the world.

[1] Connected and automated mobility in Europe. European Commission. Retrieved from: https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe
[2] The notion of V2X is further differentiated between safety-critical and non-safety-critical interactions, thereby also creating regulatory differences between the EU Member States.
[3] See more at: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic
[4] See more at: https://techcrunch.com/2019/04/22/teslas-computer-is-now-in-all-new-cars-and-a-next-gen-chip-is-already-halfway-done/
[5] See more at: https://www.bmw.com/en/automotive-life/autonomous-driving.html
[6] See more at : https://www.daimler.com/innovation/case/autonomous/drive-pilot-2.html

The number of stakeholders in bringing about this change is high and diverse and includes governments, policy makers, the automotive industry (manufacturers, suppliers, automotive aftermarket), the telecommunication industry (software, hardware, ICT infrastructure), associations, standardisation and regulatory bodies, who all bring strategic competences to cooperate and develop the CAM ecosystem and its cybersecurity. These stakeholders have to cooperate to achieve the various indexes of mobility and to arrive at the final goal of full degree of automation and connectivity, and thus automated driving in a cyber secure, trustworthy and safe manner. As part of the Cooperative Intelligent Transport Systems and Services (C-ITS)[7], the vehicle-to-everything (V2X)[8] notion relies on various communication technologies. This V2X communication can only be made possible through the cooperation of the whole industry, which is critical for the success of CAM. Action areas for CAM therefore lie in cybersecurity, innovation, infrastructure, legislation, interconnectivity, and data governance.

1.1 OBJECTIVES AND SCOPE

The aim of this report is to provide a comprehensive understanding of the CAM cybersecurity ecosystem and more particularly to map the key stakeholders and relevant bodies and organisations in the European Union, as well provide an overview of the critical services and systems and infrastructures. It also complements the Recommendations for the Security of Connected and Automated Mobility report of ENISA[9], which depicts the key cybersecurity challenges in the CAM sector according to stakeholders concerned. This report supports the CAM area by proposing conclusions on the findings in order to draft the necessary baseline cybersecurity measures and key issues to decision makers specific to the protection of security and resilience of the CAM ecosystem at the EU level.

1.2 TARGET AUDIENCE

The target audience of this report comprises:

- Associations
- Automotive Aftermarket Operators
- Mobility Service Providers
- National Authorities
- Operators of Intelligent Transport Systems (OITS)
- Original Equipment Manufacturers (OEMs)
- Policy Makers
- Regulatory Bodies
- Road Authorities (RA)
- Road Equipment Manufacturers
- Smart City Operators
- Standardisation Bodies
- System Integrators
- System Providers
- Tier 1 And Tier 2 Suppliers

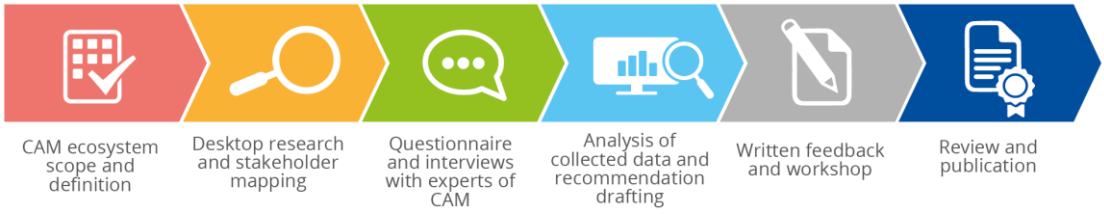
1.3 METHODOLOGY

Using a layered approach of desktop research and interviews, this report summarises insights across a complex CAM cybersecurity ecosystem. The desktop research methods included a survey and works of ENISA, official statistics, academic research, external studies and official documents, white papers, legislation, policies, strategies and initiatives to identify challenges and lessons learnt on cyber incidents against the CAM ecosystem. The interviews were

[7] Cooperative Intelligent Transport Systems (C-ITS) refers to transport systems, where the cooperation between two or more ITS sub-systems (personal, vehicle, roadside and central) enables and provides an ITS service that offers better quality and an enhanced service level, compared to the same ITS service provided by only one of the ITS sub-systems. See more at: https://www.car-2-car.org/about-c-its/ and at https://ec.europa.eu/transport/themes/its/c-its_en
[8] Passing of information from the vehicle to any entity that may affect it.
[9] Available on request.

conducted with key stakeholders from the CAM ecosystem. The information and data included in this report are therefore based on a six-step methodology as depicted in Figure 1 below.

Figure 1: Methodology



1.4 DOCUMENT STRUCTURE

In this document, the CAM ecosystem and insights involving stakeholder interactions, critical services and infrastructures, standards, as well as security measures are described. The insights gained from the survey, interviews, and desk research feed the conclusions of this report. Conclusions are put forward in order to improve the level of security and resilience of the CAM ecosystem in the European Union.

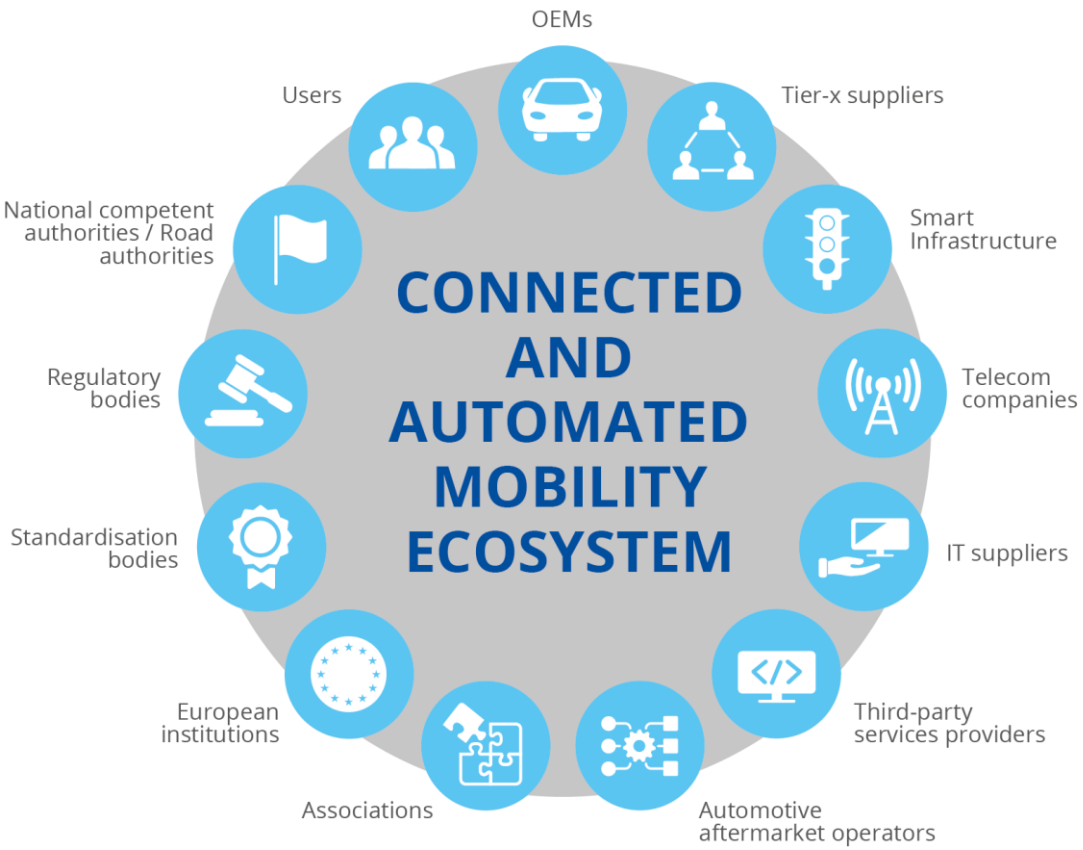
2. CAM CYBERSECURITY ECOSYSTEM

The connected and automated mobility industry relies on a wide ecosystem of actors covering the different areas of the value chain from R&D and manufacturing, retailing and service providing, operations, maintenance and management of infrastructures and fleets as well as all the standardisation and regulatory bodies framing the sector. Considering the distribution of activities and responsibilities over this ecosystem, interactions between actors are crucial for its development and effective operations, including actors who are in direct competition with each other from a business operational point of view. Relations between stakeholders are not only contractual in a logic of client and supplier but go further with various type of collaborations around technologies, practices and frameworks development and standardisation, and other business continuity related dependencies.

2.1 STAKEHOLDERS

The CAM cybersecurity ecosystem encompasses multiple stakeholders, as depicted in Figure 2 below. This section further describes these stakeholders and their role within the ecosystem.

Figure 2: CAM ecosystem stakeholders



Original Equipment Manufacturers (OEMs)

In the automotive sector, the Original Equipment Manufacturer (OEM) "is the original producer of a vehicle's components, and so OEM car parts are identical to the parts used in producing a vehicle."[10] In other words, in the automotive industry, the term OEM refers to any company that manufactures parts for use in vehicles, including hardware (e.g. brakes, electrical parts, exhaust systems, glass) as well as software systems (e.g. vehicle onboard computer) and who is in charge of the final assembly of the vehicle. For clarification, in many cases the hardware parts for the vehicle could also be produced by Tier 1 and 2 suppliers, as described in the next section.

With the emergence of CAM, OEMs have been at the forefront of innovation (along with tech companies) by giving special focus to research and development (R&D) toward vehicles connectivity and autonomous capabilities. OEMs have altered branding strategies and have set important goals to achieve autonomous driving but also to develop new offers around shared mobility and digital services. Nevertheless, the change in the automotive industry means that the value and supply chains to produce a vehicle for the market have also altered. OEMs must also face changes in the market value of their products brought about by CAM and new business models associated, as a result of increased collaborations with other relevant CAM stakeholders. Today, a typical vehicle is composed of mostly hardware and a smaller proportion of software. With the further development of CAM, though hardware will remain important, software and connected components will represent a higher share of a vehicle's market value, involving new partnerships and relations with actors mastering digital and software technologies in order to bring the right skills and knowledge for vehicles development.[11]

Tier 1 and Tier 2 suppliers

A Tier 1 supplier focuses on providing systems and parts (braking, systems, gearboxes, ECUs, exhaust systems, batteries, etc.) to OEMs which are their direct clients, and a Tier 2 supplier on sub-components of the systems and parts provided by the Tier 1 (screwing, gears, filters, tubes, electronical components, etc.) without a direct relationship to OEMs. In the same logic as Tier 1 suppliers are clients of Tier 2, the latter are supplied by Tier 3 and so on until Tier n, which produce other sub-components until the supplier that provide raw or close-to-raw materials (plastic and metal).

Tier 1 and Tier 2 suppliers thus encompass a large variety of components and materials, these include network services, engineering services, testing solutions, embedded applications, on-board units and systems, ITS systems, solutions, semiconductors, sensors, and a further array of software and hardware. These suppliers play a large role in CAM and are an important stakeholder of the hub depicted in Figure 2. Suppliers historically provided mechanical and electronic elements but also took the corner of CAM by providing parts related to connectivity (modem, infotainment systems, software, etc.) and autonomy (radar, lidar, algorithms, etc.) in order to answer to the evolution of OEM needs.

Smart Infrastructures Operators

In the CAM ecosystem, the stakeholders within the smart infrastructure category are multi-faceted. Smart Infrastructures comprise several operators from different domains of activity,

[10] What Is an Original Equipment Manufacturer (OEM) in the Automotive Sector? (2019). Investopedia. Retrieved from: https://www.investopedia.com/ask/answers/041515/what-original-equipment-manufacturer-oem-automotive-sector.asp

[11] For further reading, please refer, among others, to:

- https://www.volkswagenag.com/en/news/stories/2019/06/volkswagen-is-developing-more-of-its-own-software.html and
- https://www.porsche-consulting.com/fileadmin/docs/04_Medien/Publikationen/SRX04129_Revolutionizing_Automotive_Development_for_the_Digital_Future/Revolutionizing_Automotive_Development_for_the_Digital_Future_C_2019_Porsche_Consulting.pdf and
- https://cleantechnica.com/2019/01/06/teslas-software-first-approach-foreshadows-the-future-of-cars/ and
- https://electrek.co/2020/06/23/mercedes-cars-will-be-powered-by-nvidia-ai-for-self-driving-starting-2024/

such as energy, public transport, road management, public safety.[12] In the context of CAM, these operators of Intelligent Transport Systems (ITS), which are defined as "which without embodying intelligence as such aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and 'smarter' use of transport networks "[13] and Smart City operators which are "cities using technological solutions to improve the management and efficiency of the urban environment"[14].

Within the Smart Infrastructure, connected and automated vehicles interact with the whole ecosystem (V2X), which in part is made possible by the interaction with the smart road and urban infrastructure that are based on Internet of Things, Machine Learning, Big Data, and Mobility on Demand (V2I, I2V, V2N and I2N). The interaction of a vehicle with its surroundings and between infrastructures constituting the surrounding is crucial for the correct deployment of CAM. Road infrastructure should interact with vehicles through physical and digital elements. Today, road infrastructure is optimised for human intelligence and some roads and situations (especially in cities) are not developed enough for automated machine intelligence. Infrastructure today is not completely ready to accommodate V2I and I2V communication. The stakeholders are a blend of public authorities and private companies, that need to cooperate with the other stakeholders in the CAM ecosystem, namely OEMs, suppliers and 3rd party service providers, to best understand the needs of future infrastructure.

Telecom companies

Telecom companies are a stakeholder within the CAM ecosystem as they ensure the connectivity and data transfer stemming to and from vehicles and that of Smart Infrastructure (V2N and I2N). There are new opportunities for telecom companies in CAM which may, for instance, include the expansion of current (and installation) of fibre infrastructure or expanding the wireless bandwidth of vehicular and infrastructural data which also needs to conform to security expectations. Indeed, there are various layers to the CAM ecosystem in which a telecom company may decide to expand.

Another important evolution for the near future is the emergence of 5G V2X communication networks, which is much more sophisticated and offers higher bandwidth to enhance connectivity compared to today's 3G/4G networks. The European Commission's 5G Action Plan[15] from 2016, set out to ensure that by 2025, "all urban areas and major terrestrial transport paths have uninterrupted 5G coverage". The Action Plan also calls to diminish fragmentation among the Member states to ensure service continuity (i.e. aligned and coordinated 5G infrastructure), which is crucial for connected vehicles, especially in the EU, where cross-border mobility is an everyday phenomenon.

IT suppliers

IT suppliers provide secure software, hardware, as well as cloud functionalities. Alike to telecom companies, reliable connectivity (stability) is an absolute necessity for CAM. IT suppliers also cover the provision of emerging technologies such as Cloud computing platforms (Azure, AWS, etc.), Software platforms for automotive connectivity and mobility (e.g. Waymo, Yandex, etc.), AI (Artificial Intelligence) and IoT (Internet of Things) solutions to the CAM ecosystem.

Technology companies, especially tech giants, are also keen on joining the CAM ecosystem and bringing their services to the fore. These companies, mostly the latter, are able to invest

[12] Smart Infrastructure. ENISA. Retrieved from: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-infrastructure
[13] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040
[14] Smart cities. European Commission. Retrieved from: https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en
[15] 5G for Europe Action Plan. (last updated 2019). European Commission. Retrieved from: https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan

large sums in their development efforts, sometimes partnering with OEMs or other stakeholders depicted in Figure 2.

Third-party services provider

Third-party services providers supply, for example, content, maps, traffic data, music player, weather monitor, and mobile apps to vehicles. Satellite navigation providers are also included under this stakeholder grouping, as it is a key element of automated vehicles within the CAM ecosystem. In the European Commission's open public consultation on CAM[16], it was found that the majority of end-users would be willing to share data with third-party service providers on, for example, the state of roads, as well as data concerning the functioning of the vehicle components. Third-party service providers are significant in the CAM ecosystem to complement the services of, for example, OEMs.

Automotive aftermarket operators

Automotive aftermarket operators are aftermarket independent service providers who are independent parts producers, parts distributors, independent repairers, publishers of technical information, tool equipment manufacturers, roadside repairers, leasing companies, and insurance companies, as defined in Regulation (EU) 2018/858[17]. These automotive aftermarket operators, within the repair and maintenance activities, provide a range of traditional services such as independent parts manufacturing/distribution, repair and maintenance activities as well as a range of innovative services such as predictive maintenance, over-the-air repair and maintenance/software updates, remote diagnostics, and digital mobility services. For all these services, information exchange between all CAM stakeholders and aftermarket operators is necessary, and in particular with vehicle manufacturers for product development and system integration.

Associations

Associations, in general terms, are a group of people who work together in a single organisation for a particular purpose.[18] These purposes or goals differ depending on the type, size and scope of the association. Just as the automotive sector includes different types of companies and auto manufacturers, it does so associations as well. These associations can focus, among others, on trade, manufacturers, industry, independent trade in spare parts, repairers, repair information publishers, service providers for connected cars, and when expanding the scope to the CAM ecosystem, it also includes technology and software.

In this study, associations had a different input into the CAM ecosystem and represented the following aspects of CAM: parts manufacturing, IT security testing of C-ITS components, road assessment, automated driving software solutions, representation of wholesalers and retailers, and jointly promoting the interests of the members of the association to policy makers. Associations are thus a key component of the CAM ecosystem, as their competences and sometimes lobbying efforts bring about important change to the transportation world, at national, EU, and international levels.

European institutions

The European institutions acting in the CAM ecosystem are primarily the European Commission and Agencies. The European Commission aims to adopt various level policies and legislation in order to lead the transformation of the ecosystem. ENISA, a European agency is also highly active in cooperating with the CAM ecosystem in order to better understand how to advance

[16] Available at: https://ec.europa.eu/digital-single-market/en/news/summary-report-open-public-consultation-connected-and-automated-mobility-cam
[17] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R0858
[18] Association (definition). (n.d.) Cambridge Dictionary. Retrieved from: https://dictionary.cambridge.org/dictionary/english/association

cybersecurity at the European level. The European Parliament MEPs, in early 2019, also called for safety and liability rules for driverless cars, together with a robust legislation form the European Commission on access to in-vehicle data as this is a fundamental block for the achievement of both autonomous and connected driving in a Single European Transport Area and for competitive CAM services for end-users. A particularly important aspect in Europe is the collaboration among Member States, which the Commission coordinates in its Strategy on Cooperative Intelligent Transport Systems (C-ITS)[19]. The Commission also stated that part of its priorities is to "continue working on the regulatory environment, ecosystem-building, resource efficiency and standardisation to facilitate the market introduction of increasingly efficient cooperative, connected and automated vehicles." The European Commission's Joint Research Centre (JRC) has set up the EU-wide security Public Key Infrastructure (PKI) as a defining feature of C-ITS and critical safety V2X. As will be further described in section 2.1.1 Stakeholder interactions below, the stakeholders throughout the CAM ecosystem at times have mandatory interactions with the institutions in order to successfully carry out EU actions that will harmonise the industry.

For more information on the EU policy context, please refer to A Annex.

Standardisation bodies

Standardisation bodies, within the CAM ecosystem, are in charge of ensuring the long-term safety, security, and interoperability of the industry. Standards have different objectives, including providing standardised cybersecurity concepts, measures, solutions as well as management, furthermore, standards also encompass processes of quality necessary to homogenise conception and development practices through different frameworks. Standards offer a common ground for technological development, especially if driven as a legislative requirement. ETSI for example, a European Standards Organisation (ESO), is the recognised regional standards body for telecommunications, broadcasting and other electronic communications networks and services. ETSI's ITS (Intelligent Transport System) committee is paving the way for global standards for C-ITS, which are mainly vehicle-to-vehicle and vehicle-to-roadside communication.

For more information about the current state of play of standards in the CAM ecosystem, please refer to section 2.3.2 Standards.

Regulatory bodies

Regulatory bodies propose regulations and framework conditions to address the necessary changes brought about by CAM, including, for instance ethical and liability and privacy issues, cybersecurity, and safety. The United Nations Economic Commission for Europe (UNECE) adopted the cybersecurity regulation WP29 in June 2020, requiring all car manufacturers in the European Union (and beyond) to secure connected vehicles against cyberattacks under this new regulation set by the United Nations.[20] At the European level, the European Commission is in charge to transpose the texts defined by UNECE, which take into account the needs of all CAM stakeholders. Given that the pace of technological development is faster than the accompanying legislative process, regulatory bodies are in charge of creating a dynamic structure for governance to develop efficient technical legislation. At a national level each country may enforce some specific CAM regulation.

[19] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. 30 November 2016. Retrieved from: https://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

[20] UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles. UNECE. Retrieved from: https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html

National competent authorities/road authorities

At every national level, political support is necessary to push CAM forward. Across the EU Member States, governments have varying instances on development, testing, and deployment of CAM, in which national competent authorities/road authorities play a large role. These authorities may range from providing expertise for safety/security, to having an overview of a specific city's long-term goals, or even independent agencies that cooperate with both the public and private sectors on matters related to transport and communications.

Users

Users are defined as drivers and passengers as well as pedestrians. The bringing about of CAM shows how digitalisation affects more and more areas of society. There is a shift towards a user-centred mobility paradigm. CAM is surrounded by new technologies and one of the most important challenges to achieve by the ecosystem is to earn the trust and acceptability of the users. Today, connected mobility is thriving and making users' lives more comfortable through V2V and V2I communication, including, for instance, live information on traffic flow, construction sites, and accidents. Furthermore, vehicles are also connected to persons (V2P), by, for example, directly connecting their smartphones to their cars and accessing apps and making calls easily from their dashboards. For this aspect, the necessary trust lies in data protection schemes. For automated mobility itself, users' trust will have to go much further, in order to accept that automated cars will make the correct and necessary decisions. Though there are many facts to consider and research in order to ensure the correct deployment of CAM, it is highly beneficial for the future of society. The key opportunities are safety, comfort, efficiency, social inclusion, and accessibility.

2.1.1 Stakeholder interactions

This section describes the main stakeholder interactions towards a secure CAM ecosystem based on the primary data collected in this study. This study focuses on whether the interaction among stakeholders are mandatory (i.e. based on a legal requirement such as national or EU legislation[21], this does not include contractual obligations) or voluntary. The figures in this section show a summary of the nature of interaction between the stakeholders of the CAM ecosystem, based on the primary data collected for this report, i.e. survey, interviews, and direct feedback from the acknowledged stakeholders.

Original Equipment Manufacturers (OEMs)

Figure 3: Original Equipment Manufacturers' interactions with other CAM stakeholders

OEMs have an established network and/or partnership with the whole CAM ecosystem. From the survey and interviews, differing views were gathered on the nature (i.e. mandatory or voluntary) of the collaboration between OEMs and other stakeholders.

An OEM mainly collaborates with National Competent Authority/Road Authority, European institutions, Standardisation bodies, Tier 1 and Tier 2 suppliers, and Associations related to CAM, on a needs-basis. On the one hand, there is no mandatory collaboration necessary as the industry is proactive in cooperating as the needs call for it. On the other hand, whenever the interactions among stakeholders refer to compliance with legal requirements, such as data privacy, security and cybersecurity OEMs interactions with other stakeholders become mandatory, especially with stakeholders with whom OEMs do not have contractual relationships.

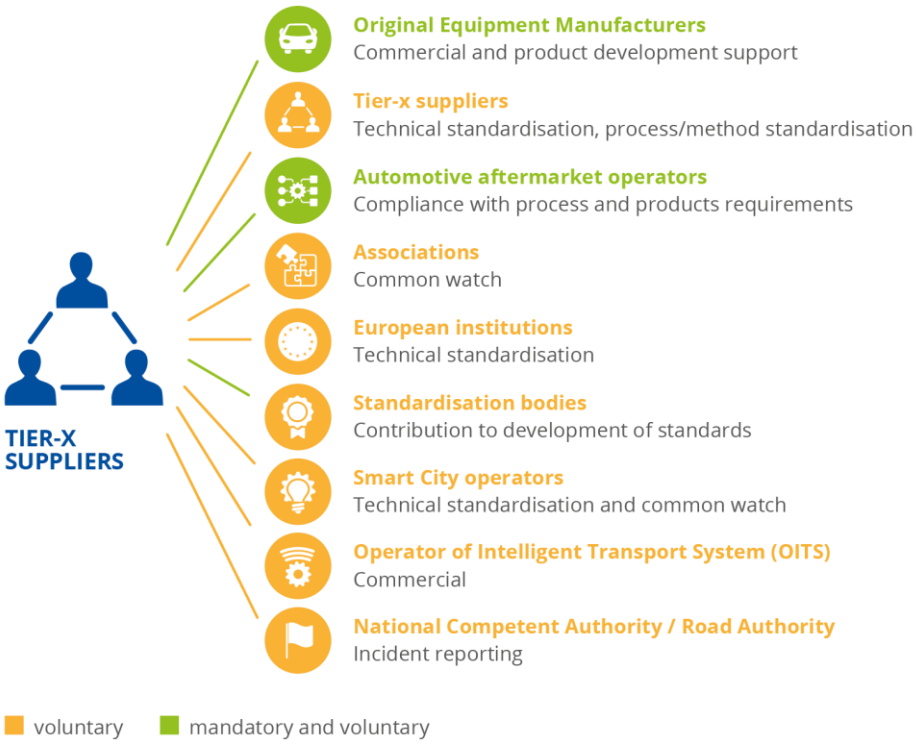
The purpose of collaboration stemming from OEMs and other stakeholders mostly hold the same values: technical standardisation, common watch (e.g. for innovation, threats), and process/method standardisation, as well as compatibility/interoperability needs. For a National Competent Authority/Road Authority, where collaboration is voluntary, technical standardisation and common watch are the main purposes of collaboration. The OEMs interviewed had differing views on the collaboration with European institutions where the nature is both voluntary and mandatory, with the purposes of technical standardisation, process/method standardisation, and common watch.

[21] This does not include the contractual obligations that may arise from bilateral contracts between stakeholders

Collaboration with standardisation bodies is voluntary from OEMs, one also noting that this cooperation is based on its voluntary contribution to the standards definition. The collaboration with Tier 1 and Tier 2 suppliers is deemed as mandatory, for the purposes of technical standardisation and process/method standardisation. In addition, collaboration with automotive aftermarket operators is necessary at both mandatory and voluntary levels for commercial and product processes, development and integration support including information sharing. OEMs interact with Automotive aftermarket operators in both mandatory and voluntary manners to ensure compliance with processes and products' requirements. Finally, with associations of the CAM ecosystem, the cooperation is voluntary for a common watch (e.g. for innovation, threats).

Tier 1 and Tier 2 suppliers

Figure 4: Tier-x suppliers' interactions with other CAM stakeholders



Tier 1 and Tier 2 stakeholders collaborate with the whole ecosystem, namely, National Competent Authority/Road Authority, European Institution, Standardisation body, Operator of Intelligent Transport System (OITS), Original Equipment Manufacturer (OEM), fellow Tier 1 and Tier 2 suppliers, Smart city operators (e.g. traffic operators), Associations related to CAM, and automotive aftermarket operators.

Tier 1 and Tier 2 collaboration with National Competent Authority/Road Authority is always voluntary, and are mostly based on incident reporting, but also include technical standardisation, process/method standardisation, and common watch. The collaboration with European Institutions is also voluntary, and mostly based on technical standardisation. Other purposes include incident reporting, common watch, process/method standardisation, as well as, for example, regulation making on access to vehicles data and exchanges on future roadmaps of the regulatory landscape. Tiers 1 and 2 suppliers voluntarily cooperate with standardisation bodies to contribute to the development standards (e.g. ISO/SAE/VDA) and may also participate to working groups. They sometimes hold monthly meetings to discuss general interest topics around cybersecurity.

The main purposes of collaboration were thus found to be technical standardisation, process/method standardisation, and also common watch. Only a minority of Tier 1 and Tier 2 suppliers collaborate with Operators of Intelligent Transport System (OITS), on a voluntary and commercial basis, with the purposes of technical standardisation and process/method standardisation. Tier 1 and Tier 2 suppliers interact with OEMs on both mandatory and voluntary bases, and it is mostly based on commercial and product development support purposes as OEMs are customers. Other reasons include technical standardisation and process/method standardisation, common watch, and incident reporting. Tier 1 and Tier 2 suppliers may also interact both mandatorily or voluntarily amongst each other, and their interaction is also often commercial, in order to receive components. They also need to align on technical standardisation and process/method standardisation. Smart city operators and Tier 1 and Tier 2 suppliers interact voluntarily to define technical standardisation and a common watch for innovation or threats. Collaboration with automotive aftermarket operators is necessary at both mandatory and voluntary levels for product development and integration support. Finally, with Associations related to CAM, the purpose of collaboration is also mostly based on common watch.

Automotive aftermarket operators

Figure 5: Automotive aftermarket operators' interactions with other CAM stakeholders

Automotive aftermarket operators need to interact with OEMs and Tier 1 and Tier 2 suppliers for information exchange regarding compatibility and interoperability for cybersecurity engineering. In more detail, automotive aftermarket operators interact with OEMs for both mandatory and voluntary reasons, more specifically for commercial and product process and development and integration support including information sharing.

With Tier 1 and Tier 2 suppliers, the mandatory and voluntary interaction is on the basis of product development and integration support. This ensures that the automotive aftermarket operators also have the capability to produce cybersecure products and services. Automotive aftermarket operators also mandatorily interact with European institutions for common watch, ensuring a faire level-playing field amongst relevant actors, and to keep legislations up to date. For common watch and technical know-how, interactions with Associations, National Competent Authorities/Road Authorities, and Standardisation bodies is necessary on a voluntary basis.

Associations related to CAM

Figure 6: Associations' interactions with other CAM stakeholders

Given Associations' varying nature, this stakeholder group interacts with the almost the entirety of the CAM ecosystem: National Competent Authority/Road Authority, European Institution, Standardisation body, Original Equipment Manufacturer (OEM), Tier 1 and Tier 2 suppliers, Smart city operators (e.g. traffic operators), Automotive aftermarket operators, and other Associations related to CAM.

The frequency of collaboration with other stakeholder groups ranges from a needs-basis, weekly or monthly basis. In fact, it depends on the core business of the association, and which aspects of the ecosystem are targeted. For example, an association may organise meetings with the industry to discuss solutions to the challenges at hand and define mutual interests. It may also launch a project that necessitates interaction on a daily basis for only a certain given period. For this latter reason, an association can, for instance, collaborate with National Competent Authority/Road Authority, European institutions, OEMs, Automotive aftermarket operators and Smart city operators. In general, associations listed the nature of their collaboration with the stakeholders mentioned above as voluntary, for the main purposes of technical standardisation and process/method standardisation.

European Institutions

Figure 7: European institutions' interactions with other CAM stakeholders

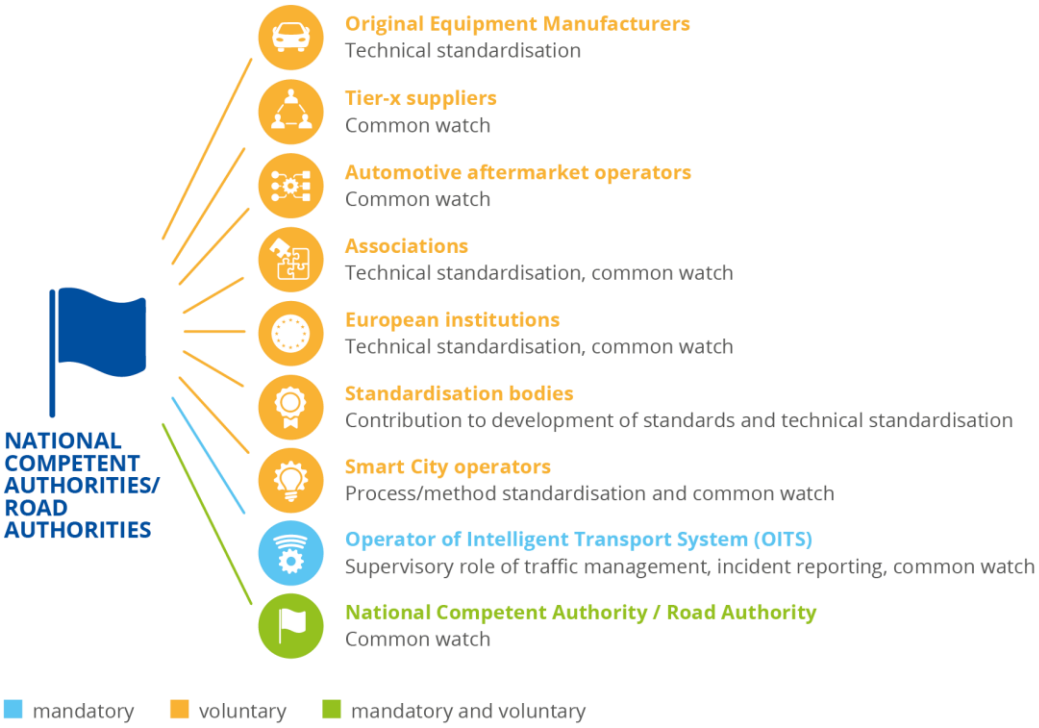
The responses received from a European-level body in the survey are not representative, for that reason, the stakeholder interaction for this section is only explored from the receiving end and the following complementary information from research.

The European Commission in particular, collaborates with the Member States and the industry to achieve the EU's ambitious vision for CAM within the Digital Single Market. The European Commission therefore publishes policy initiatives, develops standards for the European level, co-funds research and innovation projects, and adopts necessary legislation.[22] Furthermore, according to the NIS Directive[23] the European institutions, such as ENISA, are involved in receiving annual incident report from Road Authorities and ITSs.

For more information on the EU policy context, please refer to A Annex of this report.

National Competent Authority/Road Authority

Figure 8: National competent authorities'/Road authorities' interactions with other CAM stakeholders



The National Competent Authorities/Road Authorities that replied to the ENISA survey represent local and national level governments as well as cybersecurity. The information that we received from this stakeholder group shows that their interactions with the stakeholders of the CAM ecosystem differ, and so does the frequency.

The local level authority interacts with the central National Competent Authority/Road Authority on a voluntary basis for the purposes of technical standardisation, process/method standardisation, and common watch. They do not have further interactions in the CAM ecosystem. Following, the central National Competent Authority/Road Authority collaborates with the rest of the stakeholders in the CAM ecosystem. In fact, amongst each other, the

[22] Connected and automated mobility in Europe. European Commission. Retrieved from: https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe
[23] The Directive on security of network and information systems (NIS Directive). European Commission. Retrieved from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

collaboration is mandatory for common watch. States of the European union have cybersecurity agencies (such as ANSSI in France or BSI in Germany) who are in charge prevention, detection and reaction activities over information security topics for government, business and society.

These cybersecurity agencies, in turn works closely, but voluntarily, with the competent Ministry for process/method standardisation and common watch. Only the national authority interacts with the European institutions, on a voluntary basis for the purposes of process/method standardisation and common watch.

The interaction with Standardisation bodies happens on a voluntary basis stemming from both the national authority and the cybersecurity agency. Though, the interaction does not happen on a recurrent basis, the cybersecurity agencies are considered as experts and produce content for the development of new standards, as well as contributes to technical standardisation.

The national authority's intent for interaction is also technical standardisation, as well as process/method standardisation. The national authority has a mandatory interaction with the Operator of Intelligent Transport System (OITS) as it has a supervisory role of traffic management (including cybersecurity), and also provides incident reporting and a common watch. The cybersecurity agency and the national authority cooperate with OEMs and Tier 1 and Tier 2 suppliers as well as automotive aftermarket operators on a voluntary basis. The former for technical standardisation, while the latter stakeholders for common watch. Smart city operators (or traffic operators) are also a stakeholder group with which the cybersecurity agency and national authority interact voluntarily. The former for process/method standardisation and the latter for common watch. The national authority also cooperates with Associations related to CAM voluntarily for technical standardisation and common watch, as well as with communication network and cloud service providers.

Concerning Automotive aftermarket operators, the cooperation is based on common watch purposes. The national authority's competences are extensive, and it collaborates weekly with some stakeholder groups.

Operators of Intelligent Transport Systems (OITS)

Figure 9: Operators of Intelligent Transport Systems' interactions with other CAM stakeholders

Operators of Intelligent Transport System (OITS) interact with different stakeholders, depending on the parameters which are among others national legal requirements and supply chain requirements. It is possible for and OITS to have a mandatory interaction with European institutions for common watch. OITS can also focus on voluntary cooperation with

standardisation bodies for technical standardisation and process/method standardisation, and OITS can also interact with competent national IT security agencies on a voluntary basis. Furthermore, OITS may sometimes cooperate with OEMs and the entirety of the CAM ecosystem thanks to a country-wide platform and the willingness to contribute to producing an industry standard. For an OITS, the voluntary interaction is based on common watch and standardisation.

Standardisation body

Figure 10: Standardisation bodies' interactions with other CAM stakeholders

This standardization body interactions are all made on a voluntary basis, and as regards the frequency of their collaboration; standardisation issues are discussed at least once a month with the competent national agency and with European institutions. Therefore, the four stakeholders that this standardisation body cooperates with are National Competent Authority/Road Authority, European Institutions, Automotive aftermarket operators and other standardisation bodies on technical standardisation and process/method standardisation as well as common watch with the National Competent Authority/Road Authority.

Other

Various other stakeholders have also responded to the ENISA survey. These stakeholders cover other aspects of the CAM ecosystem, and provide services such as analyses to the European institutions, contribute to public consultations, act as a point of contact for law enforcement bodies, take part in European-funded projects, carry out conformity assessments, take part in the type approval certification process, or even offer trainings.

2.2 CRITICAL CAM SERVICES AND INFRASTRUCTURES

The mainspring of the Connected and Automated Mobility ecosystem is to provide a wide range of mobility services to users but also all services orbiting around mobility in order to propose a smoother, end-to-end, intermodal experience. While CAM services will enhance users' mobility, enabling to make it greener, safer, smarter, and more inclusive, the connectivity of all vehicles, infrastructures and devices of the ecosystem provides new capabilities to its stakeholders through B2B services and legislative driven-measures that enable better management and monitoring of the CAM assets. While CAM enables better practicality, comfort and safety for long haul journeys on road and highway networks, its development is essential in order to fully implement an operational Smart City model. As part of the transportation sector, CAM is subject to great safety and continuity stakes for which cybersecurity plays a major role since it is becoming a trigger targeted by malicious parties. In the CAM ecosystem, specifically in the field of critical safety, it is essential for all stakeholders to cooperate, and building upon the common standards, interoperability is imperative. Though interaction between stakeholders varies from

use-case to use-case, the obligation to cooperate will bring stronger involvement from EU Member States, who through the NIS Directive and their responsibility for road safety control play a bigger role than in other cybersecurity fields. The C-ITS Strategy focuses on services that bring benefits on road safety, sustainability and automation. Hence, cybersecurity must be considered as an essential part of CAM development.

In a landscape where some European cities have a very high population density and transportation flows are tensed, CAM represents one of the solutions to answer transportation problematics by transforming the mobility model. The CAM model is increasingly acknowledged by the ecosystem which is pushing R&D and investments in the sector. New actors are rising to provide disruptive services while existing forces in the ecosystem are transforming their business model to adapt to the rapid changes in the way users consume mobility. This model requires collaboration between CAM stakeholders from OEMs and public transport operators, to Mobility as a Service start-ups, automotive aftermarket operators and authorities managing public areas and infrastructures. All the capabilities provided by connectivity and autonomy are enabled by different technological stacks interacting between each other that are owned and managed by different stakeholders which illustrate why collaboration between stakeholders is much required to make the CAM technological frame consistent, as explained in section 2.1.1 Stakeholder interactions. In all technological areas, cybersecurity is a crucial topic to be addressed in order to ensure security for the infrastructures, the users and the ecosystem. In the CAM area, the collaboration of stakeholders around the different technological stacks requires to settle agreement about the cybersecurity model and governance enabling to share responsibilities regarding risks coverage and ensure that none of the relevant stakeholders become the weakest link for cybersecurity.

Implementing these technologies and connectivity to public network in mobility and the transport sector introduces cyber threats that must be managed. Hence, the connected and autonomous capabilities generate different types and levels of impacts for the stakeholders, users and ecosystem that need to be assessed and covered. This study enabled to evaluate what are the most important services and infrastructures following the stakeholders' point of view.

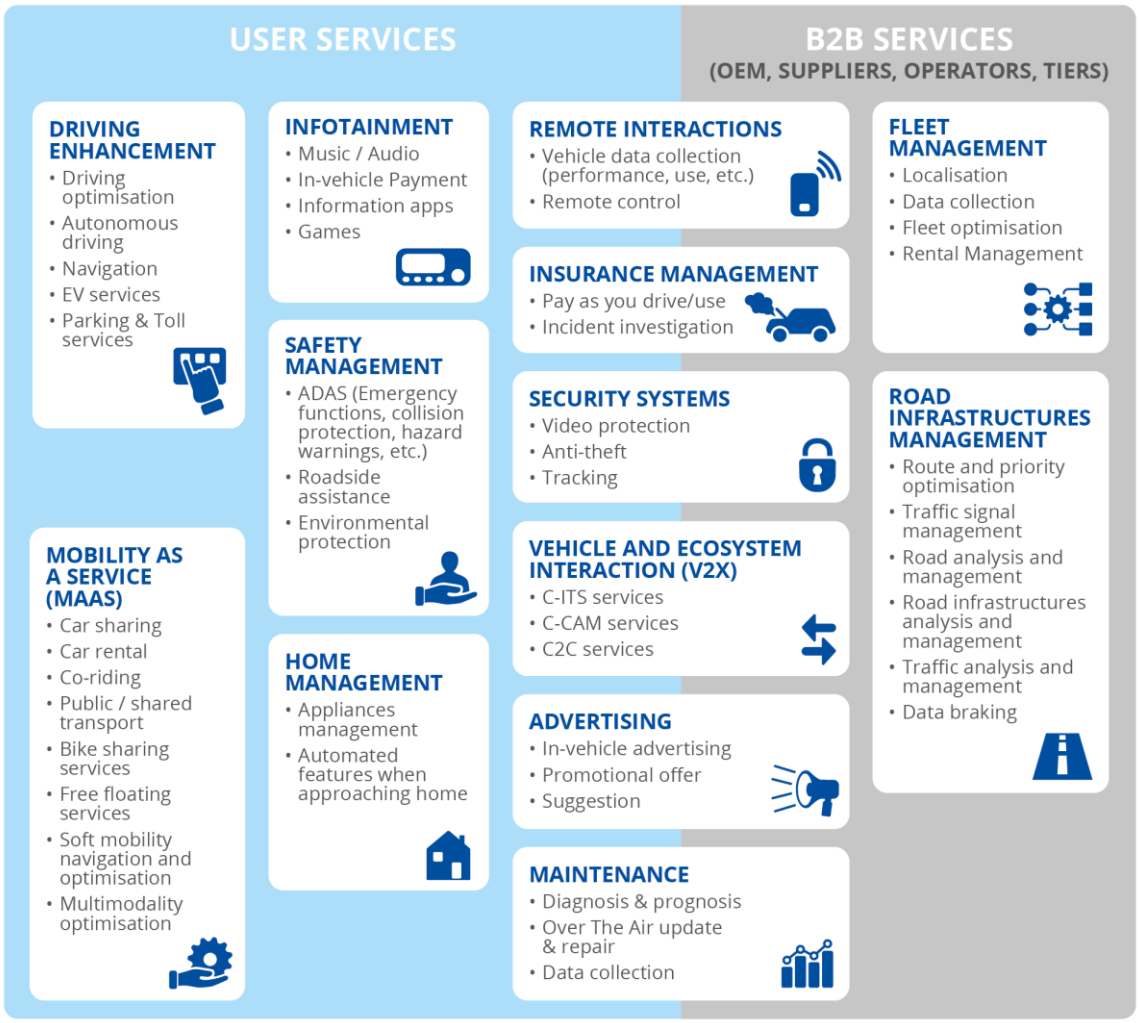
2.2.1 CAM services

The CAM services were established according to primary data gathered from the stakeholders through a survey, interviews, and direct feedback. The services are therefore represented according to the input collected. These CAM services have therefore been categorised following two criteria and are illustrated in Figure 11:

- User services (drivers, passengers, pedestrians) and
- B2B services (OEMs, suppliers, operators, tiers)

Some services can be relevant for both the users and CAM stakeholders.

Figure 11: CAM services mapping



Following the input received from the survey and interviews, the **most important services** that were pointed out are those enabling to access or interact with core mobility and driving functions of connected and autonomous vehicles, mobility devices and road infrastructures that can cause safety impacts for the users and the surrounding ecosystem:

User services

- Services related to the **driving enhancement** and core driving functions of vehicles and mobility devices: These features enable to automatise all functions and actions previously required to be performed by users in order to foster the autonomous ability of vehicles and mobility devices. These abilities aim to transform the role of the user from a driver perspective toward a passenger consuming mobility services model. In the same fashion as for safety functions provided by ADAS, driving enhancement services rely on a wide range of sensors and communications through different types of protocols and networks in order to exchange information between the assets of the CAM ecosystem. In addition, these services enable to automatise some functionalities such as EV charging for example which can be managed remotely from the user's smartphone or enabling the vehicle to automatically pay for the electricity refill by interacting with the charging infrastructures. The first concern raised by autonomous capabilities being safety, cybersecurity is seen as a major stake to ensure these services are implemented securely in order to enable their reliability and trustworthiness. As well, these services

are going to generate large amounts of personal data resulting from the use of these services which also raises consistent privacy concern.

- Services related to the **safety management** of the users and surrounding ecosystem: Those services known as Advanced driver-assistance systems (ADAS), provide new capabilities enabling to better prevent and avoid accidents as well as better assist in case of accident in order to increase the users' and the ecosystem's safety. These services enable actions from vehicles such as emergency braking or steering to avoid a collision. They also allow vehicles and mobility devices to contact rescue services and provide information about unusual events involving users' safety. Safety being the first concern of the transport sector, the connectivity and autonomous abilities are an opportunity for the ecosystem to assist users and better anticipate impromptu events thanks to V2X communications. However, since these functionalities carry safety properties, they are subject to regulations such as the General Safety Regulation and must cope with specific requirements. Also, the automation of safety features introduces risks since they represent a critical point of failure for CAM assets.

B2B services

- Services related to **road infrastructures management:** In the CAM ecosystem, vehicles and mobility devices are gaining new capabilities thanks to connectivity and automation, and they are interacting with the surroundings infrastructures that provide information and data enabling to broaden data sets available for computing and decision taking. Road infrastructures are also increasingly connected and automated, enabling generation of data about traffic flows and other information needed for management and maintenance operations. It enables operators to perform analyses about traffic in order to better adapt flows management, implement dynamic signalling with improved automation and anticipation as well as optimising all operations related to cleaning, maintenance or improvement. From a cybersecurity point of view, the ability to control remotely signalling systems from a potential connection over a public network represent an important threat. Hence there are important safety and operational impacts that would result from the take-over of road signalling systems.

Common services

- Services related to **vehicle and ecosystem interactions (V2X):** As mentioned for the previous safety and driving enhancement services, mobility is increasingly automated in order to transform personal vehicles in mobility devices that are shared and autonomous. The prerequisite for these capabilities is to ensure secure and efficient information and data exchange between CAM assets. Since CAM assets (vehicles, mobility devices, intelligent signalling systems, etc.) cannot only rely on sensors and cameras to produce and analyse data, it is essential that assets exchange data with their surroundings about their behaviour and environment in order to dispose of sufficient data to guarantee correct analysis and understanding of situations and events. From a cybersecurity point of view, integrity of such communication is critical. To ensure that the stakeholders align on technologies and framework, the ITS Directive[24] has been defined to provide a framework for communications between intelligent transport systems. This Directive aims to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and 'smarter' use of transport networks.

- Services enabling **remote interactions** with CAM assets (vehicles, bikes, e-bikes, e-scooters, etc.): Connectivity of CAM assets unlocked a range of services enabling users and operators to interact with vehicles and mobility devices remotely from various types

[24] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040

of portable devices and workstations. These services enable to collect many types of data generated by CAM assets about their location, performance, use history, parameters and so on, which include personal data related to the users' activity. In addition to the data collection, these services can allow to perform remote actions such as starting, unlocking, managing parameters and some functionalities like smart charging, remote diagnostic and repair. In this case, cybersecurity risks can trigger privacy and operational impacts for the users that remain high concerns in the transport sector.

- Services enabling **maintenance** of connected and automated vehicles and assets: In the transport sector, the maintenance of vehicles and infrastructures has always been a key point in order to maintain the right level of safety and operability. For the past 30 years, vehicles and infrastructures have increasingly integrated electronic components enabling enhancement of their functions. Through data collection, these features enable diagnostic and prognosis of CAM assets. Hence, with connectivity capabilities, it is now possible to collect data in order to anticipate and plan maintenance and repairs of either electronical or physical systems. In addition, it is also important to maintain a level-playing field for all relevant CAM operators and to ensure that there is no market foreclosure in the name of cybersecurity. Also, a big improvement brought by connectivity is the ability to update systems' firmware and software over the air in order to perform maintenance of systems remotely but also improving or adding functionalities to assets, making their lifecycle evolutive. The maintenance of CAM assets having a direct impact on operability and safety for users and their ecosystem, hence integrity of data used for diagnostic and prognostic must be strictly guaranteed. Considering over the air updates, cybersecurity is also a main driver when developing and operating such features. The upcoming UNECE Recommendation on Software Update Processes[25] aims to provide a secure and standardised manner for over the air updates to take place, ensuring that all stakeholders are certified. Since the functioning of assets will be driven by firmware and software of electronical components, it is crucial that their integrity is assured to avoid any malicious modification that could have severe impact.

Cybersecurity wise, the services stated above are very important because they directly involve users and the surrounding ecosystem safety. Misuse or abuse of these services and functions provide the attackers a direct access to core safety, driving, traffic management and signalling functions of the CAM ecosystem.

In the CAM ecosystem the assets are interdependent between each other and can be managed by fleet, which means potential take-over enables malicious actions at a large scale such as neutralisation or hijacking of a fleet, blockage of road traffic, etc. Indeed, these types of services are particularly targeted by attackers and some researchers have already proven the feasibility of these attack scenarios at a large scale in different experimentations. Indeed, the services below are **considered as important** by interviewed stakeholders:

User services

- **Mobility as a Service (MaaS):** Connected and autonomous capabilities are enabling to develop a new model of mobility which is end-to-end, multimodal and based on the sharing of vehicles and mobility devices. These services allow users to locate, access and rent different types of vehicles and mobility devices such as bikes and e-scooters that are made available in dedicated stations or in free-floating. There are several business models where vehicles and devices can be rented to a user or to a company, owned by multiple users and so on. Users access the services through terminals, applications and platforms where they may have a recurrent subscription or perform one-off purchases. These sharing and rental services are increasingly integrated within the

[25] See more at: https://undocs.org/ECE/TRANS/WP.29/2020/80

offers of public transport operators in order to cover the last kilometre and enhance the mobility experience. Hence, they are not used only as a substitution to personal vehicles or public transports but as a complementary mean. Those renting and sharing services are supplemented with a stack of services providing users the information enabling them to better optimise their journey and navigation with these mobility means. These services enabling users to travel around carry an operational impact for them since they rely on them for their journey which means principally safety and operational impacts, but there is also consequent privacy impact since the operators of these services will collect and store personal data about users and their trips. Financial impact is also to be considered since user payment information will be stored by service providers and also attackers may block devices or fleet in the aim to obtain a ransom.

- **Infotainment** services: For a long time, vehicles have been providing infotainment to their passengers such as music and radio. Thanks to connectivity and autonomy, these services have been evolving to represent one of the core values of a vehicle to its users, which represents its quality and technological advancement. Different strategies have been implemented by manufacturers for the development of their infotainment systems. These strategies tend to evolve from in-house development of their operating systems and applications to a model closer to the smartphone and PC industry where OS and apps are provided by partners and/or 3rd parties. Vehicle services are becoming more operational within the vehicle where CAM stakeholders like automotive aftermarket operators need to have access to the user through the vehicle HMI as well as in-depth access to vehicle data as close to the source as possible. Effective implementation of rights and roles is of paramount importance to manage these access needs. Vehicles now onboard various applications making it able to become the 5th screen of users and participate in the multi-device interoperability scheme proposed by digital services providers. In this case, the cybersecurity stakes are similar to those considered for applications in order to avoid privacy, financial and operational impact for the users. However, when considering the cybersecurity of vehicles, these services represent a consequent entry door for malicious parties willing to gain access with services or functions with a safety impact.

B2B services

- **Fleet management** services: The various business models emerging from Mobility as a Service but also historic actors such as car renters require for the operators to manage fleets of vehicles and mobility devices. Connectivity provides the opportunity to operators to manage remotely their assets in order to optimise and facilitate their operations. In the same way as a user would obtain data for one device, these services enable to monitor a whole fleet, obtain localisation, collect data about use (distance covered or duration of the rental), manage rental by unlocking, locking, monitor fuel or battery levels and so on. These services enable to digitalise operators' operations but also enable faster and easier access to vehicles and mobility devices for users by making them independent from a physical rental agency. From a cybersecurity point of view the main impacts will affect stakeholders' operations in case of misuse or attack on their fleet management services.

In the CAM ecosystem, most services provided to users and between stakeholders rely on various actors involved in physical devices and infrastructures operations but also digital assets and back-ends. The delivery of mobility services as well as services to manage stakeholders' operations or to enhance user experience impacts the transport industry reliability. These impacts are, for example, traffic and passenger flow fluidity, which also impacts users' privacy since a large amount of personal data can be collected, stored and processed. Moreover, since these services might be executed by the same OS or systems as services carrying safety impacts, they could be used as an entry door to perform an attack that could harm users or their

direct environment. Therefore, cybersecurity should be considered an important part of the ecosystem.

The CAM model, thanks to capabilities brought by connectivity of assets and IoT but also by the digitalisation of user interactions through applications, enabled stakeholders to develop and propose large sets of digital services gravitating around core mobility services. These **services have been stated as less important** by the interviewed stakeholders:

User services

- **Home management** services: Since vehicles are becoming increasingly connected and able to act as personal devices, CAM stakeholders are partnering with IoT and home automation actors in order to integrate use-cases where vehicles and mobility devices interact with home appliances in order to trigger automated action such as thermostat management, energetical optimisation, and doors and shutters operation.

Common services

- **Insurance management** services: The new usages associated to CAM are transforming the way users consume mobility services which means they also need to be contractually covered by insurances answering the challenges brought by these new use-cases. On one side, these new usages require an evolution of insurance offers to be adapted to a model where assets are increasingly shared and autonomous, and on the other side, connectivity capabilities enable to collect data about the use of asset that can be processed as inputs to manage insurance contracts. The ability to capture, store and analyse behavioural, mobility and data generated from the connected car, mobility device or road infrastructure will be a key factor to enable insurance management in CAM. This will serve as an enabler to build connected insurance products individually tailored, going forward (e.g. pay as you drive insurance, traffic incident analysis). In this model, insurance companies become a 3rd party consuming data produced by the CAM ecosystem with relatively high privacy and financial impact for the end user, meaning that confidentiality and integrity will be high stakes for the implementation of these services.

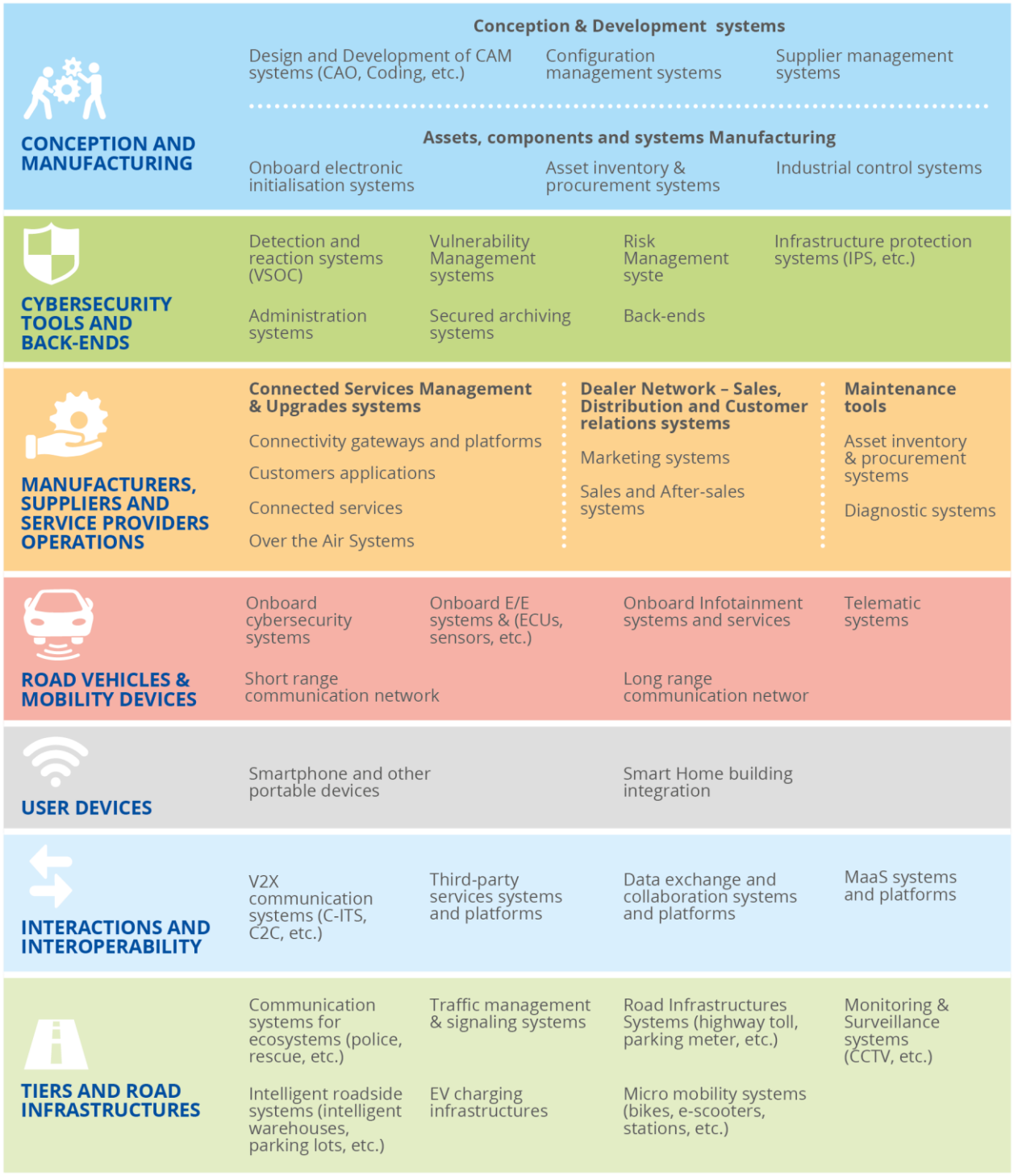
- **Advertising** services: Connected and autonomous vehicles and mobility devices increasingly integrate screen for infotainment but also interact with users through mobile applications. CAM stakeholders provide various services to users and these interfaces have started to be used as a display for advertising these services, make recommendations to users or highlight potential points of interest over the users' route.

- Services related to **security systems:** For vehicles and mobility devices for which theft is a common issue, connectivity enabled to integrate functionalities improving assets security against malicious acts and theft thanks to integrated video protection, localisation and tracking, and hardened anti-theft systems.

2.2.2 CAM systems and infrastructures

In order to implement the various services of the CAM model, many technical stacks, depending on different stakeholders, are implemented and interact among each other. These stacks support the systems and infrastructures enabling interactions between the CAM stakeholders and assets, but also storage and processing of data. These stacks go from Operational Technology (OT), Internet of Things (IoT) and onboard system, to devices and back-ends supporting digital assets but also infrastructures supporting specific communication networks and cybersecurity is an essential part which flows through the whole ecosystem.

Figure 12: CAM systems and infrastructures mapping



The fact that the delivery of CAM services relies on systems and infrastructures depending on different stakeholders defines the complexity of the CAM technical ecosystem. Technologies developed and used by a stakeholder might depend on the ones used on another stack but could also require harmonisation between a group of stakeholders in order to ensure interoperability. For example, regarding the communication between vehicles and other infrastructures (V2X), the technological framework for communication between assets has been formalised within the ITS Directive[26] in order to ensure that all the stakeholders standardise the technologies used to implement these communications. Availability of standards is critical to develop future-proof, scalable and sustainable solutions and to push forward innovation in the CAM area.

From a cybersecurity standpoint, the different systems and infrastructures do not carry the same criticality. In the CAM ecosystem, cybersecurity requires a holistic approach in order to cover risks, which means that each stakeholder at its level plays a role in the risk coverage. In some cases, the cybersecurity approach must be coordinated between stakeholders in order to define interfaces and perimeters of responsibility over systems and infrastructures protection. Depending on the stakeholder activity, the systems and infrastructure under its sphere of influence will differ, however, they might still have requirements regarding cybersecurity measures and risk management over systems and infrastructures with which they have interfaces. Additionally, interoperability is a leading factor for the functioning and development of the CAM ecosystem, meaning to ensure proper level of cybersecurity is required to ensure integrity and confidentiality of data flows between components and actors, as well as ensuring the compatibility and secure operation of different products and services managed by different CAM stakeholders.

A main point to address when securing CAM systems and infrastructures is the attack surface. In order to perform an attack, malicious parties will need an entry point that will be the first step to put in place the complete the attack path enabling to make the compromise successful. Then all systems and infrastructures that are exposed on public networks, provide an applicative interface or with a physical access to an interface or port will be considered as critical from a cybersecurity point of view. Then the systems and assets that carry functionalities or services that may generate a safety impact shall also be considered as critical since in the typical adversary model, they will be defined as one of the main targets malicious parties will aim to compromise, in addition to cyberattacks resulting in vehicle theft.

During the study, interviewees belonging to different stakeholder groups provided insights on which categories of systems and infrastructures they consider as critical regarding cybersecurity, and hence, consider that ensuring their protection is a priority for the ecosystem:

- Tiers and road infrastructures
    - Traffic management and signalling systems
    - Road infrastructures systems
    - Intelligent roadside systems
- Interactions and interoperability
    - V2X communication systems
    - Data exchange and collaboration systems and platforms
    - 3rd party services systems and platforms

All systems and infrastructures part of a CAM Cybersecurity Management System perimeter

- Road vehicles & mobility devices
    - Onboard cybersecurity systems

[26] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040

- Onboard E/E systems
- Onboard infotainment systems and services
- Telematic systems
- Short- and long-range communication networks

- Connected services management & Upgrade systems
  - Connectivity gateways and platforms
  - Connected services
  - Over the air systems

- Cybersecurity tools and back-ends
  - Back-ends environments
  - Cybersecurity tools
- Conception and manufacturing
  - Conception and development systems

- Maintenance tools

2.3 CYBERSECURITY CHALLENGES AND MEASURES

In the ENISA Report on Recommendations for the Security of Connected and Automated Mobility[27], seven cybersecurity challenges were identified in accordance with the stakeholder consultation and multiple recommendations can be found for all stakeholders of the CAM ecosystem. These challenges are:

1. **Governance and cybersecurity integration into corporate activities.**
   Cybersecurity governance is an organisational and technical challenge for all stakeholders. In the CAM ecosystem especially, digital technology and connectivity are tangled with physical transportation. New skills are necessary within organisations, with clearly defined roles and responsibilities. A cybersecurity team is needed to be relied upon, to manage risks and address potential vulnerabilities.

2. **Lack of top management support and cybersecurity prioritisation.**
   There are too few interactions between cybersecurity executives and corporate executives, leading to insufficient financial support (e.g. for research & development, awareness and training programmes, operational activities) to ensure that cybersecurity is a key topic in the lifecycle of CAM products and services.

3. **Technical complexity in the CAM ecosystem.**
   Given the large array of actors and their objectives in the CAM ecosystem, the implementation and management of cybersecurity and risk management prove to be a challenge. In addition, it is also a difficulty to find the correct liability measures for the final product, as components stem from many parties, and retracing the fault can be nearly impossible. In addition, due to the competitive nature of the automotive industry, obtaining cybersecurity information for product development and integration is difficult to achieve for certain SMEs CAM stakeholders.

4. **Technical constraints for implementation of security into CAM.**
   In the CAM ecosystem, there is a large array of technological diversity, and the securing of CAM products and services requires an assessment of a wide variety of systems and technical assets in order to implement the necessary cybersecurity measures to counter possible attacks. Cybersecurity needs to be addressed in the early conception phases of a product or service to ensure that there are no gaps or

[27] Upcoming, to receive a copy, please contact the authors.

vulnerabilities. Due to the highly interdependent nature of the automotive domain, this requires information sharing between different CAM stakeholders.

5. **Fragmented regulatory environment.**
   In order to manage cybersecurity risks, there are a large number of standards and regulations to comply with, especially given the mix of local and international environments. In Europe, regulations tend to be harmonised by the Member States, but there are also countries with specific and independent regulations. An organisation may therefore be subject to different schemes of one product range. The current regulatory framework does not include any test requirements or performance criteria for cybersecurity evaluation/assessment.

6. **Lack of expertise and skilled resources for CAM cybersecurity.**
   The lack of human resources with expertise in cybersecurity (e.g. software security, network security, cryptography, embedded systems, operational technology, etc.) on the market is a major obstacle that hinders the adoption of security measures specific to the CAM products and solutions. Furthermore, companies and organisations face a strong competition to recruit the desired profiles.

7. **Lack of information sharing and coordination on security issues among the CAM actors.**
   Considering data access and exchange within the ecosystem, trust between parties and data governance is a key challenge to address in order to implement a secure, competitive and lasting cybersecurity model

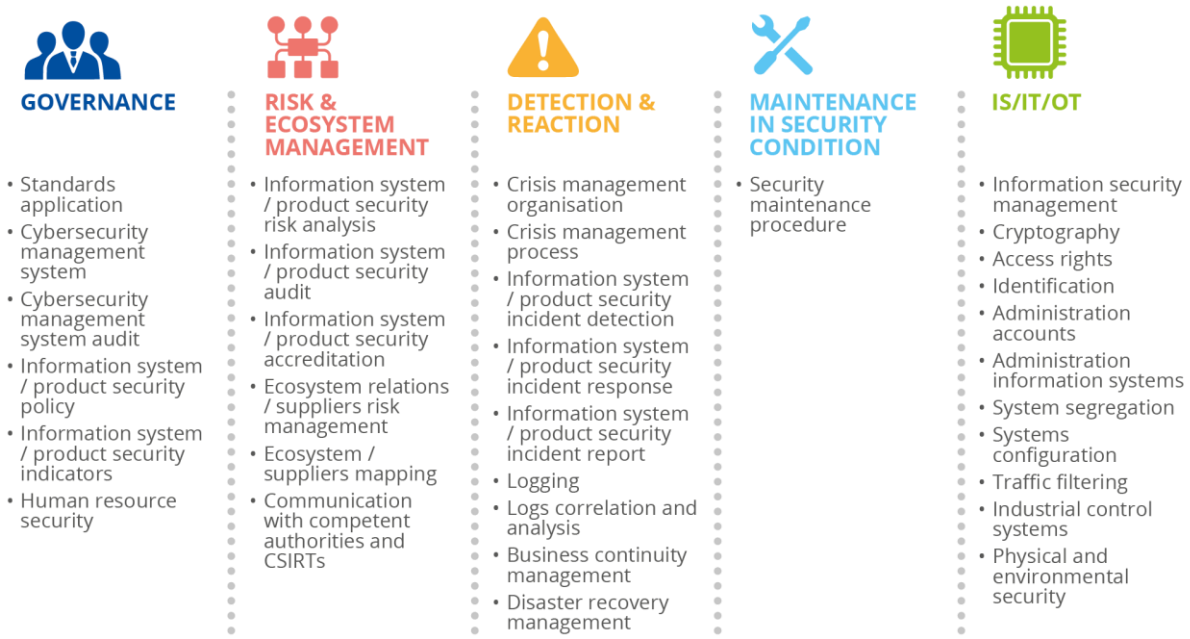
As discovered in the 2.1.1 Stakeholder interactions section of this document, the stakeholders in the CAM ecosystem are intertwined. For that reason, so are the cybersecurity challenges that they are facing, which are not standardised. The recommendations proposed by ENISA aim to guide the CAM ecosystem stakeholders and to contribute to the improvement and harmonisation of cybersecurity in the CAM ecosystem in the European Union.

2.3.1 Cybersecurity measures

The section presents CAM oriented security measures along with their level of implementation by the CAM stakeholders. The list of security measures (presented in Figure 13 and detailed in B Annex) was established through the analysis of relevant documents and standards identified during desk research. The analysis identified the most important cybersecurity aspects of the CAM ecosystem and the resulting 33 security measures issued from the NIS Cooperation Group[28], were classified into five categories[29]: Governance; Risk & Ecosystem Management; Detection & Reaction; Maintenance in Security Condition; IS/IT/OT security measures. The full overview is presented in Figure 13.

[28] The 33 cybersecurity measures are issued from the NIS Cooperation Group and are aligned with the NIS Directive. See more at: https://www.enisa.europa.eu/topics/nis-directive
The NIS Cooperation Group is the leading body for implementing the NIS directive. See more at: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
[29] See more at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

Figure 13: CAM security measures



Depending on the operations of the organisation, cybersecurity may or may not have to be directly implemented, especially when there are multiple actors and ways of working involved. For this reason, the security measures do not apply to all stakeholders, rather it depends on the services and systems that they use. The survey respondents were asked to assess the level of implementation of security measures between not implemented, partially implemented, implemented, or implemented and controlled, as well as don't know/no opinion. These answers were also chosen by the stakeholders depending on the risk assessments that need to be conducted, according to the perceived level of risk. Some organisations, such as the aftermarket, were still in the process of evaluation standards and legislation (drafting/implementation), for that reason, they may not have reached the required level of implementation. Furthermore, as a general comment, it was pointed out that globally acceptable testing processes that are objective and traceable are missing in the CAM ecosystem.

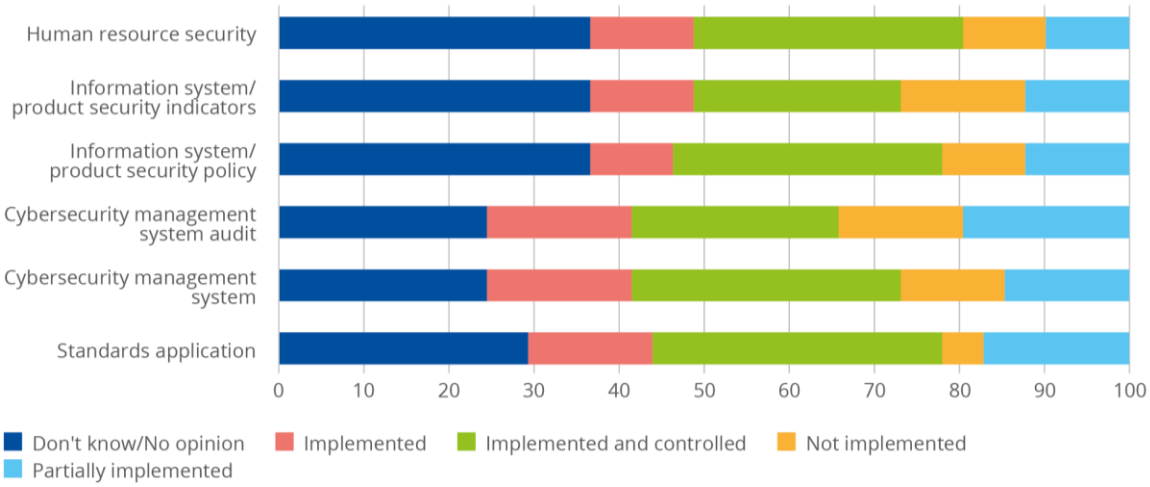
The below sub-categories present the five domains of CAM security measures. In this chapter, a number of selected security measures are discovered in-depth. The data used in the analysis below is indicative and is therefore meant to give only an insight on the answers of the respondents of the survey.

The described measures are discussed because the answers received from the participants showed relatively lower score compared to other security measures and need further development.

Governance

The following graph represents the answers given by all stakeholders in the survey.

Figure 14: Survey answer about the Governance Analysis



Under the governance umbrella, two cybersecurity measures will be further discussed, due to their low overall implementation:

- Cybersecurity management system audit
- Information system/product security indicators.

An operator regularly audits the cybersecurity management system it has implemented. As part of their cybersecurity management systems, stakeholders should implement organisations and processes to identify, among others, the threats vulnerabilities, and risks they are facing. Any shortcomings may pose risks, and these may materialise and impact the areas in which the organisation is active, for example, governance, data security, physical security, third-party management. Though, this assessment is difficult to organise as it requires to cover many business process, information systems and technologies, and requires an involvement of all businesses and associated top management. This organisation should be audited regularly in order to ensure its processes are relevant and efficient for risk management. The stakeholders responding to the survey had mixed views given the difficulty to organise auditing, including privacy issues that need to be considered, among others. OEMs' level of implementation of cybersecurity management system audit is implemented and sometimes also controlled. Tier 1 and Tier 2 suppliers, OITS, National Competent Authorities/Road Authorities, standardisation bodies as well as associations have different practices among themselves, ranging throughout the four levels of implementation.

As for information system/product security indicators, these are a challenge for all CAM stakeholders within the ecosystem. ENISA, in 2018, published a report on Good practices for identifying and assessing cybersecurity interdependencies particularly between Operators of Essential Services (OES), Digital Service Providers (DSPs) and National Competent Authorities (NCA).[30] It provides a description of interdependencies, highlights risk assessment practices, proposes a framework as well as defines good practices for assessing interdependencies. The CAM ecosystem stakeholders mostly responded (not taking into account don't know answers) that information system/product security indicators are implemented and controlled, which is especially true for Tier 1 and Tier 2 suppliers in the CAM area, as well as OEMs. OITS and

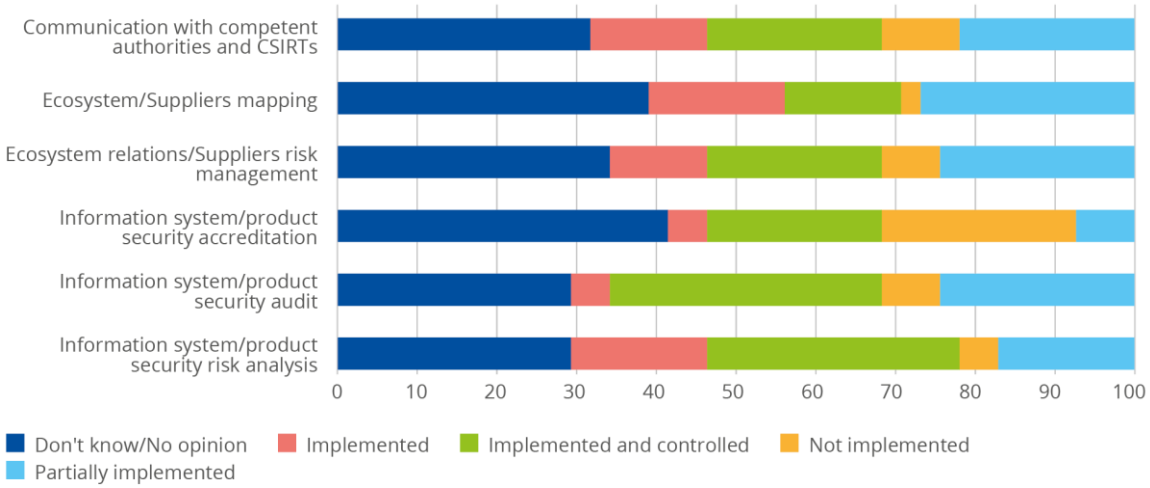
[30] Good practices on interdependencies between OES and DSPs. (2018). ENISA. Retrieved from: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps

National Competent Authorities/Road Authorities are on the other end of the spectrum, with most answers of partially or not at all implemented for this specific security measure.

Ecosystem Management

The following graph represents the answers given by all stakeholders in the survey.

Figure 15: Survey answer about the Ecosystem



The four following security measures related to the management of the CAM ecosystem will be further discussed:

- Information system/product security accreditation;
- Communication with competent authorities and CSIRTs.

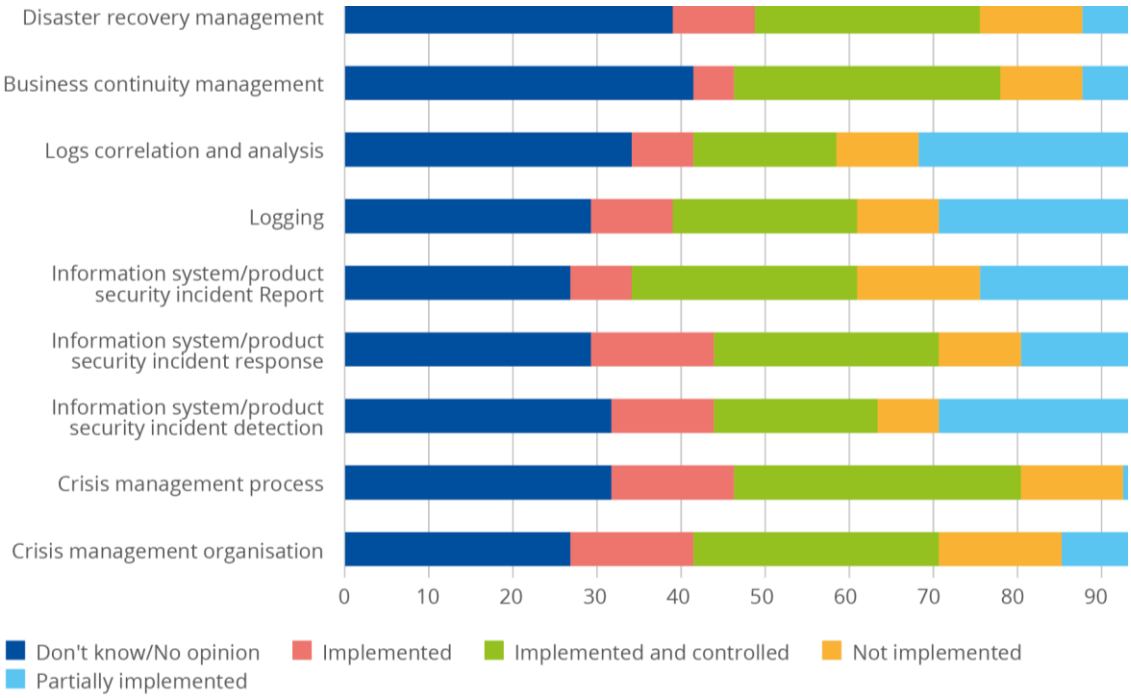
According to interviews conducted with the CAM stakeholders, the security measure related to the security accreditation of information system and product is mainly implemented by Tier 1 and Tier 2 suppliers and OEMs, and the automotive aftermarket. Otherwise, in general, operators do not necessarily accredit their product(s) prior to release. This can be explained by the fact that security accreditation of products is not yet mandatory for connected mobility related services in Europe. Additionally, it has to be acknowledged that cost to certify a product is something that should be always taken on a risk-based approach, as not all products should and can be certified.

The communication of stakeholders with the competent authorities and CSIRTs is part of the ecosystem management framework. Nevertheless, there are not a lot of CSIRTs exist with knowledge for CAM. The stakeholders are invited to set up a service enabling them to take note, without undue delay, of the information sent by their competent national authority concerning incidents, vulnerabilities, threats and relevant mapping (up-to-date inventory of CIS, interconnections of CIS with third-party networks, etc.). The CAM stakeholders have confirmed that security incidents are collected and treated, but the process of sending incidents and potential threats to their national competent authority is not mandatory for connected mobility-related services at this time. As a result, very few stakeholders have implemented this security measure focusing on communication between operators and authorities. Moreover, many stakeholders, apart from OEMs, do not have specific standards for their products.

Detection & Reaction

The following graph represents the answers given by all stakeholders in the survey.

Figure 16: Survey answer about the Detection and Reaction



The three following security measures related to the management of the CAM ecosystem will be further discussed:

- Logs correlation and analysis
- Logging

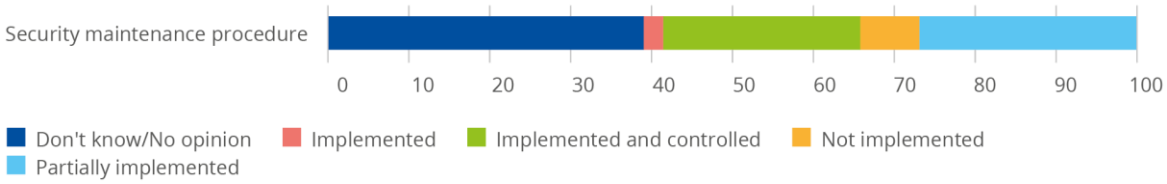
As concerns logs correlation and analysis, an operator creates a system that mines the events recorded by the logging system installed on each of the CIS/product in order to detect events that affect CIS/product security. There are different types of logs (e.g. system, network, technical, monitoring). For OITS, device behaviour is monitored with systematic processes when measuring logs correlation and analysis. In the CAM ecosystem, the correlation and analysis are tricky to set up as it can be on the vehicle, at the platform level, or even the infrastructure level, which means employing different computational resources. In this case as well, this security measure mostly revolves around OITS, Tier 1 and Tier 2 suppliers and OEMs, where associations have not expressed an opinion or reported that they do not implement this measure.

An operator, as part of the detection and reaction security measures, should also carry out logging, which is setting up a logging system on each CIS/product in order to record security-relevant events. An OITS for example, collects system logs for security, which are then cross analysed from different sources to detect security incidents. This happens systematically on servers, but yet to be installed on embedded devices due to feasibility, costs and system capabilities. These challenges are common throughout the ecosystem as analysing the collected (or logged) data necessitate resources, technical skills and awareness. In addition to OITS, Tier 1 and Tier 2 suppliers and OEMs have also mostly implemented the logging security measure.

Maintenance

The following graph represents the answers given by all stakeholders in the survey.

Figure 178: Survey answer about the Maintenance



The security maintenance procedure is the sole security measure under the maintenance domain. It refers to an operator developing and implementing a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum security level to be maintained for CIS/products resources.

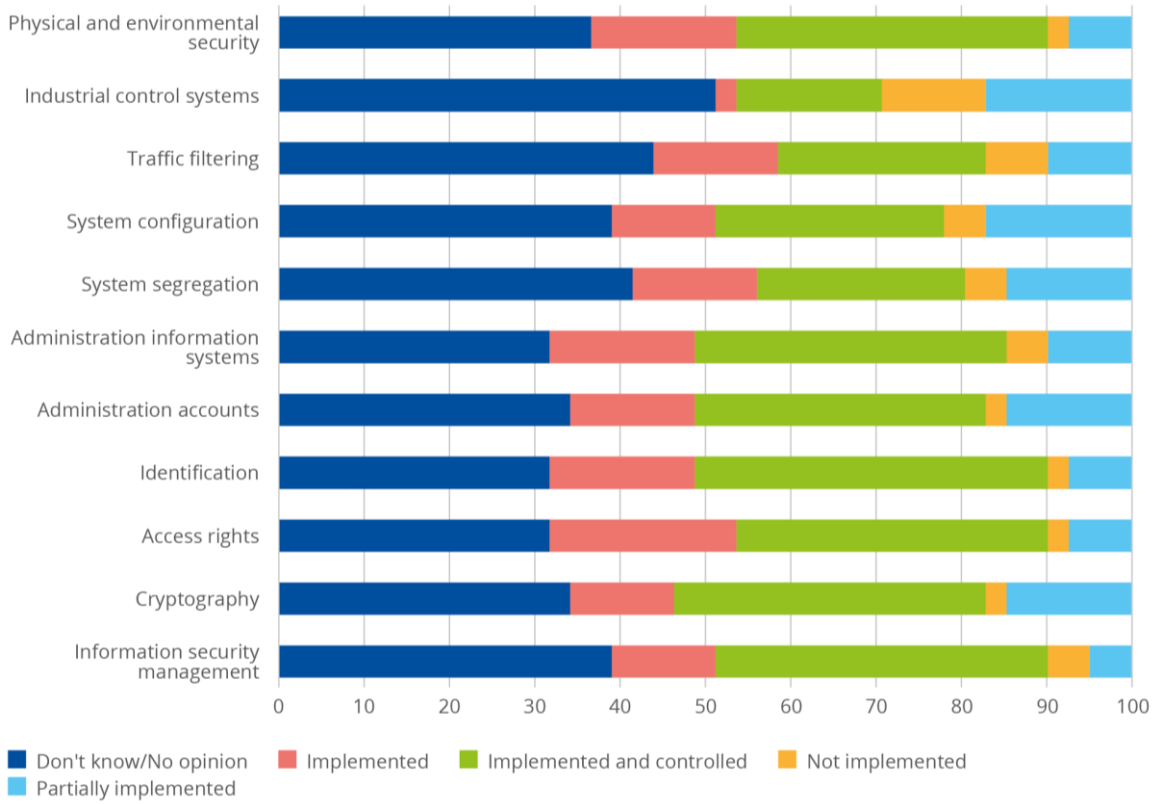
In the EU, there is legislation covering the fair access to repair and maintenance information by independent repairers, i.e. information that an OEM needs to be made available to automotive aftermarket operators to repair a vehicle.[31] However, at present, "there is no sector specific approach on the protection of the vehicle against cyberattacks", as stated in the legislation. The large majority of all respondents do not know or have no opinion on this security measure (incl. standardisation bodies, associations). Nevertheless, Tier 1 and Tier 2 suppliers (to a smaller extent OEMs and OITS too) have mostly responded with partially implemented and implemented and controlled.

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions: On the road to automated mobility: An EU strategy for mobility of the future. COM(2018) 283 final. Retrieved from: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf

IS/IT/OT security measures

The following graph represents the answers given by all stakeholders in the survey.

Figure 19: Survey answer about IS/IT/OT security measures



The following Information System (IS) / Information Technology (IT) / Operational Technology (OT) security measures of the CAM ecosystem will be further discussed:

- Industrial controlling systems

For industrial control systems (ICS), the operator takes the particular security requirements for ICS into account. ICS include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors. Control systems are important for critical infrastructures and are mutually dependable in the CAM ecosystem. These systems, integrated with new IT capabilities, need to be highly secure and tailored to the environment. Over half of the respondents do not know or have no opinion about this particular security measure. Nevertheless, among the rest of the respondents, especially Tier and Tier 2 suppliers, OEMs and OITS have partially implemented or even implemented and control this measure.

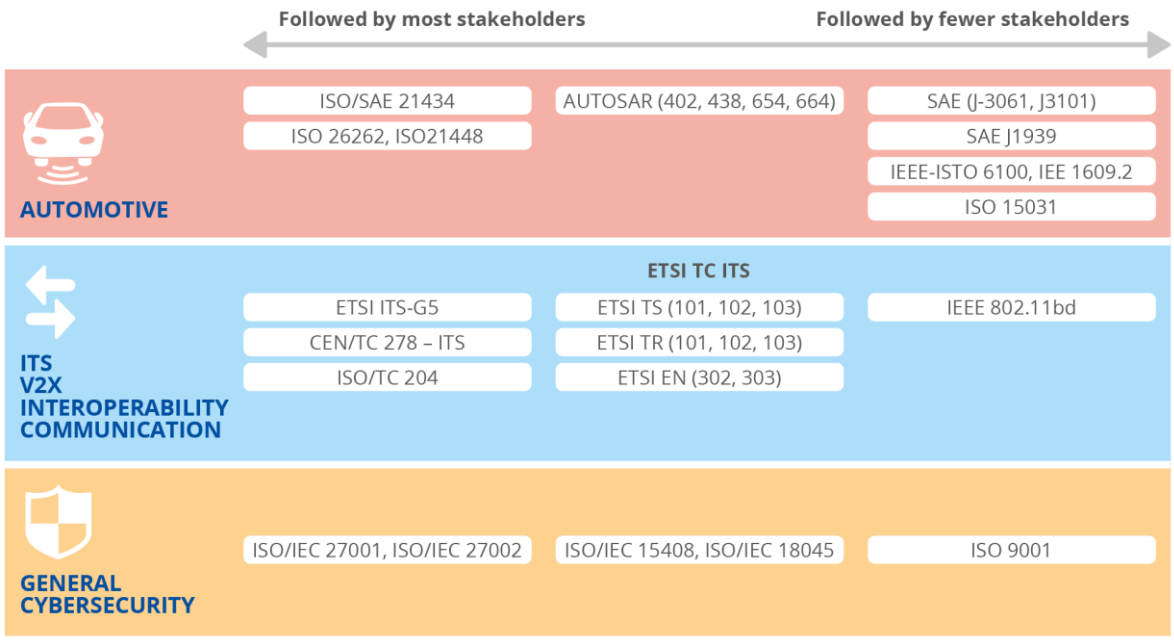
2.3.2 Standards

In the CAM ecosystem, developing technologies that are interoperable, safe and secure is a main challenge. As it has been done in the automotive industry in the last decades, CAM stakeholders are collaborating with various standardisation bodies in order to create standards that help to homogenise technologies used in the different technological stacks of the ecosystem, but also to standardise security measures, process and activities regarding cybersecurity of the CAM assets' lifecycle. These standards have different objectives:

- Standardise conception & development practices trough frameworks;
- Provide standardised processes for quality, cybersecurity and safety management;
- Provide frameworks for interoperability of systems between stakeholders;
- Provide standardised cybersecurity concepts, measures and solutions.

In the CAM industry, the most represented standardisation bodies are ISO (International Organization for Standardization), ETSI (European Telecommunication Standard Institute), IEEE (Institute of Electrical and Electronics Engineers Standards Association), and SAE (Society of Automotive Engineers).

Figure 20: CAM standards mapping



ISO standards are very transversal and cover themes of general cybersecurity processes (ISO/IEC 27k[32]) or quality management (ISO 9001[33]), cybersecurity recommendations for IT security (ISO/IEC 15408[34] & ISO/IEC 18045[35]) that are applicable for all CAM stakeholders to very specific development standards for automotive cybersecurity process (ISO/SAE 21434[36]), automotive safety process and recommendations for on-board systems (ISO 26262[37] &

[32] See more at: https://iso27001security.com/html/iso27000.html
[33] See more at: https://www.iso.org/iso-9001-quality-management.html
[34] See more at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408
[35] See more at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-18045
[36] See more at: https://www.iso.org/standard/70918.html
[37] See more at: https://www.iso.org/standard/43464.html

21448[38]) which are more focused around OEMs, their supply chain, and other relevant CAM stakeholder that interact with the vehicle. The currently in development standard on road vehicles: software update engineering is also relevant for CAM stakeholders (ISO/AWI 24089[39]).

ETSI, especially the TC ITS[40] committee, is focusing around standardisation of telecommunications and indeed developing multiple standards intended to provide guidance and frameworks for the implementation of secure communication between CAM assets such as vehicles and road infrastructures (ETSI ITS-G5[41]). More specifically, C-ITS, automotive radars, and dedicated short-range communications are addressed related to ITS. ETSI standards about telecommunications are also very important for interoperability purposes.

IEEE standards are generally focused on Intelligent Transport Systems and Automotive communications (IEEE 802.11bd[42]) but also providing specific guidance for implementing security measures when developing automotive software (IEEE-ISTO 6100[43]) or in-vehicle wireless access (IEEE 1609.2[44]).

Within stakeholders' groups such as the automotive industry, companies are collaborating in order to standardise conception practices and provide frameworks about on-board systems, software and intelligent mobility development. Regarding cybersecurity, AUTOSAR (Automotive Open System Architecture) provides different frameworks relevant within CAM ecosystem such as cryptography implementation (402[45], 438[46]), secure on-board communications (654[47]) and functional safety features (664[48]).

Depending on their activities, stakeholders are more or less involved with standardisation bodies. While some standards are very focused for stakeholders intended to conceive and develop CAM systems and infrastructures, standards providing general guidance about cybersecurity processes are relevant for all stakeholders because they provide a generic approach for risk management which enable the stakeholders to better identify and manage risks over their products lifecycle and operations.

[38] See more at: https://www.iso.org/standard/70939.html
[39] See more at: https://www.iso.org/standard/77796.html
[40] See more at: https://www.etsi.org/technologies/automotive-intelligent-transport
[41] See more at: https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.00_20/en_302663v010300a.pdf
[42] See more at: https://ieeexplore.ieee.org/document/8723326
[43] See more at: https://uptane.github.io/papers/ieee-isto-6100.1.0.0.uptane-standard.html
[44] See more at: https://standards.ieee.org/standard/1609_2-2016.html
[45] See more at: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SWS_CryptoServiceManager.pdf
[46] See more at: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-1/AUTOSAR_SWS_CryptoAbstractionLibrary.pdf
[47] See more at: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SWS_SecureOnboardCommunication.pdf
[48] https://www.autosar.org/fileadmin/user_upload/standards/classic/19-11/AUTOSAR_EXP_FunctionalSafetyMeasures.pdf

3. CONCLUSIONS

Regarding current security measures and challenges encountered, stakeholders had mixed views as cybersecurity maturity within CAM ecosystem is quite heterogeneous regarding the diversity of actors involved in the ecosystem. This also results in the diversity of cybersecurity regulations that may apply to the different types of stakeholders depending on their origin, though, the regulatory frame regarding cybersecurity over CAM ecosystem remain light. When being developed, this regulatory frame should specify what standards are preferred in order to comply with requirements defined. This shall aim to specify what cybersecurity measures should be considered the acceptable minimum for CAM actors in order to provide a certain level of secure products and services.

The CAM industry and stakeholders should work together in order to ensure technical terms are standardised and minimum requirements are agreed.

A future CAM system would need to rely on suitable and robust security mechanisms. Therefore, the cybersecurity challenges identified, as well as the proposed recommendations have to be covered by CAM stakeholders. For now, it cannot be reliably forecasted whether this is to be done mostly in the context of one overarching, maybe even mandatory framework, or if these aspects will mostly be covered in more individual concepts tailored to specific cybersecurity domains within the CAM ecosystem. In relation to type approval processes, OEMs have a well-defined framework associated to Regulation (EU) 2018/858[49], other stakeholders nevertheless need to conform to existing and future type approval processes.

As of today, there is no global cybersecurity governance framework covering the whole CAM ecosystem that propose an end to end model to cover cybersecurity risks. Hence, stakeholders generally collaborate through standardisation bodies and associations in order to develop homogenised cybersecurity frameworks and measures. Additionally, stakeholders collaborate through their contractual relationship that enable to formalise responsibilities regarding cybersecurity and risk management. However, these collaborations do not cover all aspects of cybersecurity for CAM and some specific topics are not considered yet, especially in some technical cybersecurity areas such as vulnerability disclosure, involvement of the national CSIRTs and information sharing. The CAM industry and stakeholders should work together in order to ensure technical terms are standardised and/or minimum requirements are agreed, to ensure all stakeholder can set-up cybersecurity activities specific to CAM assets using common methods and vocabulary.

[49] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. See more at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R0858

ABBREVIATIONS

Acronym	Definition
ADAS	Advanced Driver-Assistance Systems
AI	Artificial Intelligence
CAM	Connected and Automated Mobility
CCAM	Cooperative, Connected and Automated Mobility
C-ITS	Cooperative Intelligent Transport Systems
CSIRT	Computer Security Incident Response Team
DCS	Distributed Control Systems
DSP	Digital Service Provider
ESO	European Standards Organisation
ETSI	European Telecommunication Standard Institute
EV	Electronic Vehicle
GDPR	General Data Protection Regulation
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronic Engineers Standards Association
IoT	Internet of Things
IS	Information System
ISO	International Organisation for Standardisation
ISMS	Information security management
ISSP	Issue Specific Security Policy
IT	Information Technology
ITS	Intelligent Transport System
JRC	Joint Research Centre
MaaS	Mobility as a Service

Acronym	Definition
NCA	National Competent Authority
NIS	Network and Information Security Directive
OEM	Original Equipment Manufacturer
OES	Operator of Essential Services
OITS	Operator of Intelligent Transport System
OS	Operation System
OT	Operational Technology
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
RA	Road Authorities
R&D	Research and Development
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition system
UNECE	United Nations Economic Commission for Europe
V2V	Vehicle-to-vehicle
V2N and I2N	Vehicle-to-mobile network and Infrastructure-to-mobile network
V2D	Vehicle-to-devices
V2P	Vehicle-to-persons
V2G	Vehicle-to-grid
V2X	Vehicle-to-everything (Includes the notion of V2V, V2I, V2P and V2N communications)

A ANNEX: EU POLICY CONTEXT

Europe accounts for 23% of global motor vehicle production.[50] The European Commission supports the introduction and deployment of CAM on various levels, including safety, social responsibility, efficiency, as well as environmental friendliness. These include policy and legal initiatives, co-funding and/or launching research and innovation projects.

In 2016, the European Commission adopted the European Strategy on Cooperative Intelligent Transport Systems (C-ITS).[51] C-ITS refers to the group of technologies and applications that allow data exchange through various wireless communication technologies. In this light, the Strategy set out to deploy vehicles that communicate with each other (V2V) and with infrastructure (V2I) on roads in the European Union. Further elements of the Strategy included, among others, supporting various communication technologies, addressing security and data protection issues, developing a legal framework, and ensuring cooperation among the Member States. The EU also put in place a learning-by-doing approach, such as with the C-ROADS platform, a joint initiative by the Member States and road operators, in order to test and implement C-ITS services.[52] The platform as well as projects are co-funded by the EU through the Connecting Europe Facility (CEF).

In 2016 as well, the Directive on Security of Network and Information Systems (the NIS Directive)[53] was adopted and entered into force in August. The Member States then transposed the Directive into national law in May 2018. The NIS Directive is the first EU-wide legislation on cybersecurity, providing the legal measures boosting the overall level of cybersecurity in the EU. The Directive focuses on three parts: national capabilities, cross-border collaboration, and national supervision of critical sectors. The transport sector includes rail, air, water, and road and the Directive calls to identify the relevant road authorities and Operators of Intelligent Transport Systems. ENISA continuously supports the implementation of the NIS Directive in the road transport sector through, for example, the publication of reports on good practices for cybersecurity of smart cars, collaborating with DG MOVE through the C-ITS Platform, and the regular engagement with industrial stakeholders.

The two ENISA reports of good practices for cybersecurity of smart cars are as follows. ENISA, in 2017, published a study on Cybersecurity and Resilience of Smart Cars[54]. The report identifies good practices that ensure the security of smart cars against cyber threats, taking into account that smart cars' security should also guarantee safety. The three categories of good practices identified were policy and standards, organisational measures, and security functions. ENISA proposed recommendations for the different stakeholders in the smart car ecosystem, comprising smart car manufacturers, tiers, aftermarket vendors, insurance companies, industry

[50] As reported in 2018.
Factsheet: Connected & Automated Mobility – For a competitive Europe. (2018). European Commission. Retrieved from: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/3rd-mobility-pack-factsheets-automatedconnected.pdf
[51] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. 30 November 2016. Retrieved from: https://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf
[52] See more at: https://www.c-roads.eu/platform.html
[53] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[54] Cyber Security and Resilience of Smart Cars. (2017). ENISA. Retrieved from: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

groups, associations, and security companies. In 2019, ENISA then complemented the above-mentioned report by broadening the scope to (semi-)autonomous cars and Vehicle-to-Everything (V2X) communications. The published report on Good Practices for Security of Smart Cars[55] highlights the importance of cybersecurity for connected cars. The report identifies the asset and threat taxonomy of connected and autonomous vehicles, the threats targeting the smart cars ecosystem as well as the potential security measures, complemented by good practices mitigating them.

In 2017 through 2018, after years of negotiation the European Parliament, Commission and Council of Ministers agreed on the adoption of three Mobility Packages.[56] These Mobility Packages are a collection of three initiatives that aim to implement changes to EU road transport rules. Mobility Package 1 covers various aspects of the industry, including social, enforcement, technical, and regulatory issues. Mobility Package 2, also named Clean Mobility Package, contains legislative proposals for the transport sector that aim for low and zero emission vehicles and fight climate change. Finally, Mobility Package 3 encompasses legislative proposals in the areas of safe, clean and connected mobility.

In 2018, the Commission published a Communication on the road to automated mobility: An EU strategy for mobility of the future.[57] Europe aims to become a world leader in the deployment of connected and automated mobility, and also insists on bringing down road fatalities, reducing harmful emission, and decreasing congestion. The final goal is full automation and safe driverless mobility, with a timeline envisaged to achieve this by 2030, followed by the so-called Vision Zero[58]: no road fatalities on European roads by 2050.

In 2019, the European Commission launched the EU-wide Cooperative, Connected, Automated and Autonomous Mobility (CCAM) Single Platform, consisting of both private and public stakeholders. The CCAM Single Platform is a joint directive of Directorate-General for Mobility and Transport (DG MOVE), Directorate-General for Communications Networks, Content and Technology (DG CNECT), Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) and Directorate-General for Research and Innovation (DG RTD). The platform advises and supports the Commission for open road testing, as well as coordinated research, piloting, testing and deployment activities. Furthermore, there are six working groups for the different facets of CCAM: WG1 Develop an EU agenda for testing; WG2 Coordination and cooperation of R&I; WG3 Physical and digital road infrastructure; WG4 Road safety; WG5 Connectivity and digital infrastructure for CCAM; WG6 Cybersecurity and access to in-vehicle data linked to CCAM.

[55] Good Practices for Security of Smart Cars. (2019). ENISA. Retrieved from: https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars
[56] See more at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/package-eu-mobility-package
[57] Communication from the Commission on the road to automated mobility: An EU strategy for mobility of the future. 15 May 2018. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0283
[58] White Paper: Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system. European Commission. 28 March 2011. Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0144:FIN:en:PDF

B ANNEX: CYBERSECURITY MEASURES

The proposed cybersecurity measures, according to domain, are listed below.

Governance

Security measures	Description
Standards application	The operator refers to standards in its assessment of cybersecurity risks and the mitigations, as well as when describing the process employed.
Cybersecurity management system	The operator has a Cyber Security Management System in place that considers the whole lifecycle of the Critical Information System (CIS) / product, particularly development, production and postproduction.
Cybersecurity management system audit	The operator regularly audits its Cyber Security Management System.
Information system / product security policy	The operator establishes, maintains up-to-date and implements an information system security policy (ISSP) approved by senior management, guaranteeing high level endorsement of the policy.
Information system / product security indicators	For each CIS / product and according to a number of indicators and assessment methods, the operator evaluates its compliance with its ISSP. Indicators may relate to the risk management organisation's performance, the maintaining of resources in secure conditions, etc.
Human resource security	The established information system security policies set up a CIS / product security awareness raising program for all staff and a security training program for employees with CIS related responsibilities.

Risk & Ecosystem management

Security measures	Description
Information system / product security risk analysis	The operator conducts and regularly updates a risk analysis, identifying its Critical Information Systems (CIS) / products underpinning the provision of the essential services and identifies the main risks to these CIS.
Information system / product security audit	The operator establishes and updates a policy and procedures for performing information system and product security assessments and audits of critical assets and CIS, taking into account the regularly updated risks analysis.
Information system / product security accreditation	The operator accredits the CIS / product prior to release.
Ecosystem relations / Suppliers risk management	The operator establishes a policy towards its relations with its ecosystem in order to mitigate the potential risks identified. This includes suppliers in particular but is not limited to interfaces between the CIS and third parties. In addition to risk identification, such a policy should also include sharing of relevant interoperability and compatibility related cybersecurity information for product development and integration.
Ecosystem / Suppliers mapping	The operator establishes a mapping of its ecosystem and specifies responsibilities sharing, including internal and external stakeholders, including but not limited to suppliers, in particular those with access to or managing operator's critical assets / products.
Communication with competent authorities and CSIRTs	The operator implements a service that enables it to take note, without undue delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings (up-to-date inventory of CIS, interconnections of CIS with third-party networks, etc.).

Detection & Reaction

Security measures	Description
Crisis management organisation	The operator defines in its ISSP the organisation for crisis management in case of security incidents or cyber-attacks and the continuity of organisation's activities.
Crisis management process	The operator defines in its ISSP the processes for crisis management which the crisis management organisation will implement in case of security incidents or cyber-attacks and the continuity of an organisation's activities.
Information system / product security incident detection	The operator sets up a security incident detection system for detection of incidents or cyber-attacks that affect the functioning or the security of its CIS / products, in accordance with its ISSP.
Information system / product security incident response	The operator creates and keeps up-to-date and implements a procedure for handling, response to and analyses of incidents that affect the functioning or the security of its CIS, in accordance with its ISSP.
Information system / product security incident Report	The operator creates and keeps up-to-date and implements procedures for incidents' reporting.
Logging	The operator sets up a logging system on each CIS / product in order to record security relevant events.
Logs correlation and analysis	The operator creates a log correlation and analysis system that mines the events recorded by the logging system installed on each of the CIS / product in order to detect events that affects CIS / product security.
Business continuity management	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding business continuity management, in case of IT security incident.
Disaster recovery management	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding disaster recovery management, in case of a severe IT security incident.

Maintenance in security condition

Security measures	Description
Security maintenance procedure	The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum-security level to be maintained for CIS / products resources.

IS/IT/OT security measures

Security measures	Description
Information security management	The relevant information security information about Critical Information Systems (CIS) and products is managed by an information security management system. The operator protects its sensitive documents and files on dedicated file servers with adequate protection measures.
Cryptography	In its ISSP, the operator establishes and implements a policy and procedures related to cryptography, in view of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in its CIS (use of standard, security controls shall be implemented for storing cryptographic keys, etc.).
Access rights	Among the rules defined in its systems security policy, the operator grants access rights to a user or an automated process only when that access is strictly necessary for the user to carry out their mission or for the automated process to carry out its technical operations based on the principle of least access privilege.
Identification	For identification, the operator sets up unique accounts and supporting authentication schemes for users or for automated processes that need to access resources of its CIS. Unused or no longer needed accounts are to be deactivated. A regular review process should be established.
Administration accounts	The operator sets up specific accounts for the administration, to be used only for administrators that are carrying out administration operations (installation, configuration, management, maintenance, etc.) on its CIS. These accounts are kept on an up-to-date list.
Administration information systems	Hardware and software resources used for administration purposes are managed and configured by the operator, or, where appropriate, by the service provider that the operator has authorised to carry out administration operations.
System segregation	The operator segregates its systems in order to limit the propagation of IT security incidents within its systems or subsystems.
Systems configuration	The operator only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS.
Traffic filtering	The operator filters traffic flows circulating in its Critical Information Systems (CIS). The operator therefore forbids traffic flows that are not needed for the functioning of its systems and that are likely to facilitate an attack.
Industrial control systems	The operator takes the particular security requirements for ICS (control systems, SCADA systems, etc) into account.
Physical and environmental security	The operator prevents unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

TP-03-20-676-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-407-7
DOI: 10.2824/24902