EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RECOMMENDATIONS FOR THE SECURITY OF CAM

Recommendations for the Security of Connected and Automated Mobility

MAY 2021

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 (Sylpheo), 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), Chris Church (INTERPOL), 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

ISBN 978-92-9204-408-4, DOI 10.2824/748518

TABLE OF CONTENTS

ABBREVIATIONS

Acronym	Definition
AI	Artificial Intelligence
CAM	Connected and Automated Mobility
CISOs	Chief information security officer
CSIRT	Computer Security Incident Response Teams
CVSS	Common Vulnerability Scoring System
E/E	Electrics/Electronics architectures
GDPR	General Data Protection Regulation
GSR	General Vehicle Safety Regulation
IS	Information System
ISAC	Information Sharing and Analysis Centre
ISMS	Information Security Management System
ISP	Internet Service Provider
IT	Information Technology
ML	Machine Learning
OEM	Original Equipment Manufacturer
OITS	Operator of Intelligent Transport System
OT	Operational Technology
R&D	Research and Development
RA	Road Authority
ROI	Return on Investment
SME	Small and medium-sized enterprise
UNECE	United Nations Economic Commission for Europe
V2D	Vehicle-to-devices
V2G	Vehicle-to-grid
V2I and I2V	Vehicle-to-infrastructure and Infrastructure-to-vehicle
V2N and I2N	Vehicle-to-mobile network and Infrastructure-to-mobile network
V2P	Vehicle-to-persons
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything (Includes the notion of V2V, V2I, V2P and V2N communications)

1. INTRODUCTION

1.1 STUDY OBJECTIVES AND SCOPE

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. Under a new regulation set by the United Nations[2], car manufacturers are required to secure vehicles against cyberattacks. In the European Union, the new regulation on cybersecurity will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.[3] Moreover, the UNECE Regulation and related ISO standards apply to all CAM stakeholders who must ensure that their products and services conform to cybersecurity goals. Increased connectivity and technological development in the ecosystem through various services, components and technologies are continuously expanding. Therefore, within the CAM sector, where innovation and market growth are expanding, global players in the CAM sector face a risk of cyberattacks. Connected services may be attacked by cyber-attackers and create cyber fraud, data breach and privacy incidents, as well as software overrides resulting in dangerous situations and accidents when part of the vehicle to everything (V2X) network is attacked, thereby threatening the drivers, road users and companies. Efforts across the whole industry should be made to ensure that even if one system is compromised and/or tampered, the rest of the systems remain unaffected.

The interlinking of systems and services (both inside and outside the vehicle) and thus intelligent and connected mobility are already revolutionising users' lives. The whole ecosystem involved in the CAM lifecycle has to cope with key challenges that add complexity to responding and managing CAM cybersecurity risks. Today, connected vehicles, connected environment and connected infrastructure should be designed with new capabilities and features that have the potential to provide increased safety, better vehicle performance, competitive digital products and services, more comfort, environmental friendliness, as well as convenience for its end-users. Governments, manufacturers, private companies (incl. SMEs and start-ups) as well as IT enterprises are all involved in the future development of intelligent and connected and automated mobility. Fixed and mobile telecommunication infrastructure is necessary for cars to communicate with the smart road infrastructure (I2V and V2I), with devices (V2D), between vehicles (V2V), with other networks such as access to cloud infrastructure (V2N) as well as within the vehicle.

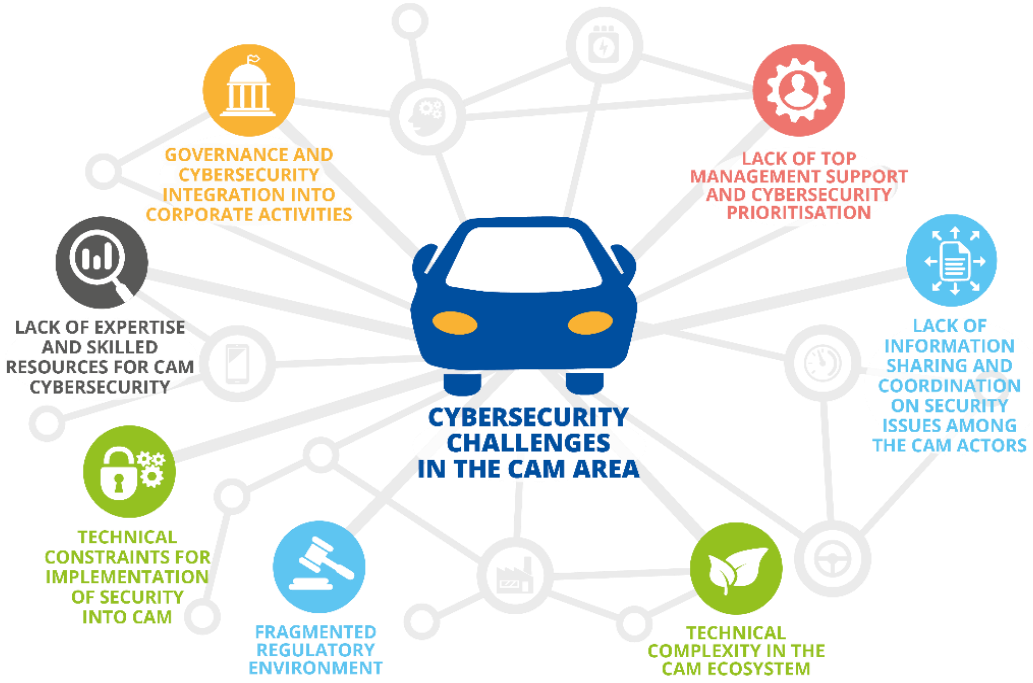
The aim of this report is to provide a high-level overview of the cybersecurity challenges in the CAM sector and to highlight both the concerned CAM actors and associated recommendations. Cybersecurity in the CAM ecosystem is partially standardised and the role of standards is widely recognised. All stakeholders' contributions to the CAM ecosystem are intertwined. Standards and regulations are often not adopted uniformly worldwide, and therefore some countries may advance faster than others in building a safe and secure cybersecurity system around CAM infrastructure. In the context of growing cybersecurity threats and concerns about cybersecurity and data protection, this report aims to identify the main challenges in the current situation and to propose actionable recommendations for the different stakeholders involved in the CAM ecosystem to enhance the level of security and resilience of CAM infrastructures and systems in Europe. Challenges in the CAM ecosystem arise from the whole lifecycle, therefore this report

[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] 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
[3] See more at: 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

points to detailed challenges that the stakeholders are facing across Europe. The recommendations proposed by ENISA aim to guide all CAM ecosystem stakeholders and to contribute to the improvement and harmonisation of cybersecurity in the CAM ecosystem in the European Union.

Using a layered approach of primary and secondary research, this report summarises insights across a complex CAM ecosystem. Primary research methods included a survey and a series of interviews and validation discussions with key stakeholders from the CAM ecosystem. Secondary research methods included desktop research of 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.

Figure 1: Cybersecurity Challenges in the CAM area

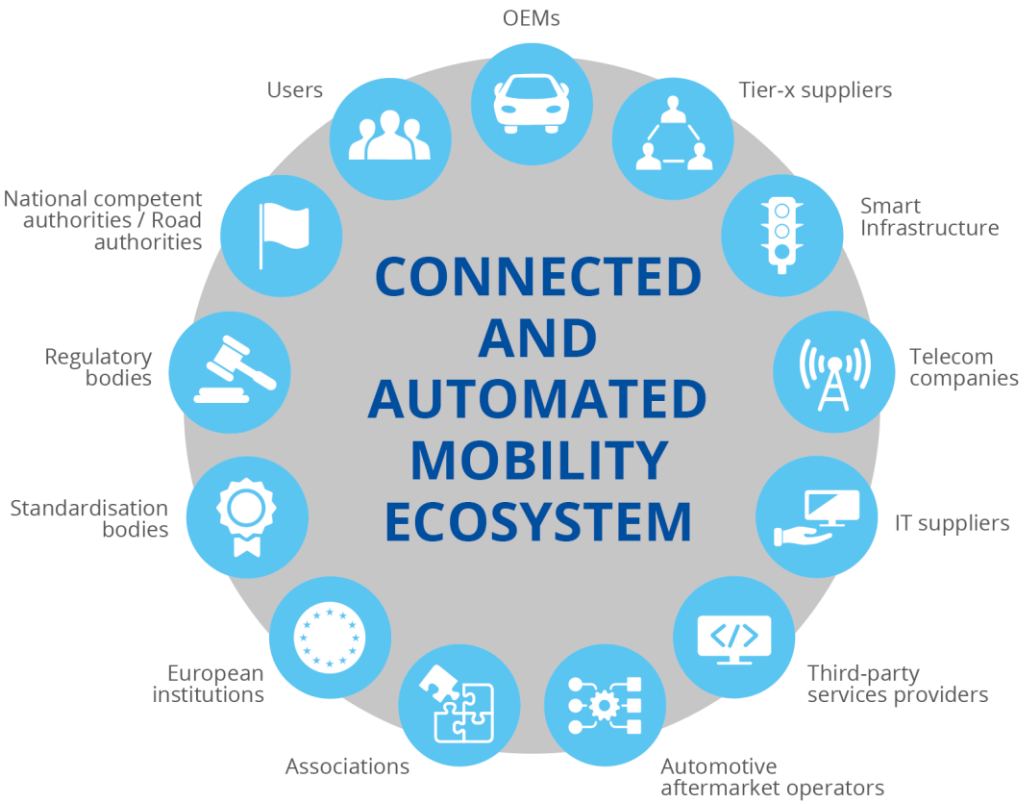


1.2 TARGET AUDIENCE

The target audience of this report comprises the following actors of the CAM ecosystem:

- 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

Figure 2: CAM Stakeholders' Mapping



1.3 DOCUMENT STRUCTURE

In this brief document, the main challenges emerging in the CAM sector and associated recommendations are proposed. Each challenge identified is complemented with a set of actionable recommendations, which are followed by the target stakeholder groups they address.

2. CYBERSECURITY CHALLENGES AND RECOMMENDATIONS IN THE CAM AREA

2.1 GOVERNANCE AND CYBERSECURITY INTEGRATION INTO CORPORATE ACTIVITIES

Cybersecurity governance in the CAM ecosystem represents an organisational and technical challenge for all stakeholders within it. The emergence of CAM where digital technology and connectivity encounter the physical world of transportation involves the definition of a cybersecurity approach that answers the specific needs and constraints of CAM. In the CAM environment, there are:

- **Connected services and off-board systems** that are characterised by agile development cycles involving the continuous evolution of services following staggered releases, a large number of short-term projects generally based on scalable and modular cloud architectures which are managed by Information System (IS)/Information Technology (IT) teams or hosting services providers.

- **Various physical infrastructures, equipment, products and associated services, vehicles and soft-mobility devices** based on Operational Technology (OT), electrics/electronics (E/E) architectures and on-board systems managed by engineering teams, which are characterised by a much longer development cycle and which must meet the security and technical requirements associated with various types of quality validations or regulatory approvals (e.g. vehicle type approval).

The above two different parts of the environment have an impact on cybersecurity and its integration into development projects as well as broadly into corporate activities. This new relation between teams evolving into the digital world, and 'historic' teams developing and operating physical products is a challenge in terms of collaboration, which does not ease cybersecurity governance. Developments on each side can affect the security of the other side, thereby making the risk approach holistic which has proven to be challenging in environments where a clearly stated and efficient governance has not yet been put in place.

The different actors of the CAM ecosystem, from international companies to start-ups, have started to tackle this new model. Indeed, companies have started to grow new expertise, skills and competences, enabling the integration of digital into the transport sector by hiring new profiles, transferring competences and opening up internally. Companies have also started collaborating with partners, start-ups and other suppliers that could provide the required expertise. However, for the larger structures, it has been more difficult to implement this new model of governance requiring the mastery of digital and IT technologies in their research and development (R&D) and core processes considering their size, thereby generating inertia for organisational change.

The introduction of new skills within existing entities or through new entities is necessary to adapt organisations and to clarify roles and responsibilities vis-à-vis these new capabilities. In this context, the roles and responsibilities of employees regarding cybersecurity within the different entities are not clearly defined, creating a gap in the capacity to deal with security-related issues. In addition, a seamless integration of security activities into the execution of core

business activities is directly related to the lack of concern for cybersecurity. If cybersecurity becomes a core business objective, businesses would become integrated and prepared to rely more effectively on cybersecurity teams to manage their risks and address potential vulnerabilities. Responsibility and accountability for security needs to be clearly defined for the various stakeholders, which is generally not the case. This is directly linked to the lack of cybersecurity integration into the corporate strategy and business planning, associated to lack of awareness and trainings to corporate resources, as well as the legislative requirements that need to be adapted.

2.1.1 Recommendations

Cybersecurity is a shared responsibility, and when considering CAM products and services, this becomes even more of a reality because their security and privacy are part of the very core business value. Software and data are integrated into objects designed and engineered to provide mobility and transport services using on-board and off-board systems with very specific technologies. In the CAM ecosystem, cybersecurity shall not be seen as a standalone topic that provides requirements and expertise beside other engineering, development and operations teams. It should be seen as a core enabler that protects safety and provides value to products and services, and is integrated in the lifecycles of products' and services' activities.

At all stages of CAM products' and services' lifecycles, risks must be managed, and cybersecurity activities performed. It shall be the responsibility of product and process owners to ensure that, by relying on the security expertise and resources provided by their organisation, the risks related to their activity is well assessed and treated. Cybersecurity must become part of the core business of an organisation in the delivery of its activities.

To foster better governance and integration of cybersecurity into corporate activities, ENISA recommends to:

- Raise awareness to the top management level of the organisation, where appropriate, about the impact of cybersecurity and technology on the CAM ecosystem lifecycle.
- Raise awareness throughout the organisation, and especially at the right decision level within the company or group, about the impact of cybersecurity and technology on the CAM ecosystem lifecycle.
- Promote the integration of cybersecurity along with digital transformation at the board level in the organisation.
- Advise on fast-moving business and technology topics such as cybersecurity on a permanent basis at board level of the organisation.
- Promote the acceleration of cybersecurity in research and development spending on CAM technology to keep up with cybersecurity developments.
- Promote procurement processes to integrate cybersecurity risk-oriented requirements.
- Address cybersecurity skills to keep up with the creative (e.g. design thinking) skills that the company's strategy aims to foster.
- Define clear roles and responsibilities regarding cybersecurity within the organisation, not only for the cybersecurity branch, but also the relevant business and corporate functions, up to the global risk owner for the product, system or service.
- Take into regard the cybersecurity needs of both business and supporting processes according to the cybersecurity risks of assets handled by such processes.
- Define a risk management process enabling risk assessment, treatment decision and ownership over the product/service lifecycle.
- Consider cybersecurity activities in projects and business planning, by establishing collaboration schemes between different teams (e.g. business and cybersecurity).

The recommendations are targeted at:

- Automotive Aftermarket Operators
- Mobility Services Providers
- Original Equipment Manufacturers (OEMs)
- Road Equipment Manufacturers
- Smart City Operators
- System Providers
- Tier 1 and Tier 2 Suppliers

2.2 LACK OF TOP MANAGEMENT SUPPORT AND CYBERSECURITY PRIORITISATION

In the complex context of CAM, cybersecurity has generally not been considered a priority by corporate management in the CAM industry. So far, cybersecurity has not been perceived as a board-level topic. Indeed, not all organisations of the CAM ecosystem are involving the corporate management in cybersecurity problematics. Furthermore, cybersecurity executives have few interactions with corporate executives which is why it is so shallowly integrated into the global strategy and objectives of companies. As a primary consequence, the lack of management involvement leads to insufficient financial support to ensure cybersecurity is addressed as a key topic in the lifecycle of CAM products and services. Also, the lack of cybersecurity consideration that involves cybersecurity strategic planning is generally not as robust as it should be. It also makes it difficult for the teams in charge of cybersecurity to obtain enough resources for R&D, to deploy awareness and training programs, as well as to carry out operational activities in the most effective manner. Hence, the cybersecurity dimension is rarely anticipated and integrated into business planning since business priorities tend to focus primarily on innovation, quality, cost, and time-to-market rather than on cybersecurity. However, with the emergence of legislation and requirements from national and international regulatory bodies for CAM cybersecurity, such as the General Vehicle Safety Regulation (GSR) from the European Commission that will enforce the UNECE WP29 cybersecurity regulation for European countries as of 2022. It regulates that vehicles will have to comply with applicable cybersecurity regulations and standards in order to be put on the market. The UNECE regulation however covers just part of the CAM ecosystem, providing only qualitative requirements and does not include all stakeholders.

In addition to the low consideration of cybersecurity in corporate management, most of the stakeholders interviewed ranked the financial resources available for cybersecurity as a main challenge to enable the teams to carry out state-of-the-art activities and effectively address all identified risks. The budget allocation of companies is generally based on the estimated Return on Investment (ROI) of business activities and it is sometimes acknowledged that the difficulty of calculating the ROI of budgets allocated to cybersecurity is the reason why companies limit their investments. The impact of cybersecurity on increasing revenues or optimising costs generally remains uncertain for companies in the CAM industry. Regulatory aspects might tend to rationalise the perception of cybersecurity ROI since it is becoming a requirement to be integrated in the products' and services' planning and lifecycle.

In the context of quickly increasing development of CAM products and services, as well as a regulatory landscape that becomes demanding regarding cybersecurity, a lack of cybersecurity consideration can significantly impact companies' operations and reputations which can lead to severe safety impacts or financial loss.

Regarding the complexity of the CAM ecosystem and of its services and products, implementing cybersecurity in an efficient way requires implementing an adequate strategy and associated funding for its deployment. To foster success, the cybersecurity strategy must not be built in a standalone manner but streamlined with the business strategy in order to make it realistic and capitalise on synergies. Hence the cybersecurity strategy must be acknowledged and supported

by top management as an enabler to the satisfying development and operations of CAM products and services.

2.2.1 Recommendations

To build a strategy, a mind-set shift is required so that cybersecurity is not seen as a cost and pure loss of money that may avoid potential risks, but as a real enabler of important business opportunities made possible by the mastering of technologies. Cybersecurity allows to reduce time to market and provide state-of-the-art products and services to customers that are secure, reliable and trustworthy. In order to follow the technological developments, adequate budgets must be devoted for cybersecurity innovation and R&D activities, as well as ensured for cybersecurity operations such as security maintenance, detection and reaction activities.

Since new regulations will enforce to perform risk management activities and ensure products' and services' security, CAM actors shall transform this constraint into an opportunity to add value to their deliveries by making the process more robust and by raising the quality of their products and services through security and privacy.

To foster better prioritisation of cybersecurity by corporate leads and better funding and budget allocation of cybersecurity, ENISA recommends:

- Establish administrative structures for top-level management to discuss and exchange views with cybersecurity experts and CISOs.
- Incentivise innovation and R&D activities for securing IT and CAM environments, components, systems and services.
- Promote the aspect of security in companies' business strategies by learning from automotive industry practices.
- Consider the development of certification schemes for automotive industry security (taking into account the inherent particularities when defining the target of evaluation), in order to promote harmonisation of the market, increase consumer trust and open up new business opportunities.
- Foster a corporate security culture by involving cybersecurity directly in the management board.
- Establish regular training programmes for the different levels of the company, including top management, in order to bring awareness on cybersecurity legal requirements as well as possible threats, risks and security measures.
- Develop targeted cybersecurity information and certification schemes for SMEs in the automotive aftermarket and servicing sector.
- Define common requirements and responsibilities for all stakeholders involved in the CAM ecosystem.

The recommendations are targeted at:

- Automotive Aftermarket Operators
- Operators of Intelligent Transport Systems (OITS)
- Original Equipment Manufacturers (OEMs)
- Road Equipment Manufacturers
- Smart City Operators
- Tier 1 and Tier 2 Suppliers

2.3 TECHNICAL COMPLEXITY IN THE CAM ECOSYSTEM

In the mobility and transportation sector, the number of actors and tiers interacting is important. The multiplicity of stakeholders involved around infrastructures, connected services and products along the value chain leads to different challenges concerning the implementation and management of cybersecurity and efficient risk management. Dependencies, interactions and

supply chain management in this sector are a well-known challenge acknowledged by the majority of the actors involved.

For instance, the delivery of a service such as public transportation will involve a vehicle manufacturer and all its supply chain: a public transport operator, its suppliers and partners for operations and maintenance, the road and public authorities and management, insurance companies, interactions with other road users, automotive aftermarket operators, service providers, and so on. In this landscape where the products, services and operations of each stakeholder can affect the security of the end users, the products and the companies involved, a comprehensive and commonly acknowledged cybersecurity alignment is needed in terms of legal, technical and practical aspects between parties. The dependencies between stakeholders generates a need for interoperability, which will stem from the cybersecurity model. It starts by defining and sharing roles and responsibilities that raises a need of alignment of role and responsibility principles within the ecosystem, and a continuous cybersecurity information sharing between stakeholders. Clarifying roles and responsibilities is one of the enablers to define and implement security by design for products and services, where all stakeholders ensure the risks are managed over their perimeter in order to secure all chain links and guarantee a holistic cybersecurity approach. The implementation of roles and responsibilities would need to be supported by establishing a harmonised authorisation process. Integrating security by design for all products and services is essential, however, security needs to be considered in a more holistic manner in terms of interactions of products and services developed by multiple stakeholders, including automotive aftermarket operators, which essentially affects the end-to-end security of the vehicle over its lifetime, including post-production. Building an approach where the technical complexity has to be settled between all the diverging and sometimes competing actors is a major challenge.

Today, users' needs are increasing in terms of connectivity and they want to get the connected products and services at the state-of-the-art, at the right time and at a low price. In parallel, despite the added value of CAM's emerging technologies for customers and new potential revenues for the companies of the CAM ecosystem, the complexity of their development, deployment and adoption has an impact on the scalability of the CAM concept as well as on the potential ROI for investor and sustainability for companies involved in the CAM ecosystem. The CAM industry, in its widest sense, is therefore confronted with the complexity of new technologies requiring skills and knowledge that were not previously managed by the industry, which are costly and time-consuming to implement. At the same time, the CAM industry needs to meet the demands of users at a reasonable cost to remain competitive in the market. In this quite recent context, finding the right balance between innovation, cost management and the need for security remains an open challenge given the current low budget allocated to cybersecurity in the CAM industry.

2.3.1 Recommendations

It is evident that technical complexity could lead to the introduction of new attack vectors due to the whole interaction of the CAM ecosystem. To overcome these challenges, ENISA recommends:

- Promote the use of common security measures across components and services to adhere to a minimum level of cybersecurity and ensure an appropriate level of security.
- Promote the use of suitable certification schemes.
- Promote security assessment for both on-board and off-board solutions and standardise the discovery and remediation of vulnerabilities during the lifetime of the product.
- Ensure that the organisation maintains a consistent and up-to-date asset inventory.

The recommendations are targeted at:

- National Authorities
- Policy Makers
- Regulatory Bodies
- Road Authorities (RA)

Additionally ENISA recommends:

- Consider defining an industry standard to share threat intelligence, report monitoring outputs and cybersecurity incidents and enable collaboration regarding cybercriminal activity targeting CAM between ecosystem parties.
- Consider applying data security strategies (privacy compliance mechanisms) and require minimum level of security measures for the whole CAM ecosystem.
- Use tools supporting asset management (e.g. servers, software, onboard components) that can automatically discover, identify and enumerate assets specific to the organisation of the CAM ecosystem (e.g. tools enabling to constitute a Configuration Management Database).
- Ensure a change management process is implemented in the CAM ecosystem, in order to verify that evolutions applicable to hardware, software or configuration are assessed and validated regarding their potential cybersecurity impacts.
- Establish cybersecurity requirements and validation methods that are incorporated as standard deliverables in OEMs' and suppliers' development processes, starting from the concept phase of any new product development.
- Incentivise the use of cybersecurity certified components if they exist to bring a better level of security.
- Designate one or several dedicated security team(s) with security specialists having a diversified and broad range of competencies in security-related topics (e.g. risk assessment, penetration testing, secure design).
- Apply a hardening approach (e.g. measures such as authentication, encryption, segmentation, filtering, code quality check) on different levels (i.e. devices, network, back-end, etc.) to reduce the possible attack surface.
- Reinforce interfaces' robustness to, among others, cope with buffer overflows or fuzzing.
- Consider strengthening applications' isolation at runtime, using trusted software technologies.
- Apply system, sub-domain and network segregation using physical and logical isolation techniques where appropriate (based on a risk assessment and an appropriate allocation of rights and roles).
- Harden against adversarial attacks, to prevent Artificial Intelligence (AI) and Machine Learning (ML) components from being attacked.
- Prevent data falsification or manipulation in regard to AI and ML.
- Use data redundancy mechanisms (e.g. sensor data fusion) that correlate data acquired from the different sensors in the system and data obtained via external communications before making a decision.

The recommendations are targeted at:

- Automotive Aftermarkets Operators
- Original Equipment Manufacturers (OEMs)
- Road Equipment Manufacturers
- Smart City Operators
- System Integrators
- System Providers
- Tier 1 and Tier 2 Suppliers

2.4 TECHNICAL CONSTRAINTS FOR IMPLEMENTATION OF SECURITY INTO CAM

As the CAM industry is moving towards increased connectivity and automation, the technical constraints of managing threats relative to the ecosystem also increases. Cybersecurity risks can be particularly complex to manage for the CAM sector. Risks can be triggered across both the physical and digital world since both consume and create data, as systems are communicating with the surrounding ecosystem through different types of short and long range connectivity. In this context of technological diversity, the adversary model to consider for risk management may be quite large, meaning that the approach to secure CAM products and services in order to identify relevant attack paths and implement the right security measures will require the assessment of a wide variety of systems and technical assets, making it a consequent approach to secure CAM assets during their conception and development phases. At the moment, there are few commitments to standardisation of CAM technologies (e.g. communication protocols, data format), which forces cybersecurity professionals to address and master different technologies and solutions for similar functions. In addition, for the CAM ecosystem, there is no holistic end-to-end approach to manage risks, nor a comprehensive security model to implement for a unified cybersecurity approach of CAM products and services.

As the CAM sector is very innovation-oriented, the continuous evolution and development of new technologies for CAM assets also involves taking into account particular technical constraints when it comes to securing the various assets. When taking into account emerging technologies such as those in CAM, security measures and standards do not yet exist to provide best practices and guidelines in order to manage risks with state-of-the-art security measures and solutions acknowledged by the industry. Cybersecurity teams often have to develop their security features and solutions from scratch for emerging CAM technologies, making it longer, more complex and costly, as well as potentially more error prone. There are not yet enough mature ‘on-the-shelf’ solutions to secure connected products, even though new actors are emerging and propose turn-key cybersecurity solutions for the CAM ecosystem, though without much feedback on their efficiency.

The new features proposed, for example by electric and autonomous vehicles, infrastructures such as charging stations or the connectivity with personal devices required for the use of e-scooters and other free-floating devices, create opportunities for malicious parties to perform attacks in order to gain access to vehicles’ functions, steal data or ransom users. When considering the potential impacts for safety and public order, if control is taken over systems at the scale of a city or a fleet of vehicles, cybersecurity must be a forefront stake, especially in a context where the threats to consider can come from the nation state or large criminal organisations. The CAM topic being fairly recent, its cybersecurity industry is not as mature as it can be for traditional IS/IT. Also, considering the nature of its services and products that are integrated into the transport sector landscape and can have safety impacts or large operational impacts for cities flows, cybersecurity experts promote the cybersecurity and privacy by design approach. Security components, software and hardware, must be removable and replaceable with compliant parts. Components, or wearing parts, have a lifetime shorter than the vehicle itself. This approach means that rather than treating cybersecurity subsequently with additional hardening or detection solutions, it should be addressed in the early conception phases by ensuring there are no vulnerabilities in the design of services and products. This requires that the right cybersecurity skills and competences are provided to the R&D and design teams and that is why the CAM ecosystem is currently making its cybersecurity teams grow.

2.4.1 Recommendations

As stated above, regarding the diversity and complexity of the technologies used in the ecosystem, there are no standardised solutions for the security of CAM products and services. In this context where there is a plentiful of constraints, especially cost-based, the engineering of security solutions shall be addressed at the root of the design, based on a risk analysis

approach. Hence, to ensure efficiency, in the CAM ecosystem, interoperability, security and privacy shall be implemented by design and by default. This will enable better flexibility and usability of the security solutions that will be adapted to their environment by better coping with functional and technical constraints. These solutions shall be part of a global security model, be based on a layered approach combining different security solutions guaranteeing the security properties of the assets, depending on the trust level required (e.g. segmentation of systems with functions impacting safety, segmentation of physical and digital environment). For each layer defined and for all relevant parts of the CAM ecosystem, principles of security-by-design, interoperability-by-design, privacy-by-design and by-default should be applied, based on the supporting justification and implementation constraints. ENISA published guidelines for good practices for security of smart cars and cybersecurity and resilience of smart cars[4], which is an additional relevant document to consult. The use of suitable certification schemes is also recommended, in order to establish mutual trust and to demonstrate the state-of-the-art.

Given the scalability of the CAM ecosystem and its quick technological evolution, the threat landscape is constantly evolving and requires keeping the cybersecurity response up-to-date by performing continuous threat intelligence and a watch on the security best practices. In a context where the assets to secure are owned by customers and remote to the operating organisation, the ability to provide update/maintenance and incident response capability over the air will be crucial for a cybersecurity coverage over the full CAM products and services lifecycles. Threat modelling should be used to discover relevant threat scenarios as well as related trust boundaries for which appropriate security measures should be devised.

In terms of applying measures to ensure CAM security and mitigate technical constraints, ENISA recommends:

- Define a security model for CAM products and services based on a methodological risk assessment.
- Ensure commitment to use of standard and/or common components
- Ensure proper implementation of relevant security measures following risk assessment and ensure the risk assessment is kept current for CAM products and services over their lifecycles.
- Implement common rules for all stakeholders, including a risk assessment method, design principles, a set of security measures and information security policy, all of which ensure that there is harmonisation, trust and clear roles and duties in the CAM ecosystem.
- Apply principles of security-by-design by default for all CAM components, devices, services, protocols, communications and processes.
- Perform validation tests and penetration tests to ensure that the security objectives are met for CAM products and services according to the risk assessment.
- Assess the maturity of implemented cybersecurity solutions periodically and collaborate with pairs and partners on cybersecurity state-of-the-art for CAM product and services.
- Implement an overall cybersecurity incident response structure to deal with and monitor the ongoing and emerging threat landscape.
- Establish a continual and secured updatability and upgradability of CAM products and services as a central security mechanism in their lifecycles.
- Ensure the compatibility of security measures taken by OEMs and ISPs developing software functionality that may be added retro-actively, after the vehicle enters into service.
- Enable ability to perform incident response using failsafe mechanisms for CAM products and services with failsafe as guiding principle.

[4] See more at: https://www.enisa.europa.eu/publications/smart-cars

- Keep track of developments in cybersecurity standards and best practices for the CAM ecosystem.
- Use suitable certification schemes in order to establish mutual trust and to demonstrate the state-of-the-art.
- Update the threat models regularly when new threats are discovered.

The recommendations are targeted at:

- Automotive Aftermarket Operators
- Operators of Intelligent Transport Systems (OITS)
- Original Equipment Manufacturers (OEMs)
- System Integrators
- System Providers
- Tier 1 and Tier 2 Suppliers

2.5 FRAGMENTED REGULATORY ENVIRONMENT

In the context of innovation and rapid development of CAM technologies, one of the key challenges in the CAM sector is the number of standards and regulations to comply with. Standardisation and regulatory environments are evolving internationally, generating new requirements for the industry regarding connectivity and autonomous capabilities. Regulators rely on these standards to provide more precision on the intended way to comply with their regulations. In Europe, regulations tend to be harmonised for the Member States, but some specific regulations exist per country. For example in Germany, large cities have to get their information security management system (ISMS) audited every two years by the National IT Security Agency (BSI).[5]

With regard to UNECE (the main regulatory body impacting the automotive and mobility sector), its requirements bind almost all countries in the world, nevertheless, type approval mechanisms differ around the world. UNECE regulations, in addition to various other regulations (e.g. privacy, telecommunication), make it difficult for OEMs and suppliers to streamline their security actions and deploy a single strategy across their entire product and service range. The lack of streamlined regulations at the global level leads to a situation where an organisation is subject to different schemes for a same product range.

The current landscape of standards related to CAM cybersecurity is quite broad, since traditional aspects of security are followed such as risk management, vulnerability management, threat analysis, detection and reaction (e.g. ISO27035[6]), but also specific aspects of CAM industry processes with regulations and standards for type approval of vehicles (e.g. ISO/SAE 21434[7], ISO26262[8], SAEJ3061[9], ISO21177[10], ISO21184[11] and ISO21185[12]) also standards for intelligent transport systems communications (e.g. ETSI TC ITS[13] and IEEE802.11bd[14]) as well as common criteria (ISO/IEC 15408[15]). Some of the recommendations provided by these

[5] See more at: https://www.bsi.bund.de/EN/Home/home_node.html
[6] See more at: https://iso27001security.com/html/27035.html
[7] See more at: https://www.iso.org/standard/70918.html
[8] See more at: https://www.iso.org/standard/68383.html
[9] See more at: https://www.sae.org/standards/content/j3061/
[10] See more at: https://www.iso.org/standard/70056.html
[11] See more at: https://www.iso.org/standard/70057.html
[12] See more at: https://www.iso.org/standard/70058.html
[13] See more at: https://www.etsi.org/technologies/automotive-intelligent-transport
[14] See more at: https://www.car-2-car.org/documents/publications/ieee-80211bd-5g-nr-v2x/
[15] 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

standards sometimes create overlaps since they can be proposed in two different standards (e.g. between ISO27001[16] and ISO/SAE 21434[17] or between ISO21434 and ISO26262[18]).

In addition, associations, groups (e.g. Auto-Isac[19], OCA[20], EuroRAP[21]) or the European Commission and European agencies, such as ENISA, provide high-level reference documents, as well as baselines, good practices and general guidance for the development of CAM products and systems. Many of these documents are process-oriented or limited to a restricted area (e.g. embedded systems) and are therefore not prescriptive as to the exact technical solution to be used or end-to-end security model. For example, with respect to vulnerability management and penetration testing on embedded systems, no common criteria or methods are proposed to streamline vocabulary and practices in the same way as is done for IT systems with Common Vulnerability Scoring System (CVSS) score[22]. This leads to heterogeneity and a wide variety of methodologies, security systems and solutions being developed and implemented by companies and their suppliers. In addition, this heterogeneity and freedom of implementation results in a lack of necessary information required for other affected stakeholders in the CAM ecosystem to effectively implement their cybersecurity strategies. However, the recently published standards and regulations, and ongoing work within CAM associations, will tend to foster harmonisation within the CAM ecosystem and a better ability to streamline the implementation of various standards.

2.5.1 Recommendations

To harmonise efforts on the regulatory environment and to define responsibilities/requirements for the complete CAM ecosystem, ENISA recommends:

- Ensure a homogeneous, detailed, and stable legal EU environment for CAM cybersecurity to allow all stakeholders to plan long-term, sustainable business strategies including the aspect of security.
- Working across all levels of policy-making (incl. governmental and European) to participate in the development of new, harmonised laws and guidance to provide clarity on national standards and responsibilities, and to reduce barriers to innovation while promoting secure product and service development.
- Conduct analyses on current automotive regulations to examine potential gaps, i.e. whether existing regulations adequately address the CAM ecosystem security requirements.
- Promote multi-stakeholder dialogues between the automotive industry actors to ensure consensus in the development of relevant technical standards and regulations.
- Foster commitment to standardisation activities addressing holistically the automotive industry security, including interoperability, that include relevant actors involved in the post-production phase such as automotive aftermarket operators.
- Conduct analyses on current automotive standards to examine potential gaps, i.e. whether existing standards adequately address the CAM ecosystem security requirements.
- Develop and maintain mapping schemes between standardisation activities (such as the ones by ENISA and UNECE) to explore cross-standard commonalities and synergies.
- Launch funding schemes to support cybersecurity initiatives in the CAM ecosystem, including financial support for cooperative actions such as standardisation activities.
- Consider measures ensuring proper implementation of standards and requirements.

[16] See more at: https://www.iso.org/isoiec-27001-information-security.html
[17] See more at: https://www.iso.org/standard/70918.html
[18] See more at: https://www.iso.org/standard/43464.html
[19] Automotive Information Sharing and Analysis Center. See more at: https://automotiveisac.com/
[20] Open traffic systems City Association. See more at: https://oca-ev.org
[21] European Road Assessment Program. See more at: https://eurorap.org/
[22] See more at: https://www.first.org/cvss/

- Define access rights for automotive aftermarket operators, information requirements and authorisation schemes.
- Define clear requirements on cybersecurity based on standardisation that allows a component to be fitted, thereby fostering interoperability throughout the ecosystem.
- Consider establishing criteria for assessing potential harmonising models.

The recommendations are targeted at:

- National Authorities
- Policy Makers
- Regulatory Bodies
- Road Authorities

2.6 LACK OF EXPERTISE AND SKILLED RESOURCES FOR CAM CYBERSECURITY

The lack of human resources with expertise in cybersecurity on the market is a major obstacle that hinders the adoption of security measures specific to CAM products and solutions. Cybersecurity experts required for the development and management of CAM products and new solutions should have knowledge, in addition to their expertise of IT security in general, in several further areas such as software security, network security, cryptography, embedded systems, and operational technology (OT). Moreover, in the different fields of technical expertise, there are various types of cybersecurity competences necessary to secure CAM products and services. Considering the lifecycle of CAM, cybersecurity profiles will be needed for different types of activities with various degrees of technical expertise for risk management/assessment, project management and reporting, conception of security features, definition of technical requirements and specifications, penetration testing, threat intelligence, incident detection, response, forensic and so on. There is not one kind of cybersecurity expert for CAM, but companies are looking for a good mix of technical and methodological knowledge in order to address all the cybersecurity problematics they have to cope with.

Given the large number of companies looking for these types of expertise, there is strong competition to recruit qualified cybersecurity resources who already have expertise in CAM topics, which makes it difficult for companies to find new talents on the market. The concurrence for hiring or contracting cybersecurity profiles with the skillset adapted to the CAM needs increase the costs, which makes cybersecurity resources expensive. Also, most CAM stakeholders confirmed that it is difficult to find qualified specialists who are familiar with security issues within their companies. In addition, there are too few cybersecurity training and awareness programmes already in place within companies that could lead to the scaling up of other IT or engineering resources on cybersecurity-related topics. Lacking expertise and familiarity with these technologies, employees thus also lack skills that are essential for the secure development and operation of CAM products and solutions. The interviews conducted as part of this study confirmed that there is a high demand and low supply of talent in the area of cybersecurity in the CAM sector. Hence, companies started to train internal resources with a previous experience either in IS/IT, OT or embedded systems to cybersecurity in order to instantiate a cybersecurity knowledge ramp-up and employees' mobility programme in order to compensate the resource shortage on the market.

2.6.1 Recommendations

Security expertise and guidance for the CAM ecosystem is of paramount importance. To address the lack of security talent, it is essential to cultivate such knowledge both within and across organisational boundaries. Persons in charge of security within the industry organisations should invest in state-of-the-art dedicated cybersecurity trainings that cover all necessary aspects specific to IT and CAM convergence. Lastly, trainings and courses at schools and universities have been launched to further promote a better understanding of the

automotive industry security among younger generations and thus, in the long term, will contribute to raising awareness.

To promote cross-functional knowledge on security expertise and guidance, ENISA recommends:

- Encourage cross-functional security and safety knowledge exchange between IT/OT and mobility experts respectively.
- Launch security education and trainings in mobility industries, including knowledge of the state-of-the-art, best practices, methodologies and tools for secure convergence of IT/OT and mobility systems.
- Establish tailor-made training courses focussed on mobility industry security to increase the effectiveness of the trainings and assist mobility and IT/OT security experts to address relevant cybersecurity issues more efficiently.
- Develop competency profiles to provide mobility industry-specific awareness and education training for all staff.
- Introduce programmes at schools and universities to address the lack of security and safety knowledge across the industry and to empower the next generation of IT/OT and mobility security experts.
- Organise cyber-culture and cyber-hygiene introduction courses for personnel and conversely safety-culture and safety-hygiene courses all personnel, especially IT/OT staff. Introduce the notion of security and the notion of safety, with special mentions to cases where the two notions may or may not align.
- Extend the courses to the whole supply chain, or require that all parts of it have cybersecurity training included in their companies.
- Enhance corporate culture to include cybersecurity in job profiles, and to attract and retain security talents/experts.
- Participate in information exchange programs such as Information Sharing and Analysis Centres (ISACs)[23] to further increase information knowledge and exchange of good practices.

The recommendations are targeted at:

- Automotive Aftermarket Operators
- 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
- System Integrators
- System Providers
- Tier 1 and Tier 2 Suppliers

2.7 LACK OF INFORMATION SHARING AND COORDINATION ON SECURITY ISSUES AMONG THE CAM ACTORS

The CAM sector is one of the largest generators of data. For example, a self-driving vehicle is expected to generate and consume 40 terabytes of data every 8 hours of driving, giving a hint of the amount of data that will be generated at the scale of a smart city or road infrastructures.[24] Data is evolving as a key production factor, and large data applications enable stakeholders

[23] See more at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[24] Barua, Suhrid. (n.d.). *Flood of Data Will Get Generated in Autonomous Cars*. Auto Tech Review. Retrieved from: https://autotechreview.com/features/flood-of-data-will-get-generated-in-autonomous-cars

such as car manufacturers, suppliers, automotive aftermarket operators, service providers, transport operators and public authorities to utilise consumers', infrastructures' and vehicles' information to provide modern mobility services. In the consideration that all types of data, let it be from vehicles, free-floating devices or road infrastructures are going to be exchanged and shared among CAM actors, within the boundaries of data protection and privacy regulation like the General Data Protection Regulation (GDPR)[25] and the forthcoming ePrivacy Directive[26], this implies the implementation of cybersecurity measures, protocols and standards to secure the exchange itself. 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 and lasting model. Such models need to be supported with establishing a pan-European authentication and authorisation scheme based on clearly defined roles and responsibilities, to ensure that every CAM stakeholder has the possibility to access the required vehicle data, functions and resources in a safe and secure way.

Considering cybersecurity, one of the current challenges is the lack of visibility and sharing of information within the ecosystem on evolving attacks and threats. Since CAM products and services delivery rely on multiple interactions between different actors, as mentioned earlier, one stakeholder may need to access data or information related to cybersecurity operations of another stakeholder. This could be insightful for its own cybersecurity operations and protection of its perimeter, and vice-versa. This need is particularly noteworthy in the interactions between a company and its supplier where collaboration, information sharing about incidents and discovered vulnerabilities, collective implementation of security measures or shared threat intelligence will be decisive for the efficiency of cyber security operations. However, it is also important to note that the impact of cybersecurity is at the whole vehicle level and at the level of interaction between components and services managed by different actors within the CAM ecosystem. The cohesive interdependent nature of the vehicle, its components and services, require that in addition to incidents and vulnerabilities, additional information regarding cybersecurity compatibility and interoperability be shared among the relevant stakeholders of the CAM ecosystem. Such information sharing is of paramount importance to ensure that components and services implemented within the vehicle architecture by multiple CAM stakeholders are still able to function as required in a safe and secure way.

This challenge is also linked to the problem of interoperability. With the massive development of solutions and to ensure a system of interconnected transport infrastructures, CAM actors should have the possibility to share information about, among others, their new solutions, developments and technologies. CAM actors confirmed that there are many solutions developed in the world that are not interoperable which should be standardised in order to achieve a more global solution in Europe, and to ensure business continuity of all CAM stakeholders in the automotive sector. Where there are interdependencies between products and services developed by multiple CAM stakeholders, in addition to perimeter level cybersecurity considerations, there should be an information sharing mechanism (at European level - supported by legislation) to ensure that these products and services can be developed and integrated with the products in a safe and secure way. Changes or updates to cybersecurity requirements of one CAM stakeholder, that affects the cybersecurity and functioning of the components and services of other CAM stakeholders need to be communicated to all relevant CAM stakeholders.

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). See more at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[26] See more at: https://ec.europa.eu/digital-single-market/en/online-privacy

2.7.1 Recommendations

To ensure information sharing among the stakeholders in the CAM ecosystem, ENISA recommends:

- Consider developing the analysing capabilities within and among the existing and potential forthcoming EU-focussed ISACs.
- Explore and initiate cooperation in an ISAC where it does not already exist. The starting point is smaller groups of stakeholders that grow into establishing cross-connections throughout the remainder of the ecosystem to further enrich the information available.
- Consider exploring cooperation with Computer Security Incident Response Teams (CSIRT) communities, including the European CSIRTs Network[27].
- Consider involving the right stakeholders in the ISACs, including but not limited to EU agencies and bodies, law enforcement agencies, other industry bodies, as well as associations and telecom operators.
- Consider creating interfaces of cooperation with other sectorial actors and EU-wide ISACs to exchange good practices for information sharing, as well as knowledge on attacks and threats that might be relevant for the CAM industry (especially the automotive supply chain).
- Ensure legally that relevant cybersecurity compatibility information (for development and system integration) from relevant CAM stakeholders are be provided to all authorised CAM stakeholders, as required upon request. This information sharing is necessary as the information shared in ISACs only relates to cyber-threats, attacks and good practices for internal development, but does not include cybersecurity-relevant information for producing and replacing parts, and conducting repair and maintenance operations.
- Adapt industry standards or minimum requirements covering cybersecurity information interoperability to ensure all stakeholders are at a minimum level of security.

The recommendations are targeted at:

- Automotive Aftermarket Operators
- Operators of Intelligent Transport Systems (OITS)
- Original Equipment Manufacturers (OEMs)
- Road Equipment Manufacturers
- Smart City Operators
- System Integrators
- System Providers
- Tier 1 and Tier 2 Suppliers,

[27] See more at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

TP0420638ENN

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 978-92-9204-408-4
DOI: 10.2824/748518