【欧州】【自動車】

Road/Railway - Autonomous driving vehicle: ENISA publishes recommendations on securing the connected and automated mobility (CAM) ecosystem

Andrea Antolini Former Researcher JTTRI

【概要：Summary】

The Connected and Automated Mobility (CAM) refers to autonomous or connected vehicles that can guide themselves and operate autonomously without or less human intervention. While the CAM approach has the potential to make the transport system safer, cleaner, more efficient, and more user-friendly, it needs a coordination of tasks and connections at European level to ensure that a vehicle remains connected also when crossing Member States' borders. Therefore, the EU's Cybersecurity Agency ENISA addresses cyber security problems and provides legal measures to improve the overall level of cybersecurity.

To successfully deploying cooperative, connected and automated vehicles in road transport, the European Commission has taken steps to introduce a harmonised package of actions and legislative framework. The Commission created a European strategy for the deployment of cooperative, connected and automated vehicles. It requires a joint effort of all actors involved, also regarding cybersecurity.

The Commission will seek to ensure a leading position of the EU in the field of Connected and Automated Mobility. Regarding the problems and challenges in the CAM's cybersecurity, ENISA has considered some recommendations focusing on CAM's main aspects of cybersecurity related issues. The connected vehicles, connected environment and connected infrastructure should be designed with new capabilities and features to provide increased safety, better vehicle performance, competitive digital products and services, more comfort, environmental friendliness, as well as convenience for its end-users. The CAM ecosystem must cope with key challenges that add complexity to responding and managing CAM cybersecurity risks. Therefore, the ENISA report on recommendations for the security of the connected and automated mobility (CAM) identifies key cybersecurity challenges in the CAM sector and provides recommendations how to solve these problems. It intends to enhance the level of security and resilience of CAM infrastructures and systems in Europe.

【記事：Article】

1. The connected and automated mobility (CAM)

Connected and Automated Mobility (CAM) essentially refers to autonomous or connected vehicles that can share data or operate autonomously, without or less human intervention. This CAM approach is expected to make the transport system safer, cleaner, more efficient, and more user-friendly. The introduction of

digital technologies, such as internet of things, artificial intelligence, high-performance computers, and powerful communication networks, in vehicles are changing the transport environment. Policies and legislation relating to digital technology, including cybersecurity, liability, data use, privacy and radio spectrum/connectivity are of increasing relevance to the transport sector. These digital technologies and their connections need to be introduced and coordinated at European level to ensure that CAM vehicles remain connected also when they are crossing the EU Member States' borders. Furthermore, different stakeholders along the automotive value chain are expected to be affected by the introduction of CAM, from vehicle manufacturers and suppliers to dealers, aftermarket, and mobility services providers. The European Commission supports the introduction and deployment of CAM on various levels with the introduction of legislation, standards and policies, roadmaps, strategies in close collaboration with stakeholders.

In 2016, the Commission presented its communication on "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" COM (2016) 766 final). The Cooperative Intelligent Transport Systems (C-ITS) allows road users and traffic managers to share and use information and in future they will also interact directly with each other and with the road infrastructure. This interaction under the C-ITS will allow road users and traffic managers to share information and use it to coordinate their actions. This cooperative element is expected to significantly improve road safety, traffic efficiency and comfort of driving. Since 2019, C-ITS based on ITS-G5 has also been introduced at large scale in production vehicles.

On 13 March 2019, the Commission adopted a delegated regulation on specifications for the provision of C-ITS, supported by an impact assessment. However, this delegated regulation did not enter into force following an objection by the Council of the European Union.

Furthermore, the European Commission's "Communication on the road to automated mobility: An EU strategy for mobility of the future" (COM (2018) 0283 final) of 17 May 2018 aims to ensure a smooth transition towards a safe, clean, and connected & automated mobility system in the EU. The Commission's Communication proposes rules for self-driving cars under common EU legislation. Regarding Connected and Automated Mobility (CAM), the EU Member States, industry and the European Commission collaborate to achieve the vision for connected and automated mobility across the EU.

The EU Cybersecurity Agency ENISA acts as a centre of expertise to enhancing network and information security in the EU and contributes to the overall goal of ensuring a high level of network and information security.

2. Connected and automated mobility under the Sustainable and Smart Mobility Strategy (COM (2020) 789 final)

Under the impact of the COVID-19 pandemic, the European Commission presented a communication on sustainable and smart mobility for the future on 9 December 2020. (COM (2020) 789 final). Under this sustainable and smart mobility strategy, also the seamless, safe, and efficient connectivity and smart mobility plays an important role. To making the connected and automated multimodal mobility a reality, the EU needs to take full advantage of smart digital solutions and intelligent transport systems (ITS). The connected, cooperative, and automated mobility (CCAM) can provide mobility for all, give back valuable time, and improve road safety. The Commission will drive research and innovation, possibly with a new European partnership on CCAM envisaged under Horizon Europe and through other partnerships focusing on digital technologies.

Such partnerships are important as the EU needs to make sure that efforts are well coordinated. The vision is to make Europe leading in the development and deployment of CCAM systems and to provide a significant contribution to safe and sustainable road transport. The Commission will explore options to further support safe, smart, and sustainable road transport operations under an existing agency or another body, which could support the deployment and management of ITS and sustainable connected and automated mobility across Europe. It could facilitate the preparation of relevant technical rules, regarding the use of automated vehicles cross-border and the deployment of recharging and refuelling infrastructure, under EU legislation and to be adopted by the Commission.

3. ENISA and the security of smart cars

Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity, ENISA, became a permanent EU agency for cybersecurity, based on the European Cybersecurity Act, Regulation (EU) 2019/881 of 27 June 2019. ENISA is dedicated to achieving a high common level of cybersecurity across Europe and it also contributes to the EU's cyber policy, and cooperates with Member States and EU bodies, among others.

Autonomous and connected vehicles are expected to have the potential to change the entire transport sector in the mid- and long term. However, the development of increasingly autonomous and connected vehicles also increases the vulnerability of the autonomous vehicles to cyberthreats, cyberattacks or physical attacks. Therefore, alongside the development of CAM technologies, there will arise new vulnerabilities regarding cyber and physical threats for the highly automated vehicles. Since automotive security is closely connected to safety, the security implications of CAM have also the potential to have a direct negative impact on the safety of passengers, pedestrians, other vehicles, and related infrastructures.

The CAM sector is an entire ecosystem of services, operations and infrastructures comprised of a variety of actors and stakeholders. It has the potential to change the way society views transportation, benefit from digitalisation to connect vehicles with their surroundings and with the drivers. It is expected to contribute to solving congestion, it reduces pollution, and potentially diminishes road accidents, and improves access to mobility.

On 25 November 2019, ENISA published its report entitled "ENISA Good Practices for Security of Smart Cars" regarding cybersecurity and resilience of smart cars. With the increased connectivity that will be driven by the emergence of 5G broadband technology standard, it is expected that new cybersecurity risks and threats will arise, which need to be managed. Building on the existing standardisation, legislation, and policies, ENISA aims at promoting cybersecurity for smart cars including the connected and automated cars.

4. ENISA's recommendations for the CAM related security measures

On 5 May 2021, the ENISA issued a report on recommendations for the security of the connected and automated mobility (CAM). The ENISA contributes to the overall goal of ensuring a high level of network and information security. In its report of 5 May 2021, it identifies the main cybersecurity challenges faced by the CAM sector and provides 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. The report identifies the key cybersecurity challenges for the sector, including governance and cybersecurity integration into corporate activity; the lack of top management support and cybersecurity

prioritisation; technical complexity in the CAM ecosystem; the technical constraints for implementation of security into CAM; fragmented regulatory environment; the lack of expertise and skilled resources for CAM cybersecurity; the lack of information sharing, and the coordination on security issues among the CAM actors.

Regarding governance and cybersecurity integration into corporate activities, ENISA recommends seeing cybersecurity not as a standalone topic in the CAM ecosystem, but as a core enabler that protects safety and provides value to products and services. According to ENISA's report of 5 May 2021, at all stages of CAM product and service lifecycles, risks must be managed, and cybersecurity activities must be performed. ENISA recommends raising awareness to the top management level of the organisation and throughout the organisation, especially at the right decision level, about the impact of cybersecurity and technology on the CAM ecosystem lifecycle. Furthermore, the acceleration of cybersecurity in research and development on CAM technology needs to keep up with cybersecurity developments and should be promoted. The report recommends, among others, to promote the integration of cybersecurity along with digital transformation at an organisation's board level, and to promote procurement processes to integrate cybersecurity and risk-oriented requirements.

In fact, so far, cybersecurity has generally not been considered a priority by corporate management in the CAM industry and has not been perceived as a board-level topic. This lack of management involvement leads also to insufficient financial support to ensure cybersecurity, which needs to be addressed as a key topic in the lifecycle of CAM products and services. Furthermore, due to 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.

In this context, the ENISA report recommends a mind-set shift so that cybersecurity is not seen as a cost and pure loss of money that may avoid potential risks. Instead, it could be seen as a real enabler of important business opportunities made possible by the mastering of technologies. Cybersecurity allows to reduce time to market and provides state-of-the-art products and services to customers that are secure, reliable, and trustworthy.

To introduce a prioritisation of cybersecurity by corporate top management and better funding of cybersecurity, ENISA recommends to establish administrative structures for top-level management to discuss and exchange views with cybersecurity experts, to incentivise innovation and R&D activities for securing IT and CAM environments, components, systems and services, to establish regular training programmes for the different levels of the company, including top management, and to foster a corporate security culture by involving cybersecurity directly in the management board, among others.

Regarding the technical complexity in the CAM ecosystem, 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. The dependencies between stakeholders generates a need for interoperability, which will stem from the cybersecurity model. Due to the increasing technical complexity, which could lead to the introduction of new attack vectors in the CAM ecosystem, ENISA recommends promoting the use of common security measures across components and services to adhere to a minimum level of cybersecurity, to promote the use of suitable certification schemes, to promote security assessment for solutions and standardise the discovery and remediation of vulnerabilities during the product lifetime, among others.

Regarding the technical constraints for implementing of security into CAM, 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. As the CAM sector is very innovation-oriented, the continuous evolution and development of new technologies for CAM assets also involves considering technical constraints for securing the various assets. When emerging technologies such as those in CAM are taken up, security measures and standards do not yet exist to provide best practices and guidelines. Cybersecurity teams often must 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.

However, in the CAM ecosystem 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. ENISA recommends using threat modelling to discover relevant threat scenarios as well as related trust boundaries for which appropriate security measures should be devised. Regarding the application of measures to ensure CAM security and mitigate technical constraints, ENISA recommends defining a security model for CAM products and services based on a methodological risk assessment, to ensure commitment to use of standard and/or common components, to ensure proper implementation of relevant security measures following risk assessment and to ensure the risk assessment is kept current for CAM products and services over their lifecycles, among others.

Regarding the problem of a fragmented regulations for innovation and rapid development of CAM technologies, it is a major challenge to comply with the number of standards and regulations. Standardisation and regulatory environments are evolving internationally, and in Europe, regulations tend to be harmonised for the EU Member States, but there also exist specific regulations at national level. 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. To improve the regulatory environment for the complete CAM ecosystem, ENISA recommends to ensure a homogeneous, detailed, and stable legal EU environment for CAM cybersecurity including the aspect of security, to 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, among others. Furthermore, ENISA recommends, to conduct analyses on current automotive regulations to examine potential gaps, and whether existing regulations adequately address the CAM ecosystem security requirements. ENISA recommends also to launch funding schemes to support cybersecurity initiatives in the CAM ecosystem, including financial support for cooperative actions such as standardisation activities, among others.

Regarding the lack of human resources with expertise in CAM cybersecurity on the market is seen as a major obstacle that hinders the adoption of security measures specific to CAM products and solutions. There is strong competition to recruit qualified cybersecurity resources who already have expertise in CAM topics. ENISA recommends that persons in charge of security within the industry organisations should invest in state-of-the-art dedicated cybersecurity trainings that cover all necessary aspects of the CAM environment. ENISA also recommends that cross-functional security and safety knowledge exchange between IT/OT and mobility experts should be encouraged. Security education and trainings in

mobility industries should be launched, and corporate culture should be enhanced to include cybersecurity in job profiles, and to attract and retain security talents/experts, among others.

There also exist a lack of information sharing and coordination on security issues among the CAM actors. Data is evolving as a key production factor, and large data applications enable stakeholders to utilise information on consumers and infrastructure to provide modern mobility services. Considering cybersecurity, one of the current challenges is the lack of visibility and sharing of information on evolving attacks and threats within the CAM ecosystem. To improve information sharing among the stakeholders in the CAM ecosystem, ENISA recommends to consider developing the analysing capabilities within and among the existing and potential forthcoming EU-focussed Information Sharing and Analysis Centres (ISACs), to explore and initiate cooperation in an ISAC, to explore cooperation with Computer Security Incident Response Teams (CSIRT) communities, to consider creating interfaces of cooperation with other sectorial actors and the EU-wide ISACs to exchange good practices as well as knowledge on attacks and threats that might be relevant for the CAM industry especially in the automotive supply chain, among others.

5. Conclusion

The CAM ecosystem is quite heterogeneous regarding the diversity of actors involved and shows also the great diversity of cybersecurity risks and threats. Furthermore, for organisations in the CAM ecosystem, there also apply different types of regulations regarding cybersecurity of the CAM ecosystem, depending on the international, EU-wide, or national requirements.

The ENISA report of 5 May 2021, on recommendations for the security of the connected and automated mobility (CAM) gives a wide overview on CAM related security threats, including the lack of top management support and cybersecurity prioritisation; the technical constraints for implementation of security into CAM; fragmented regulatory environment; as well as the lack of expertise and skilled human resources for CAM cybersecurity, among others.

The ENISA report gives some approaches to solve these cybersecurity challenges. A future CAM system will need to rely on suitable and robust security mechanisms and the ENISA recommendations intend to guide all CAM stakeholders in the context of growing cybersecurity threats and concerns to improve and harmonise the cybersecurity in the CAM ecosystem in the EU.

References:

ENISA: Cyber Security and Resilience of smart cars. In: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars, December 2016, retrieved 5 March 2021

ENISA: Recommendations for the security of CAM. Recommendations for the Security of Connected and Automated Mobility. In: https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam/, 5 May 2021, retrieved 12 May 2021

ENISA good practices For Security of Smart Cars. In: https://www.enisa.europa.eu/publications/smart-cars, 25 November 2019, retrieved 5 March 2021

ENISA: How to secure the Connected & Automated Mobility (CAM) Ecosystem. In: https://www.enisa.europa.eu/news/enisa-news/how-to-secure-the-connected-automated-mobility-cam-ecosystem, retrieved 12 May 2021

European Commission: An EU strategy on cooperative, connected and automated mobility. In: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_3933, 30 November 2016, retrieved 12 May 2021

European Commission: COMMISSION STAFF WORKING DOCUMENT Towards clean, competitive, and

connected mobility: the contribution of Transport Research and Innovation to the Mobility package. In: https://ec.europa.eu/transport/sites/transport/files/swd20170223-transportresearchandinnovationtomobilitypackage.pdf, SWD(2017) 223 final, 31.5.2017, retrieved 11 May 2021

European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected, and automated mobility. COM(2016) 766 final). In: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766&from=EN, 30.11.2016, retrieved 11 May 2021

European Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Sustainable and Smart Mobility Strategy - putting European transport on track for the future. (COM(2020) 789 final). In: https://ec.europa.eu/transport/sites/transport/files/legislation/com20200789.pdf, 9.12.2020, retrieved 11 May 2021

European Commission: Connected and automated mobility. In: https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility, 30 April 2021, retrieved 11 May 2021

European Commission: Intelligent transport systems. Commission presents a Strategy towards cooperative, connected, and automated mobility. In: https://ec.europa.eu/transport/themes/its/news/2016-11-30-c-its-strategy_en, 30/11/2016, retrieved 11 May 2021

European Commission: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. In: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391, 16 December 2020, retrieved 12 May 2021