【欧州】【自動車】

Road/Railway - Autonomous driving vehicles: JRC and ENISA report on artificial intelligence (AI) cybersecurity challenges in autonomous vehicles

Andrea Antolini Former Researcher JTTRI

【概要：Summary】

Artificial intelligence (AI) is playing an increasingly important role in the development of new generations of autonomous vehicles. AI is utilised for improving security and safety in driving autonomous vehicles of level 4 and level 5 autonomation. However, the development of increasingly autonomous and connected vehicles requires a higher level of connectivity, which increases the vulnerability of the autonomous vehicles to cyberattacks or physical attacks. Since automotive security is closely connected to safety, the security implications of AI can potentially have a direct impact on the safety of passengers, pedestrians, other vehicles and related infrastructures.

Therefore, the ENISA/JRC report aims at explaining the cybersecurity challenges for AI techniques in autonomous vehicles. One of the main findings and recommendations is that the automobile manufacturers should increase their preparedness for incident response and improve their capabilities to handle emerging cybersecurity issues connected to AI. The automotive industry should introduce a "security by design" approach for the development and deployment of AI functionalities. AI security policies and a proper AI security culture should govern the entire supply chain of the automotive industry and the entire lifecycle of AI related functions in the autonomous vehicles of level 4 and level 5 autonomation.

【記事：Article】

1. The background of autonomous vehicles

Self-driving, autonomous vehicles are expected to have the potential to change the entire transport sector in the mid- and long-term. The Society of Automotive Engineers SAE determines the intelligence level and automation capabilities of vehicles, ranking from Level 0 to Level 5, from fully manual vehicles (level 0) to level 5 on which human driving is completely eliminated. Level 5 vehicles are the only class of automated vehicles that do not have manual driving control devices such as steering wheels, and gas and brake pedals anymore. The autonomous vehicles of level 5 of automation are expected to be commercially available and introduced by 2030. Leading automobile manufacturing companies but also IT companies are developing and testing high level autonomous vehicles. Several IT Companies are leading the development of software and communication technologies as well as artificial intelligence (AI) digital technologies for autonomous vehicles. A key enabler towards

establishing fully autonomous vehicles are the recent advances in AI, and in particular in Machine Learning (ML). Currently, fully autonomous driving solutions are being mostly experimental prototypes. However, level 3 automated vehicles are already on the roads. Driving assistance functionalities relying on AI and ML include braking assistance, smart parking, or vocal interactions with the infotainment system. AI and its subfield of Machine Learning (ML) are the core enabling technologies of such functionalities. The ultimate objective will be to reach the vehicle automation level 5 of fully autonomous driving. Since fully autonomous or driverless cars are connected to the Internet to function properly, this connection also highly increases their vulnerability against cyberthreats and cyberattacks. Therefore, alongside the development of these new technologies there will arise new vulnerabilities regarding cyber and physical threats for the highly automated vehicles.

2. Autonomous vehicles and the EU's cyber security plans

Since the challenges for security of the Internet of things (IoT) and the digitally connected devices including autonomous vehicles are increasing, resilience against cyber threats and cyberattacks need to be increased. In case of autonomous cars, there are concerns regarding cybersecurity, data security, and their impact on infrastructure. Cyberattacks targeting smart cars including connected and automated vehicles could lead to a vehicle's immobilisation, road accidents and endanger road users' safety among others. Therefore, the EU has started to introduce the necessary regulations regarding autonomous vehicles' safety, liability, cyber security, data security and privacy.

In 2016, the European Commission adopted "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" (COM/2016/0766 final, 2016). The objective of this Cooperative Intelligent Transport Systems (C-ITS) Strategy is to facilitate the convergence of EU investments and regulatory frameworks in order to see deployment of mature C-ITS services in 2019 and beyond. The Network and Information Security directive (NIS) Directive (EU) 2016/1148 of 6 July 2016 is related to measures for a high common level of security of network and information systems across the EU. This NIS Directive puts in place a key role to the European Union Agency for Network and Information Security (ENISA) in supporting the implementation the Directive and also addresses the autonomous vehicles' cybersecurity issues as it intends to provide generic security measures in order to enhance cybersecurity across EU. In September 2017, the European Commission presented a proposal on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM (2017) 477 final). The ENISA as the EU's agency for cybersecurity with its cyber security expertise acts as a centre of expertise to enhancing network and information security in the EU. It contributes to the overall goal of ensuring a high level of network and information security. It addresses and responds to network and information security problems and provides legal measures to boost the overall level of cybersecurity in the EU.

The Communication on Cyber Resilience (COM (2016) 410 final) aims at mitigating the cyber security threats at different levels and promotes cybersecurity for connected and semi-automated cars. It defines good practices for those vehicles and targets security measures to mitigate those threats.

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 intended to establish rules for self-driving cars under common EU legislation.

3. ENISA studies on vehicles' cyber security and recent Commission proposals to improve cybersecurity

On 27 June 2019, the European Cybersecurity Act, Regulation (EU) 2019/881, on ENISA and on information and communications technology cybersecurity certification became effective. It upgrades ENISA into a permanent EU agency for cybersecurity and strengthens ENISA's ability to help EU Member States to address cybersecurity threats. With the emergence of semi-autonomous and autonomous cars, which make use of advanced machine learning and artificial intelligence techniques, the potential risks and cybersecurity will increase. On 25 November 2019, ENISA published its study entitled "ENISA Good Practices for Security of Smart Cars" regarding cybersecurity and resilience of smart cars. It intends to identify the relevant assets and the rising concerns related to cyber threats and smart cars. With the increased connectivity that will be driven by the emergence of 5G broadbandb technology standard, it is expected that new cybersecurity risks and threats will arise, which need to be managed. The ENISA study defines good practices for security of smart cars, including connected and (semi-) autonomous vehicles and identifies the smart cars' sensitive assets, as well as the potential and main cyber threats, risks and attack scenarios for smart cars.

On 16 December 2020, the European Commission adopted a package of several proposals and a new Strategy on Cybersecurity with the aim of strengthening the EU's strategic autonomy to improve its resilience and collective response and to build an open and global internet. The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) presented on 16 December 2020 aims at improving the resilience against cyberattacks in transport, energy and health, telecommunications, and other sectors, which are reliant on interconnected network and information systems. The new Cybersecurity Strategy aims at improving the resilience against cyber threats and ensures that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The package also contains a proposal for a directive on the resilience of critical operators of essential services, which aims to mitigate physical threats against such operators (COM(2020) 829 final).

The Commission proposed also to reform the rules on the security of network and information systems, under a Directive on measures for high common level of cybersecurity across the EU.

The proposal for a planned revision of NIS Directive or "NIS 2 Directive" (COM(2020) 823 final), is the Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final). It modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape. The "NIS 2 Directive" (COM(2020) 823 final) is intended to increase the level of cyber resilience of critical public and private sectors, including energy grids, railways, but also data centres, public administrations, as well as other critical infrastructure and services.

4. AI security in autonomous driving

The introduction of AI technology brings further cybersecurity risks for autonomous vehicles, which could compromise their proper functioning, and which could potentially lead to serious impacts on the safety of passengers and other road users. The latest report, jointly published by ENISA and JRC on 11 February 2021, entitled "Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving",

by the authors Dede, G., Hamon, R., Junklewitz, H. et. al. points out the cyber-security challenges, connected to AI and its vulnerabilities in vehicles with autonomous driving technology, focusing on semi-autonomous (level 4 of automation) and autonomous cars (level 5 of automation).

Unintentional threats come as side effects of the introduction of AI and ML methods in autonomous vehicles and comprise unpredictable malfunctioning and failures caused by shortcomings, poor design and/or inner peculiarities of AI and ML. AI components do not obey the same rules as traditional software, ML techniques are indeed relying on implicit rules that are grounded on the statistical analysis of large collections of data. Furthermore, there are concerns that the machine learning (ML) techniques at the core of the AI components are highly vulnerable to a wide range of intentional cyberattacks that could compromise the proper functioning of autonomous vehicles. The report's objective is to raise awareness about the potential risks connected to AI and provides recommendations to improve AI security in autonomous vehicles and mitigate potential threats and risks. Securing such systems requires to consider these AI specific issues on top of the traditional cybersecurity risks connected to digital systems, and in the context of the full supply chain involved in their development and of their integration with other automotive systems.

The report focuses specifically on adversarial machine learning that regroups a set of techniques that are currently susceptible to compromise AI components in autonomous vehicles. They potentially allow a malicious actor to design specific attacks in AI systems while staying undetectable by human supervisors. One simple example is the adding of paint on the road to misguide the navigation, or stickers on a stop sign to prevent its recognition. However, there are also more complex kinds of attacks, which are less tracable and which could have severe safety consequences. Malicious actors could exploit the high complexity of AI systems to their own advantage. Therefore, the automobile manufacturers should implement defence mechanisms to mitigate these type of AI risks and consider these AI specific issues on top of the traditional cybersecurity risks connected to digital systems.

5. Challenges and recommendations to improve AI security in autonomous vehicles

In the jointly published ENISA/JRC report, the authors Dede, G., Hamon, R., Junklewitz, H. et. al. analyse a set of challenges and provide recommendations to improve AI security in autonomous vehicles in order to mitigate potential threats and risks. In the light of the connections between AI and autonomous vehicles, the report analyses the systematic security validation of AI models and data, AI supply chain security in the automotive industry, cybersecurity processes and controls of AI techniques in autonomous driving, incident handling and vulnerability discovery related to AI and lessons learned, They also point out the limited capacity and expertise on AI cybersecurity in the automotive industry and how to increase capacity and expertise on AI cybersecurity for automotive systems.

Firstly, the data and AI models play an important role in the implementation of autonomous capabilities in autonomous vehicles. These components are dynamic in nature and can change their behaviour overtime as they learn from new data, are updated by manufacturers, or encounter unexpected or intentionally manipulated data. The authors point out that in this context it is important that security and robustness assessments of AI components are systematically performed through-out their lifecycle. The systematic validation of AI models and data is essential to ensure the right behaviour of the autonomous vehicles. This implies developing and

maintaining strict systematic and continuous process of security validation of AI models and data in order to make sure that data used at the development and production stages have not been altered with a malicious intent, and that they do not contain vulnerabilities, which could be exploited. Therefore, also the links between industrial actors and research centres have to be reinforced to address the challenges associated with the implementation of this systematic validation. The security and robustness assessments of AI components need to be systematically performed through-out their lifecycle. Therefore, the report recommends to establishing proactive or reactive monitoring and maintenance processes for the AI models.

Audit processes need to be established to support forensic analysis after incidents, among others, in order to learn lessons for the future. It is also recommended to introduce additional validation check points to limit the impact of erroneous data.

Secondly, regarding the AI software and hardware supply chain, security is of paramount importance, also due to the increased uptake of AI technologies with the addition of complex and opaque ML algorithms. The large and complex dependencies of hardware and software supply chains in the automotive sector add to this complexity. The absence of proper security policies and sufficient strategies across the supply chain of AI components results in a lack of resilience and the presence of potential security breaches in systems. Therefore, the proper governance of security policy across the supply chain requires the involvement of many stakeholders including developers, manufacturers, vendors, aftermarket support, end users, and others. The recommendation regarding the supply chain includes the establishment of a proper AI security policy and security culture should be developed across the supply chain and to ensure its governance. Furthermore, potential risks and threats related to AI in autonomous driving should be identified and monitored.

Thirdly, the uptake of artificial intelligence in autonomous driving is challenging regarding cybersecurity processes and controls of AI techniques. Cyberattacks against autonomous vehicles do not only concern the particularities related to AI, but also include the security of the underlying digital infrastructure and related digital systems. Regarding the increased uptake of AI technologies and digitalization in the context of autonomous driving, the automotive industry needs to introduce a security by design approach for the development and an end-to-end holistic approach for integrating AI cybersecurity with traditional cybersecurity principles for the deployment of AI functionalities. Integrating AI cybersecurity, for all the steps of the AI lifecycle, with traditional security principles is very important, since a vulnerability may jeopardize the security of the whole autonomous vehicle. The report recommends to establishing security processes in the organizations integrating AI particularities, to promote security by design principles when it comes with deployment and development of AI in automotive context. Further recommendations include to ensure proper governance of AI cybersecurity policy in the organizations defining specific roles and responsibilities.

Fourthly, the current cybersecurity connected to the uptake of AI in autonomous vehicles of level 4 and 5 is limited to theoretical analysis and experimental use case studies carried out in laboratories and controlled environments. However, the expected increase in the deployment of these higher levels of automation in road vehicles could quickly change this picture. Accordingly, the level of preparedness and incident response capabilities need to be increased in order to handle emerging cybersecurity issues connected to AI. This includes the establishment of cybersecurity incident handling and response

plans based on standards. The absence of AI security awareness and an inadequate AI security training also have a negative impact on the security of autonomous vehicles. Therefore, it is essential to apply real-world training in order to deal with the negative AI security impacts of optimistic bias. An AI incident could be considered as an incident in which the behaviour of the vehicle as dictated by the planning module of the autonomous vehicles system is susceptible due to an intentional malicious attack or due to the failure of an element in the ML. A plan of action that immediately acts following an AI security breach or failure is essential in order to reduce the incident costs and damages. The report by Dede, G., Hamon, R., Junklewitz, H. et. al. recommends that regarding the incident handling and vulnerability discovery related to AI, an incident response plan should be adapted that includes AI particularities and that establishes a learning culture from AI security incidents. It should also promote knowledge sharing and the use of mandatory standards for AI security incidents reporting. Disaster drills should be organised, involving high management, so that they understand the potential impact in case a vulnerability is discovered.

Fifthly, there exists a limited capacity and expertise on AI cybersecurity in the automotive industry, including a lack of sufficient security knowledge and expertise among developers and system designers. The proper application of the security by design principle requires that all actors involved in the lifecycle of the product are sufficiently proficient on cybersecurity and work systematically together towards the common goal of building a secure product.

AI cybersecurity cannot just be an afterthought, as cybersecurity in the automotive sector is a multidisciplinary task. Companies may also lack the resources to offer AI security training and most people are not trained, either properly or not at all, to be able to recognize the security implications of AI software requirements. Regarding the limited capacity and expertise on AI cybersecurity in the automotive industry, the report recommends to integrating AI cybersecurity particularities in the whole organization policy and to create diverse teams consisted of experts from ML-related fields, cybersecurity and the automotive sector. Security training focused on AI systems cybersecurity should be launched, integrating them across the automotive ecosystem. Automated testing of each security request needs to be allowed to improving response and remediating vulnerabilities as they appear.

6. Conclusion

By increasing the level of autonomy of vehicles and introducing AI and ML functions, the problem of unintentional malfunction problems or intentional cyberthreats and attacks on autonomous vehicles can be expected to increase significantly. Considering the introduction of autonomous vehicles with level 4 or 5 of autonomy by 2030 including AI functions, the ENISA/JRC report recommends the automotive industry to improve its level of preparedness and incident response capabilities to handle emerging cybersecurity issues connected to AI. The automobile manufacturers should increase their preparedness for incident response and implement defence mechanisms to improve their capabilities to handle emerging cybersecurity issues connected to AI. The automotive industry should introduce a “security by design” approach for the development and deployment of AI functionalities, where cybersecurity becomes the central element of the entire supply chain for autonomous vehicles and the entire lifecycle of AI and ML related functions in the autonomous vehicles.

References

Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A. and Sanchez, I., Cybersecurity challenges in the uptake of artificial intelligence

in autonomous driving, EUR 30568 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-28646-2, doi:10.2760/551271, JRC122440. In: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving, retrieved 5 March 2021

ENISA: CYBERSECURITY CHALLENGES IN THE UPTAKE OF ARTIFICIAL INTELLIGENCE IN AUTONOMOUS DRIVING. In: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122440/jrc122440_enisa_jrc_final.pdf, retrieved 5 March 2021

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

ENISA: Press Release: Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. A report by the European Union Agency for Cybersecurity (ENISA) and the Joint Research Centre (JRC) looks at cybersecurity risks connected to Artificial Intelligence (AI) in autonomous vehicles and provides recommendations for mitigating them. Published on February 11, 2021. In: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving, retrieved 5 March 2021

ENISA puts Cybersecurity in the driver's seat. In: https://www.enisa.europa.eu/news/enisa-news/enisa-puts-cybersecurity-in-the-drivers-seat, November 25, 2019, retrieved 12 March 2021

European Commission: REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). In: Official Journal of the European Union, L 151/15, 7.6.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

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 March 2021

European Commission: Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final. In: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166, and https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union, 16 December 2020, retrieved 5 March 2021