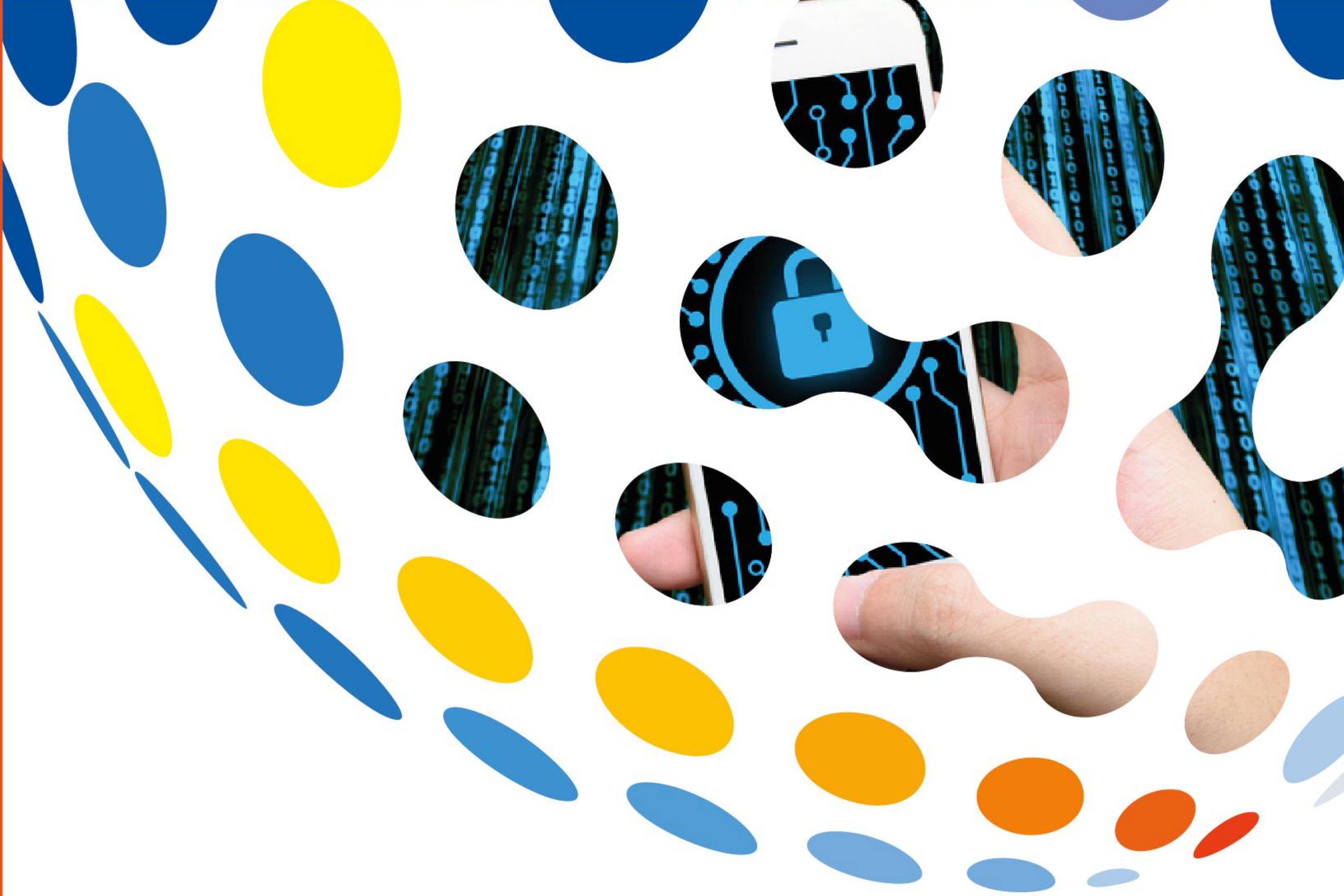

EU Coordinated Risk Assessment

Connected and Automated Vehicles

30 January 2026

NIS COOPERATION GROUP

Executive summary

This is a coordinated Union level security risk assessment of connected and automated vehicles (CAVs) and their supply chains carried out under Article 22 of the NIS2 Directive by the Network and Information Systems (NIS) Cooperation Group in cooperation with the European Commission and ENISA. The primary objective of this report is to provide a comprehensive overview of the cybersecurity risks and their consequences, as mitigating measures which are considered necessary to efficiently address them.

As digitalisation and connectivity spread through the automotive sector, CAVs are increasingly being used in the EU. CAVs offer numerous potential benefits, including improved road safety by reducing human error and their contribution to environmental sustainability through more efficient driving patterns and reduced emissions.

However, CAVs also come with new and significant cybersecurity risks. CAVs process troves of personal and sensitive data, making them potential targets or vectors for surveillance and espionage and in possibly allowing even for their weaponisation.

Member States, the Commission and ENISA identified and assessed 107 risks associated with CAVs, of which 14 are identified as top risks. The assessment expounds on each risk, reviewing related incidents, existing scientific literature and existing measures in place for each of the top-ranking risks.

The assessment identifies vehicle control systems and processing and decision-making systems are particularly critical asset groups. Attacks on these asset groups are linked to severe consequences, including loss of life and significant material damage. Communication and connectivity systems, as well as cloud and backend systems, are also identified as critical asset groups as they constitute typical vectors of attack, in large part due to their public-facing interfaces. Additionally, these systems contain troves of sensitive data which require stringent protection against loss. Furthermore, experts identified the lack of cybersecurity in charging infrastructure as an additional concern.

The assessment has found that, while many of the top risks identified are addressed by the EU's current type-approval rules, they are not able to cover all risks. Existing

research and recorded incidents clearly show that CAVs can be hacked through various pathways. Such hacks have also been shown to have potentially severe consequences, including the full remote takeovers of vehicles or the leaking large amounts of highly sensitive data.

Moreover, the assessment identifies a series of top risks pertaining to high-risk suppliers subjected to, e.g., government or military pressure to implement hidden and malicious hard- or software, updates or configurations in their products or changing the functioning of in-vehicle automated driving systems. A supplier can leverage both known and hidden direct access pathways to the vehicle as an attack vector, thereby effectively bypassing many of the controls mandated by the type-approval regulation. Moreover, such attackers can leverage normal over-the-air updates, another top risk scenario identified to prevent immediate detection. The type-approval regime was mainly created to ensure traffic safety and does not sufficiently mitigate against such risks.

To this end, the Cooperation Group recommends that, amongst other cybersecurity enhancing measures, the Commission, together with the Member States, identifies proportionate measures to de-risk EU supply chains from high-risk suppliers, especially where it pertains to processing and decision-making systems, communication and connectivity systems and vehicle control systems that can receive remote updates. Moreover, the Cooperation Group recommends that Member States have national policies and/or regulations in place in order to take decisions to restrict or exclude high-risk suppliers from supply chains identified as critical.

Additionally, the report suggests follow-up research to assess the impact of cyberattacks on charging infrastructure on the wider energy grid.

Disclaimer

The document is legally of non-binding nature. It is only of advisory character and therefore cannot alter the application of cybersecurity measures applicable in Member States. References to terms such as ‘critical supplier’ or ‘high-risk supplier’ should be understood as working concepts for the purpose of creating a common framework. Those are without prejudice to national laws implementing the NIS 2 Directive or sector-specific EU legislation, such as the Digital Operational Resilience Act (DORA).

Table of Contents

1 INTRODUCTION 5

1.1 EU CAV MARKET 6

1.2 RELEVANT POLICIES AND LEGISLATIVE FRAMEWORKS 7

1.2.1 International regulations and standards 8

1.2.2 European Union regulatory context and framework 9

1.3 SCOPE AND OBJECTIVE 14

2 RISK ASSESSMENT 17

2.1 RISKS INVOLVING PROCESSING AND DECISION-MAKING SYSTEMS 17

2.2 RISKS INVOLVING VEHICLE CONTROL SYSTEMS 19

2.3 RISKS INVOLVING COMMUNICATION AND CONNECTIVITY SYSTEMS 21

2.4 RISKS INVOLVING SENSING SYSTEMS 23

2.5 RISKS INVOLVING CHARGING INFRASTRUCTURE 25

2.6 RISKS INVOLVING CLOUD AND BACKEND SYSTEMS 27

2.7 RISKS INVOLVING HIGH-RISK SUPPLIERS 29

3 CONCLUSIONS 34

4 RECOMMENDATIONS 36

1 Introduction

As digitalisation and connectivity spreads through the automotive sector, connected and automated vehicles (CAVs) are increasingly being used in the European Union (EU). CAV technologies may offer tremendous benefits, including improved road safety by reducing human error, which is major cause of road accidents, and optimising traffic flows by enabling vehicles to communicate with each other and the infrastructures around them. Additionally, they can contribute to environmental sustainability through more efficient driving patterns and reduced emissions, making CAVs an important technology in achieving the EU's transition to climate neutrality by 2050.

However, the increasingly connected nature of CAVs also comes with new risks. CAVs utilise a variety of communication channels to interact with cloud services, other vehicles and infrastructure around them. Moreover, critical CAV functions, such as (automated) driving, are increasingly connected to other systems to enable remote control and monitoring for user convenience. Combined, each of these channels presents an attack surface that cyber attackers can exploit to gain unauthorised access to the vehicle's critical systems.

The cybersecurity of CAVs is critical to the whole of the EU for a number of reasons. First, the compromise of any of a CAV's control systems can have catastrophic consequences, including accidents leading to loss of life and significant material damage. Second, theft or manipulation of personal or otherwise sensitive data, such as location information, user preferences or external data on restricted areas poses serious privacy and security concerns. Third, cyberattacks on CAVs can undermine trust in the technology and hinder further adoption of CAV technologies. Fourth, in view of the EU's principle of free movement, these risks present themselves as inherently cross-border and require, therefore, a Union-wide mitigation approach.

This document is structured as follows: section 1 sets up the risk assessment, by providing the context, including a brief overview of the market and relevant policies and legislative frameworks, and defining the scope, objective and method of the assessment; section 2 provides an analysis of the results of the risk assessment, including a review of existing literature and existing measures in place; section 3 sets out the conclusions based on the analysis and section 4 provides a set of recommendations aimed at the European Commission, EU Member States and original equipment manufacturers (OEMs).

As set out in the **Industrial Action Plan for the European automotive sector,** the Commission will follow up on this risk assessment with concrete measures and will explore ways to build up a European industrial value chain for critical components.[1]

1.1 EU CAV Market

The EU automotive industry is of strategic importance to the EU economy. It provides 13.8 million jobs, directly and indirectly, representing 6.1% of total EU employment.[2] The industry accounts for 8% of European manufacturing value added. The EU has 255 automotive factories assembling vehicles and making batteries and engines.[3] It produced 14.8 million vehicles in 2023, including 12.2 million cars. The EU has some of the world's leading carmakers and automotive suppliers and is a net exporter of vehicles.[4] However, the sector's economic relevance varies across EU countries.[5] Its largest relevance can be found in Czechia, Germany, Hungary, Romania, Slovakia and Sweden, where it represents more than 10% of total manufacturing employment. In general, the automotive sector depends on a complex network of cross-border supply chains, including a large number of specialized European SMEs.[6]

The EU is committed to a transition from combustion to battery electric vehicles in the automotive industry, where all new vehicles in the EU should be zero emission by

[1] COM/2025/95 final, Industrial Action Plan for the European automotive sector. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0095

[2] European Commission (2024) *The future of European competitiveness*. https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf

[3] ACEA (2024) *Economic and Market Report Global and EU auto industry: Full year 2023.* https://www.acea.auto/files/Economic_and_Market_Report-Full_year_2023.pdf

[4] BCG (2023) *European Auto Industry Is at a Crossroads.* https://www.bcg.com/publications/2023/european-auto-industry-is-under-pressure

[5] European Committee of the Regions (2024) *State of play and future challenges of automotive regions*. https://panteia.com/files/state-of-play-and-future-challenges-of-automotive-regions-pdf/

[6] European Commission (2024) *Reshaping the Road Ahead: Exploring Supply Chain Transformations in the EU Automobile Industry.* https://single-market-economy.ec.europa.eu/document/download/5bf3adb5-809d-4012-9242-b6797cc0e412_en?filename=EconomicBrief_5_ETBD_23_005_ENN_TheRoadAhead_ConnellAndGarroneV2.pdf

2035.[7] This has led to a surge in the sale of electric vehicles in the EU, with the share of battery electric vehicles in the EU almost tripling between 2020 and 2023.[8] In tandem with the growing electrification, vehicles are increasingly connected and automated. To illustrate, the widespread adoption of electrified vehicle control and autonomous driving has doubled the number of lines of software code per vehicle, from 100 million lines of code to 200 million, over the period 2015-2020.[9]

The transition to electricity and connectivity also brings changes in the industry's market structure. New companies from the battery and tech sectors have entered the market.[10] Recently, China, Turkey and the UK became the biggest vehicle exporters to the EU. Simultaneously, vehicle imports from Japan, Korea and the US have decreased. Especially, imports from China have shown a remarkable growth: China rose from the 8th largest exporter of vehicles, with 170,000 vehicles in 2020, to now being the highest volume exporter to the EU, with € 781 bn worth of motor cars and vehicles, and € 784 bn worth of motor vehicle parts, imported in 2024.[11]

1.2 Relevant policies and legislative frameworks

Over the past years, multiple policy initiatives – at both the international and EU level – have been undertaken to establish security and cybersecurity requirements for CAVs, with the aim of ensuring that the innovation in the automotive sector goes hand in hand with the safety of vehicle occupants and vulnerable road users.

[7] Regulation (EU) 2023/851 of the European Parliament and of the Council of 19 April 2023 on CO_2 emission performance standards for new passenger cars and for new light commercial vehicles, in line with the Union's increased climate ambition, OJ L 111, 26.4.2023, p. 1–60. https://eur-lex.europa.eu/eli/reg/2023/851/oj/eng

[8] European Parliament (2024) *The crisis facing the EU's automotive industry.* https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)762419

[9] Goldman Sachs (2022) *Software is taking over the auto industry.* https://www.goldmansachs.com/insights/articles/software-is-taking-over-the-auto-industry

[10] European Parliament (2024) *The crisis facing the EU's automotive industry.* https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)762419

[11] Eurostat (2025) *China-EU – international trade in goods statistics.* https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics&stable=0#Explore_further

1.2.1 International regulations and standards

Among key relevant regulations adopted at the international level – and to which the European Union adheres – are the United Nations (UN) Regulations No. 155, No. 156 and No. 157.

The **UN Regulation No. 155** sets cybersecurity requirements for manufacturers of certain categories of vehicles – including those with electronic control units or automated driving features – to enhance the latter's protection against cyber threats. More specifically, the Regulation mandates that manufacturers implement and maintain a Cybersecurity Management System (CSMS) to manage risks throughout the vehicle's lifecycle – from development and production to post-deployment – that must remain effective over time and adapt to evolving threats. Security must be integrated into the entire development process, with continuous risk assessments and the implementation of such protective measures as secure coding, encryption and vulnerability monitoring. Manufacturers are additionally required to establish an incident response plan, obtain type approval to demonstrate compliance and manage cybersecurity across their supply chains. The Regulation thus emphasizes a cybersecurity-by-design and continuous monitoring approach for managing cyber risks.[12]

The **UN Regulation No. 156** focuses on software updates and mandates both the implementation and the maintenance of a Software Update Management System (SUMS), which is a systematic approach defining organisational processes and procedures to comply with certain requirements for the delivery of software updates. Automotive manufacturers are required to operate a certified SUMS, subject to periodic assessment and renewal at intervals not exceeding three years. Similarly to UN Regulation No. 155, UN Regulation No. 156 thus also places particular emphasis on the enforcement of security and safety measures throughout the entire automotive software update process.[13]

[12] UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system (UN/ECE R155), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

[13] UN Regulation No. 156 – Uniform provisions concerning the approval of vehicles with regard to software update and software update management system, as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement.

The **UN Regulation No. 157** addresses the type-approval of Automated Lane Keeping Systems (ALKS) and is the first international regulation governing the introduction of so-called 'level 3' systems with a limited use case on motorways, especially traffic jam situations. The Regulation includes several safety requirements, driver monitoring-related provisions of importance when the driver is requested to take back the driving tasks, as well as provisions for Data Storage Systems for Automated Driving, which are black boxes that collect system and driver monitoring data.[14]

By way of illustration, worth mentioning here are also the **ISO/IEC 2700x**[15], the **IEC 62443**[16], the **NIST Cybersecurity Framework (CSF)**[17], the **Cybersecurity Maturity Model Certification (CMMC)**[18], **TISAX / VDA ISA**[19] and **ISO 21434** as they are among the additional international standards on which vehicle safety regulations are based.

1.2.2 European Union regulatory context and framework

Over the past decade, the European Union (EU) and its Member States have also been engaged in regulating the connected and automated vehicles (CAVs) industry. In the 2016 Amsterdam Declaration[20], Member States urged the European Commission to support the transition towards automation in road transportation with an EU strategy. Responding to this call, in 2018, the European Commission published

https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

[14] UN Regulation No. 157 – Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks

[15] ISO (2025) *ISO IEC 27000 family*. https://www.iso.org/standard/iso-iec-27000-family

[16] International Society of Automation (2025) *ISA/IEC 62443 Series of Standards*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[17] NIST (2025) *Cybersecurity Framework*. https://www.nist.gov/cyberframework

[18] CISA (2025) *Cybersecurity Maturity Model Certification 2.0 Program*. https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program

[19] VDA QMC (2025) *TISAX-Assessment with VDA ISA (ID 510)* https://vda-qmc.de/en/education/510-tisax-assessment-mit-vda-isa/

[20] Netherlands Ministry of Infrastructure and the Environment (2016) *Declaration of Amsterdam: Cooperation in the field of connected and automated driving.* https://www.rijksoverheid.nl/documenten/rapporten/2016/04/29/declaration-of-amsterdam-cooperation-in-the-field-of-connected-and-automated-driving

the Communication ‘*On the road to automated mobility: An EU strategy for mobility of the future*’[21] outlining a strategy to position the European Union as a global leader in the CAVs sector. Since then, the related legislative landscape has been developing significantly.

CAV-specific legislation

Vehicle type-approval Regulation

The Regulation (EU) 2018/858 – in effect since 2020 – establishes administrative provisions and technical requirements for the placing on the EU market of vehicles and related systems, components or separate technical units. The Regulation thus lays down the core legal framework for the EU type-approval process of motor vehicles, namely the process applied by national authorities to certify that a model of vehicle, system, component or separate technical unit meets all EU safety, environmental and conformity of production requirements before authorising it to be placed on the EU market. The Regulation incorporates UN standards by making certain United Nations Economic Commission for Europe (UNECE) Regulations – as listed in Annex II and updated via delegated acts – part of the mandatory or equivalent technical requirements for obtaining EU type-approval. More specifically, according to the process defined by the Regulation, manufacturers are required to produce prototypes (including of individual parts and components, such as seats or steering wheel airbags) that will be used to test compliance with all EU requirements (e.g., safety rules, noise and emissions limits). If the latter are met, the national authority delivers an EU vehicle type approval to the manufacturer authorising the sale of the vehicle type in the EU. Such system is based on the mutual recognition of approvals granted by Member States (i.e., certified once, accepted everywhere in the EU).[22]

General Safety Regulation

[21] European Commission (2018) *On the road to automated mobility: An EU strategy for mobility of the future*. https://transport.ec.europa.eu/system/files/2018-10/on_the_road_to_automated_mobility.pdf

[22] Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (the Framework Regulation, which replaced Directive 2007/46/EC).

The Regulation (EU) 2019/2144 (hereafter General Safety Regulation) – in effect since 2022 – defines the EU's safety rules for both light-duty (passenger vehicles and vans) and heavy-duty motor vehicles (buses, coaches and trucks), focusing on the safety of drivers, passengers and vulnerable road users (e.g., pedestrians and cyclists). The Regulation establishes, *inter alia*, specific safety and cybersecurity requirements for 'automated' and 'fully automated vehicles'. As an illustration, based on the EU's 112 emergency call framework, the Regulation requires e-calling to notify emergency services from within the vehicle. Moreover, it introduces mandatory advanced driver assistant systems to improve road safety and establishes the legal framework for the approval of driverless and automated vehicles in the EU. [23]

Automated driving Regulations

The European Commission adopted technical legislation for fully driverless vehicles (level 4 of automation, e.g., urban shuttles or 'robotaxis'), which are the first international rules of their kind.[24] he technical rules, set out via a delegated and implementing act, establish a comprehensive assessment of the safety and maturity of fully automated vehicles before entering the EU market.[25, 26] The rules will cover testing procedures, cybersecurity requirements, data recording rules, as well as safety

[23] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 https://eur-lex.europa.eu/eli/reg/2019/2144/oj/eng

[24] See the relevant delegated act (https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=PI_COM:Ares%282022%292667391) and implementing act (https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=PI_COM:Ares%282022%292077610).

[25] Commission Delegated Regulation (EU) 2022/2236 of 20 June 2022 amending Annexes I, II, IV and V to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the technical requirements for vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update. https://eur-lex.europa.eu/eli/reg_del/2022/2236/oj/eng

[26] Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles. https://eur-lex.europa.eu/eli/reg_impl/2022/1426/oj/eng

performance monitoring and incident reporting requirements for manufacturers of fully driverless vehicles. For CAVs replacing the driver on motorways (level 3 automation), the EU legislation aligns with the UN Regulation No. 157.[27]

Some Member States have also taken steps towards driverless mobility. For example, Germany adopted a law in 2022 allowing autonomous motor vehicles (level 4) to operate in regular public road transport in determined areas.[28] Similarly, Luxembourg developed a cross-border digital test bed for CAVs in 2024, which extends 215 km across three Member States, offering industry and academia the opportunity to test innovative mobility solutions on public roads under a wide range of conditions.[29]

Horizontal legislation

General Data Protection Regulation

The Regulation (EU) 2016/679 – the General Data Protection Regulation (GDPR) – applies to all personal data processing relating to people in the territory of the EU. It prohibits transfer of personal data to third countries unless there are broadly equivalent safeguards.[30]

NIS2 Directive

The Directive (EU) 2022/2555 – NIS 2 Directive – introduced cybersecurity requirements for companies in the EU's critical sectors relevant to CAVs including:

- The manufacturing sector, including the subsector of vehicle manufacturing;

[27] UN Regulation No. 157 – Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks

[28] Federal Ministry for Digital and Transport (2024) Germany will be the world leader in autonomous driving. https://www.bmv.de/SharedDocs/EN/Articles/DG/act-on-autonomous-driving.html

[29] Luxembourgish government (2024) Automotive sector and smart mobility. https://luxembourg.public.lu/en/invest/key-sectors/automobile.html

[30] 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). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

- The transport sector, including the road subsector, specifically the intelligent road infrastructure;
- The telecom sector, including the mobile networks, 5G and satellite communications;
- The energy sector, including the electricity subsector.

The NIS2 Directive includes technical, operational and organisational cybersecurity risk-management measures for entities in these sectors. [31]

Cyber Resilience Act

The Regulation (EU) 2024/2847 – the Cyber Resilience Act (CRA) – establishes horizontal cybersecurity essential requirements on products with digital elements, including components placed on the market separately, as well as vulnerability handling requirements during the time the product is expected to be in use. However, CAVs and other products with digital elements to which Regulation (EU) 2019/2144 applies are excluded from the scope of the CRA, as they are covered by UN R155[32]. Components which are placed separately on the market and are not spare parts do fall within the scope of the CRA. Such components may include various software solutions to be used within the CAV.

EU Artificial Intelligence Act

The EU's Artificial Intelligence Act (AI Act)[33] aims at regulating artificial intelligence technology to ensure safety, transparency, and ethics in its deployment and use. The AI Act includes an amendment of the EU's General Safety Regulation, stating that, where it pertains to artificial intelligence systems which are safety components within the meaning of the AI Act, type-approval must take into account the requirements set out in Chapter III, Section 2, of the AI Act. These requirements include, but are not

[31] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[32] Point (c) of Article 2.2 of the CRA and recital 27.

[33] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

limited to, ensuring high data quality, implementing risk management systems, ensuring operational transparency and human oversight as well as an appropriate level of accuracy, robustness and cybersecurity. Full implementation of the rules concerning AI and vehicle type-approval is scheduled for 2 August 2027. Additionally, the AI Act includes an amendment of the Regulation on the approval and market surveillance of motor vehicles.[34]

1.3 Scope and objective

The present document illustrates key findings from a coordinated Union-level security risk assessment of CAVS, conducted by the NIS Cooperation Group – in collaboration with the European Commission and the European Union Agency for Cybersecurity (ENISA) – pursuant to Article 22 of the NIS 2 Directive.[35]

Article 22 of the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) states that:

1. *The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.*
2. *The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.* [36]

[34] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC. https://eur-lex.europa.eu/eli/reg/2018/858/oj/eng

[35] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[36] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

The risk assessment aims to identify, analyse and prioritise technical and non-technical cybersecurity risks to CAVs and their supply chains and provide a set of recommendations for mitigating the top risks.

More specifically, the risk assessment focusses on road vehicles (i.e., cars, vans, trucks and buses) equipped with automotive information and communication technology (ICT) systems (including both hardware and software) that are connected and/or enable automated driving. It is to be specified here, however, that the scope of the evaluation activities defined within the NIS Cooperation Group was not interpreted in a restrictive manner. Adequate leeway was provided in order to allow for more extensive discussions on any related matters and risks deemed relevant by the experts engaged throughout the assessment process. Additionally, while the NIS2 Directive a wider range of threats, this report focusses on malicious acts, as those were the threats predominantly identified by the experts.

To ensure a structured approach, the risk assessment followed the 'EU Methodology for Union-level Cybersecurity Risk Assessments'[37] defined by the NIS Cooperation Group on the basis of best practices and lessons learned from previous similar exercises, namely those related to the telecommunications and electricity sectors[38] and to fifth generation (5G) mobile networks[39]. The method involves several phases. In the first phase, risk identification, Member States involve a wide range of national experts from various sectors to identify the most pertinent risks. In the second phase, risk evaluation, the same experts assign motivated impact and likelihood categories to the risks collectively identified in the first stage. The third stage, risk analysis, consists of workshop with NISCG delegates and extensive follow-up discussions, which lead up to the assessment's conclusions and recommendations.

[37] Internal NISCG document.

[38] NIS Cooperation Group (2024) *Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors*. https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors

[39] NIS Cooperation Group (2019) *EU coordinated risk assessment of the cybersecurity of 5G networks*. https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

Furthermore, regarding the identification of high-risk suppliers, the assessment uses the criteria as defined in the ICT Supply Chain Security Toolbox.[40] It should be noted that identifying high-risk or critical suppliers is a complex exercise, for which the ICT Supply Chain Security Toolbox provides recommendations and initial guidelines.[41]

[40] EU Supply Chain Security Toolbox, page 21

[41] EU Supply Chain Security Toolbox, pages 40-47

2 Risk Assessment

This section sets out the results of the risk assessment. The risks are clustered based on the asset group they belong to, with exception of section 2.7 which elaborates on risks involving high-risk suppliers and not any asset group in particular. Each subsection, with the exception of section 2.7, provides a brief description of the asset group. Each subsection then expands on the highest risks identified, which were selected based on their impact and likelihood scores assigned by Member State experts. The threshold for inclusion in the paper was put at 'critical' impact and 'medium' likelihood, which is the highest combination of scores that occurred in the dataset. This constitutes the inflection point where coordinated action might be required to mitigate the consequences of a risk and the risk cannot be dismissed based on the unlikelihood of it happening. Where necessary, references are made to other identified risks that are strongly related to the top risks. The sections below are presented in no particular order.

2.1 Risks involving processing and decision-making systems

Description of the asset group

The processing and decision-making systems for CAVs are integrated hardware and software architectures that ingest real-time sensor and V2X data, fuse and interpret it with algorithms, and issue safe, optimised control and communication actions across the vehicle and network. Examples of such systems are, but are not limited to, AI-powered perception algorithms (e.g. for object detection, pedestrian recognition, and traffic sign classification), sensor fusion engines that integrate data from Light Detection and Ranging (LiDAR), radar, cameras, and other sensors, localisation and mapping systems (e.g. SLAM), and decision-making and trajectory planning modules that determine how the vehicle navigates complex traffic scenarios, driver monitoring systems that assess driver attention and readiness in semi-autonomous modes, and adaptive control systems that continuously adjust steering, braking, and acceleration based on AI inferences.

Identified risks

The risk scenarios identified by experts for this asset group are RS_47 to RS_55. Of these, the top risks identified are:

- An attacker changes the functions of the in-vehicle automated driving systems (ADAS / ADS) through adversarial techniques (RS_50).
- A hostile third country changes the functioning of the in-vehicle automated driving systems (ADAS / ADS) at the training phase, leading to unexpected behaviour in specific situations abroad (e.g. dangerously misinterpreting the road situation or being used as a weapon at a specific moment or after a specific command) (RS_51).
- An attacker uses its access to other vehicle systems to move laterally and gain access to the processing and decision-making systems (RS_49).

Analysis

Attacks involving the adversarial techniques have been demonstrated on several occasions. In 2018, researchers demonstrated an attack method that generates visible yet inconspicuous modifications to real-world objects, such as a black-and-white patterned sticker applied to road signs, to reliably mislead deep neural-network classifiers under varying physical conditions.[42] In 2020, researchers demonstrated how attackers could apply 'split-second phantom attacks' remotely by embedding phantom road signs into an advertisement presented on a digital billboard which caused a manufacturers' autopilot to suddenly stop the car in the middle of a road and an advanced collision avoidance system widely used in CAVs to issue false notifications.[43] The same researchers demonstrated an attack involving a projector to make the same autopilot apply the brakes in response to a phantom of a pedestrian that was projected on the road and the advanced collision avoidance system to issue false notifications in response to a projected road sign.[44] Finally, in 2025, researchers demonstrated the practical feasibility of LiDAR spoofing attacks against practical automated driving scenarios where the victim vehicle is driving at high speeds (60 km/h) and the attack

[42] Eykholt, K et al. (2018) *Robust Physical-World Attacks on Deep Learning Visual Classification.* https://openaccess.thecvf.com/content_cvpr_2018/papers/Eykholt_Robust_Physical-World_Attacks_CVPR_2018_paper.pdf

[43] Nassi et al. (2020) *Phantom of the ADAS: securing advanced driver-assistance systems from split-second phantom attacks.* https://dl.acm.org/doi/10.1145/3372297.3423359 ; Nassi et al. (2021) *Demo: attacking Tesla Model X's autopilot using compromised advertisement.* https://www.ndss-symposium.org/wp-content/uploads/autosec2021_23004_paper.pdf

[44] Nassi et al. (2020) *Phantom of the ADAS: securing advanced driver-assistance systems from split-second phantom attacks.* https://dl.acm.org/doi/10.1145/3372297.3423359

is launched from long distances (110 meters), testing vehicles that used popular automated driving stacks.[45]

To date, no attacks directly targeting the onboard AI systems have been recorded. Moreover, should they occur, such an attack would be difficult to prove and attribute due to the highly complex nature of such systems. However, consulted experts deemed such attacks plausible. A successful execution of such an attack, especially at a large scale, could easily lead to severe consequences, including the loss of life and significant material damage.

Existing measures

R155's threat & mitigation catalogue explicitly includes manipulation and spoofing of sensor inputs and forces manufacturers to show at type-approval that their CSMS detects, prevents, and monitors such attacks across the vehicle and back-ends.[46]

The risk of a hostile third country changing the functioning of the in-vehicle AI would be highly complex to assess and manufacturers are generally incentivised to ensure their systems work properly, due to potential legal and reputational ramifications. However, in certain cases, high-risk suppliers may be subject to coercion – which could potentially have devastating consequences (see section 2.7).

2.2 Risks involving vehicle control systems

Description of the asset group

Vehicle control systems are a set of interconnected technologies and components that manage and optimise the car's performance, safety, and comfort, including engine control, braking and stability. Components in this category are generally well protected and often include physical fail safes. For example, electronic control units (ECUs), which control the fuel injection, ignition and ancillaries of the engine using digitally

[45] Sato et al. (2025) *On the realism of LiDAR spoofing attacks against autonomous driving vehicle at high speed and long distance.* https://www.ndss-symposium.org/wp-content/uploads/2025-628-paper.pdf

[46] UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system (UN/ECE R155), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

stored equations and numeric tables, are protected from overheating. Additionally, this asset group includes the battery systems, which is the integrated assembly of energy storage components, power management electronics, thermal regulation systems, and monitoring software that supplies and manages electrical power for the vehicle's propulsion, onboard electronics, sensing and computing systems, and connectivity functions.

Identified risks

The risk scenarios identified by experts for this asset group are RS_03 to RS_16. Of these, the top risks identified are:

- An attacker targets the radio-based interfaces in the vehicle to disrupt the normal functioning of the vehicle while driving (RS_04).
- An attacker launches an attack that causes the car batteries to overheat and burn (RS_05).
- An attacker launches an attack that manipulates the functioning of the Electronic Control Units (ECUs) in a vehicle (RS_06).

Analysis

Attacks involving a takeover of vehicle control systems have been demonstrated on multiple occasions. In 2015, researchers remotely manipulated the transmission, steering and braking functions of a vehicle.[47] In 2016, researchers demonstrated a remote attack that compromised the vehicle's CAN Bus and allowed remote control of the driving functions.[48] In 2022, researchers demonstrated a number of attacks that allowed for manipulation of vehicle control systems via compromises in the cloud and back-end systems for a wide range of vehicle manufacturers.[49]

[47] Miller & Valasek (2015) *Remote exploitation of an unaltered passenger vehicle*. https://illmatics.com/Remote%20Car%20Hacking.pdf

[48] Keen Security Lab (2016) *Car hacking research: remote attack tesla motors*. https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[49] Curry (2022) *Web hackers vs. the auto industry: critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and more*. *https://samcurry.net/web-hackers-vs-the-auto-industry*

Researchers have also demonstrated attacks targeting batteries. Faulty components of battery management systems, such as a compromised voltage regulator, could lead to cyberattacks that can overdischarge or overcharge the battery. Overdischarge could lead to failures such as internal shorts in the timescale of minutes through cyberattacks that compromise energy-intensive vehicle subsystems like auxiliary components. Attacks that overcharge the pack could shorten the lifetime of a new battery pack to less than a year. Furthermore, such attacks also pose physical safety risks via the triggering of thermal events (fire).[50]

Existing measures

Under the current type-approval framework, a vehicle may not be type-approved in the EU unless the manufacturer runs a CSMS that identifies threats to control systems and shows effective mitigations and monitoring.[51] Additionally, fixes to control-system software must be delivered via a secure, authenticated OTA process with rollback/safe-state and auditable update governance.[52]

Generally, these types of systems are expected to be well secured. However, as the research has shown, such systems can occasionally be remotely accessed via other systems that provide an attack vector, including cloud and backend infrastructures (see section 2.6) and communication and connectivity systems (see section 2.3).

2.3 Risks involving communication and connectivity systems

Description of the asset group

Communications and connectivity systems in CAVs refer to the integrated technologies that enable real-time data exchange between vehicles, infrastructure, cloud services,

[50] Sripad et al. (2017) *Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks*. https://ar5iv.labs.arxiv.org/html/1711.04822

[51] UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system (UN/ECE R155), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

[52] UN Regulation No. 156 – Uniform provisions concerning the approval of vehicles with regard to software update and software update management system, as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

and other road users. These systems encompass Vehicle-to-Everything (V2X) communications and rely on wireless technologies such as Dedicated Short-Range Communications (DSRC), Cellular-V2X (C-V2X), and 5G. Their primary function is to enhance situational awareness, improve traffic efficiency, support cooperative driving, and enable over-the-air updates and cloud-based services, all of which are critical to the safe and intelligent operation of automated vehicles.

Identified risks

The risk scenarios identified by experts for this asset group are RS_56 to RS_79 and RS_89. Of these, the top risks identified is:

- An attacker uses the communications and connectivity systems to gain access to other vehicle systems (RS_56).

Analysis

Fully remote manipulation of a vehicle via the communication and connectivity systems, without the need for modifications to the vehicle or physical interaction by the attacker or driver, was first demonstrated by researchers in 2015, who gained unauthorised access to vehicle systems remotely which allowed them to affect physical systems such as steering and braking.[53] The paper lead to a 1.4 million vehicle recall by the target vehicle's manufacturer. Additionally, in 2016, security researchers demonstrated an attack involving access the vehicle's companion app and the car's Wi-Fi access point which allowed control of non-driving functions, such as toggling HVAC to drain the battery and disabling the theft alarm, enabling physical access.[54] Finally, in 2023, researchers demonstrated a full remote-to-CAN chain for a popular vehicle model.[55] The researchers exploited a chain of vulnerabilities that allowed them to go from Bluetooth to full control of the car's internal networks by hopping from an

[53] Miller & Valasek (2015) *Remote exploitation of an unaltered passenger vehicle*. https://illmatics.com/Remote%20Car%20Hacking.pdf

[54] Pen Test Partners (2016) *Hacking the Mitsubishi Outlander PHEV hybrid*. https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

[55] Berard & Dehors (2023) *Unlocking the drive, exploiting Tesla Model 3*. https://www.synacktiv.com/sites/default/files/2023-11/tesla_codeblue.pdf

infotainment app, into the wireless chipset, up to the Linux kernel, and finally past the security gateway to the CAN buses.

These attacks demonstrate the communication and connectivity systems' heightened exposure to cybersecurity attacks, making such systems a likely vector for attacks aimed at gaining access to more critical CAV systems. Furthermore, communication and connectivity systems process and store troves of sensitive and personal data.[56]

Existing measures

The current type-approval framework in the EU mandates that the manufacturer runs a Cybersecurity Management System (CSMS) that identifies threats to control systems and shows effective mitigations and monitoring.[57] This includes threats to the communications and connectivity systems. Additionally, fixes to the communication and connectivity systems must be delivered via a secure, authenticated OTA process with rollback/safe-state and auditable update governance.[58]

2.4 Risks involving sensing systems

Description of the asset group

A sensing system in CAVs refers to the integrated suite of hardware and software components that detect and perceive the vehicle's internal and external environment to enable autonomous operation and connectivity features. These systems are fundamental to vehicle autonomy, safety, and real-time decision-making. Examples of sensing systems include environmental sensors, such as cameras, radar, LiDAR, ultrasonic sensors and infrared sensors, but also internal sensors monitoring the

[56] European Data Protection Supervisor (2019) *TechDispatch #3: connected cars.* https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en

[57] UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system (UN/ECE R155), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

[58] UN Regulation No. 156 – Uniform provisions concerning the approval of vehicles with regard to software update and software update management system, as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

vehicle’s status, such as air oil or coolant level sensors and temperature sensors. Systems that fuse and interpret sensor input are not included in this section.

Identified risks

The risk scenarios identified by experts for this asset group are RS_35 to RS_46. Of these, the top risks are:

- An attacker uses the sensing systems to gain access to other vehicle systems (RS_35).
- An attacker uses its access to other vehicle systems to gain access to the sensing systems (RS_36).

Risks involving sensing systems were generally scored as lower impact and/or likelihood. Most existing research that includes sensing systems involve manipulation of the data that the sensing systems ingest. Examples include the spoofing of LiDAR systems that make the sensor either register object that are not there[59] or miss objects that are there[60]. Other examples include similar demonstrated attacks on camera systems by manipulating its inputs with various types of light sources to trigger identifications of objects that are not there[61] or false interpretations of traffic light signals.[62] Yet other researchers have described set of attack methods involving GNSS

[59] Sato et al. (2025) *On the realism of LiDAR spoofing attacks against autonomous driving vehicle at high speed and long distance.* https://www.ndss-symposium.org/wp-content/uploads/2025-628-paper.pdf

[60] Cao et al (2022) *You can’t see me: physical removal attacks on LiDAR-based autonomous vehicles driving frameworks.* https://www.usenix.org/system/files/sec23summer_349-cao-prepub.pdf

[61] Nassi et al. (2020) *Phantom of the ADAS: securing advanced driver-assistance systems from split-second phantom attacks.* https://dl.acm.org/doi/10.1145/3372297.3423359 ; Nassi et al. (2021) *Demo: attacking Tesla Model X’s autopilot using compromised advertisement.* https://www.ndss-symposium.org/wp-content/uploads/autosec2021_23004_paper.pdf

[62] Bhupathiraju et al. (2024) On the vulnerability of traffic light recognition systems to laser illumination attacks. https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-24-paper.pdf

spoofing.[63] Finally, some research demonstrated attacks related to wireless key infrastructures.[64]

Existing measures

Under the current type-approval rules, manufacturers must maintain a CSMS that covers sensors, perception, positioning, and V2X subsystems, as well as a threat analysis and risk assessment (TARA) including “manipulation of sensors and perception data.[65] Additionally, sensors supporting driver assistance or automated driving must have ASIL-graded safety fallbacks, such as degraded-mode driving, driver hand-over, or system shutdown if a sensor is compromised.[66]

Therefore, the existing measures for risks directly to the sensing systems is deemed to be adequate provided that they are sufficiently isolated from the vehicle’s critical systems and cannot alter the vehicles behaviour beyond their intended function.

While some demonstrated attacks in earlier research involves sensing systems, their impact occurs due to errors in the processing and decision-making systems. These risks are dealt with in section 2.1.

2.5 Risks involving charging infrastructure

Description of the asset group

Charging infrastructure is the combined hardware, software, and grid connections that let electric vehicles recharge at home, work, depots, and public sites. It includes AC

[63] Psiaki & Humphreys (2016) *GNSS spoofing and detection*. https://radionavlab.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf ; Ying et al. (2023) GPS spoofing attack detection on intersection movement assist using one-class classification. https://www.ndss-symposium.org/wp-content/uploads/2023/02/vehiclesec2023-23038-paper.pdf

[64] Verdult et al. (2015) Dismantling megamos crypto: wirelessly lockpicking a vehicle immobilizer. https://flaviodgarcia.com/publications/Dismantling_Megamos_Crypto.pdf ; Francillon et al. (2010) Relay attacks on passive keyless entry and start systems in modern cars. https://www.ndss-symposium.org/wp-content/uploads/2017/09/franc2.pdf

[65] UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system (UN/ECE R155), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

[66] International Organization for Standardization (ISO) (2018) *ISO 26262-1:2018 Road vehicles — Functional safety*. https://www.iso.org/standard/68383.html

chargers and DC fast/ultra-fast units, connectors and cables, metering and protection, and upstream site power like transformers and switchgear tied to utilities.

Identified risks

The identified risk scenarios in this asset group are RS_100 to RS_107, of which the top risk is:

- An attacker targets the charging system causing it to overcharge the rechargeable energy storage system (REESS), resulting in excess heat and potential explosion of the REESS (RS_103).

Analysis

A large number of experts flagged that the charging infrastructure is currently often constructed without adequate safety measures or backups. A recent large-scale measurement study of 235 publicly deployed DC charging systems across 4 European countries showed that only 12% of the charging analysed charging stations implemented Transport Layer Security (TLS), leaving all others vulnerable to attacks that have been demonstrated years ago – among other security issues.[67] Another systematic analysis of widely deployed EV charging station management systems showed an array of vulnerabilities which demonstrated their insecurity against remote cyberattacks.[68] Additionally, the researchers simulated the impact of practical cyberattack scenarios against the power grid, which result in possible service disruption and failure in the grid. Finally, several real-world examples of cyberattacks disabling electric charging stations have been observed.[69]

[67] Usenix (2025) *Current affairs: a security measurement study of CSS EV charging deployments*. https://www.usenix.org/system/files/usenixsecurity25-szakaly.pdf

[68] Nasr et al. (2022) *Power jacking your station: in-depth security analysis of electric vehicle charging station management systems.* https://www.sciencedirect.com/science/article/pii/S0167404821003357

[69] Skarga-Bandurova (2023) Cyber security of electric vehicle charging infrastructure: open issues and recommendations. https://h2020response.eu/wp-content/uploads/2023/02/BigData-2022-v02-002.pdf

Charging operators[70] fall under the NIS2 directive and have to implement cyber risk management measures (Article 21) and report incidents of significant impact (Article 23).

2.6 Risks involving cloud and backend systems

Description of the asset group

The cloud and backend systems are the off-board digital infrastructure that ingests and processes telemetry from vehicles at scale, provides secure APIs to mobile apps and partners, and orchestrates services back to the fleet. They typically include identity and access management for vehicles, drivers, and devices; message brokering and event streaming for bidirectional data flow; data lakes/warehouses for storage and analytics; digital twins for per-vehicle state; and service platforms for over-the-air updates, remote commands (lock/unlock, start/stop, charge/schedule), diagnostics, predictive maintenance, and V2X integration.

Identified risks

The identified risk scenarios in this asset group are RS_80 to RS_88 and RS_90 to RS_99, of which the top risks are:

- An attacker introduces a backdoor in an open-source library widely used in automotive operating systems (RS_98).
- An attacker manipulates over-the-air (OTA) update to deliver a malicious software, patch or configuration (RS_82).

Analysis

Attacks involving cloud and backend infrastructure have been demonstrated on several occasions. For example, in 2024, a security researcher demonstrated attacks via the vehicle manufacturers webpage or iOS application that allowed the attacker to manipulate remote control of key functions such as unlocking doors, starting the engine and disabling the starter as well as identifying geolocation data from the vehicle. The

[70] Directive (EU) 2022/2555, Annex I includes operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider.

attack only required a license plate number to target a specific vehicle.[71] Moreover, in 2022, researchers demonstrated attacks through cloud and backend systems for a wide array of vehicle manufacturers. Attack vectors included, but were not limited to, misconfigured accounts, APIs, web portals and leaked cloud credentials.[72] Additionally, several real-world incidents involving cloud and backend systems have been observed, though they mainly pertain to data theft or accidental loss of data.[73]

Existing measures

To sell new vehicle types in the EU, manufacturers must prove a CSMS that covers back-end and cloud interfaces (threat analysis, monitoring, incident response, secure comms, IAM, logging, supplier control) across the whole ecosystem.[74] Additionally, the SUMS requires secure OTA update pipelines (code signing, authenticity, version control, rollback, update campaign governance) and secure back-end update infrastructure. Both these requirements extend to open-source software. Their lack of a contractual audit leverage can be compensated with technical gates and assurance.[75]

When applied adequately, these measures should address the risks identified for cloud and backend systems. However, discussions with experts raised the issue of verification of the content of updates, which is done by the manufacturer itself.

[71] Curry (2024) *Hacking Kia: remotely controlling cars with just a license plate.* https://samcurry.net/hacking-kia

[72] Curry (2022) *Web hackers vs. the auto industry: critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and more*. *https://samcurry.net/web-hackers-vs-the-auto-industry*

[73] See for example: Toyota (2023) *Apology and notice concerning newly discovered potential data leakage of customer information due to cloud settings.* https://global.toyota/en/newsroom/corporate/39241625.html ; Tesla (2023) *Notice of data incident* . https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/014ae6db-4cb7-464b-b827-5d73f0bbc911/5f2a16ee-b501-453d-a868-8b8fb871c7a7/Tesla%20-%20Template%20Notice.pdf ; Volkswagen/Audi (2021) *Notice of data breach*. https://oag.ca.gov/system/files/Audi%20Notification%20Letter%20Template.pdf

[74] UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system (UN/ECE R155), as adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) under the 1958 Agreement. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

[75] For suggestions, see ENISA (2023) *Good practices for supply chain cybersecurity*. https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf ; ENISA (2025) *Technical Implementation guidance*, June 2025, version 1.0, chapter 5. https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

Intentional malicious updates are therefore not adequately captured by the existing mitigation measures (see section 2.7).

2.7 Risks involving high-risk suppliers

Description

High-risk suppliers are those suppliers that manufacture CAVs or CAV related critical assets and whose risk profile fits elements of the framework of laid out in the ICT Supply Chain Security Toolbox.

Identified risks

The identified risk scenarios in this asset group are RS_17 to RS_34, of which the top risks are:

- A hostile third country pressures a CAV manufacturer operating within its jurisdiction to implement hidden and malicious hard- or software, updates or configurations on their products in order to physically manipulate the fleet (RS_17).
- A hostile third country pressures a Tier 1 supplier operating within its jurisdiction (for example ECU manufacturers, cloud providers, sensor manufacturers) to implement hidden and malicious hard- or software, updates or configurations on their products in order to physically manipulate the fleet (RS_20).

Analysis

The possibility for a manufacturer to remotely manipulate a vehicle is a common feature in modern vehicles and has been leveraged in real-world incidents. In 2022, a popular tractor manufacturer remotely disabled its stolen vehicles in the context of the war in Ukraine.[76] Many modern vehicles are equipped with similar functionalities that explicitly allow the manufacturer to remotely manipulate the vehicle, usually as part of integrated theft assistance services that include manufacturer-run remote

[76] CNN (2022) *Russians plunder $5M farm vehicles from Ukraine – to find they've been remotely disabled*. https://edition.cnn.com/2022/05/01/europe/russia-farm-vehicles-ukraine-disabled-melitopol-intl

immobilisation.[77] Such services are normally mentioned explicitly by the manufacturer as part of the service agreement and can only be leveraged where there is a clear legal basis for the manufacturer to do so with consent of the vehicle's owner and in cooperation with local authorities.

However, research has shown other potentially far-reaching controls that manufacturers or telematics platform providers possess beyond those disclosed in public-facing services.[78] Additionally, vehicles are susceptible to rogue access functionalities implemented by the manufacturer. For example, in 2025, researchers of a European bus operator found an undisclosed functionality that allows for the manufacturer to remotely stop the vehicle or render it inoperable.[79]

Although such functionalities are not often used outside of the narrow context of theft assistance, the existence of pathways for manufacturers to remotely manipulate vehicles remotely have been well documented. While manufacturer abuse of such access is unlikely due to the damaging consequences it would have on the manufacturer's reputation and potential legal consequences, the legal and political circumstances of high-risk suppliers can lower the confidence levels that such abuse by the manufacturer shall not take place. For example, high-risk vehicle or component suppliers with a link to foreign militaries can be forced to weaponise privileged access to vehicle control systems. While not highly likely, such a 'black swan' event would have devastating consequences on the EU, including loss of life of EU citizens and significant material damage.

[77] Examples include, but are not limited to: Stellantis' 'Mopar Connect', which allows for the disabling the engine on stop (see: https://www.mopar.eu/eu/en/connected-services/mopar-connect); Ford's 'Theft Mode' allowing for disabling of some vehicle features (see: *https://media.ford.com/content/fordmedia/feu/en/news/2021/10/07/ford-helps-theft-victims-recover-stolen-vehicles-using-connected.*html); Volvo's 'stolen vehicle tracking' and 'remote vehicle immobilisation / mobilisation services' (see: https://www.volvocars.com/en-me/legal/privacy/privacy-car/); Nissan's 'Stolen Vehicle Tracking' that allows remote disabling of the vehicle start (see: https://www-europe.nissan-cdn.net/content/dam/Nissan/gb/Ownership/ncs/How%20Stolen%20Vehicle%20Tracking%20Works.pdf); BMW's Security Pro S5 which includes an 'engine lock' option (see:

[78] Curry (2022) *Web hackers vs. the auto industry: critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and more*. *https://samcurry.net/web-hackers-vs-the-auto-industry*

[79] Ruter (2025) *We have conducted a comprehensive safety test of electric buses*. https://ruter.no/en/ruter-with-extensive-security-testing-of-electric-buses

These considerations can be a hostile third country changes the functioning of the in-vehicle AI (ADAS / ADS) at the training phase, leading to unexpected behaviour in specific situations abroad (e.g. dangerously misinterpreting the road situation or being used as a weapon at a specific moment or after a specific command) (RS_51, see section 2.1 for further details).

Additionally, vehicle manufacturers have access to highly specific location- and user data. The European Data Protection Supervisor already reported in 2019 that 'the increasing amount of sensors used in [CAVs] raises the risk of excessive data collection beyond the needs for the provided services' and flagged issues with data retention, collection of sensitive personal data, as well as the lack of transparency, user control and purpose limitation.[80] Moreover, recent data leaks provided evidence of the high level of granularity in data collected by vehicle manufacturers.[81] While these leaks emphasise the need for connected service providers to implement adequate cybersecurity measures for suppliers of connected services in CAVs, such measures might not provide sufficient guarantees of security or EU data where this data is collected by high-risk suppliers. It is, for example, impossible to guarantee that high-risk suppliers that operate from jurisdictions with far-reaching intelligence laws requiring them to share any data held by the supplier with government authorities, or suppliers that have links to military bodies, will not hand over data collected within Europe. Several identified risks deal with this issue (RS_18, RS_21, RS_23). Experts assigned an overall lower impact score to these risks due to the fact that such data collection is already happening. However, this does not dimmish the real risks that these practices pose to EU security. Data from CAVs can be used for a range of strategic objectives, including persistent location tracking and profiling individuals (even from anonymised data)[82] and collecting location data, imagery and other data

[80] European Data Protection Supervisor (2019) *TechDispatch #3: connected cars.* https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en

[81] As evidenced by several recent data leaks, e.g.: Spiegel (2024) *Wir Wissen, wo dein Auto steht*. https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027 ; Toyota (2023) *Apology and notice concerning newly discovered potential data leakage of customer information due to cloud settings.* https://global.toyota/en/newsroom/corporate/39241625.html.

[82] Maerivoet & Ons (2025) *Trusted integrity and authenticity for road applications (TIARA).* https://www.cedr.eu/docs/view/671a142d82dd7-en ; Mozilla Foundation (2023) 'privacy nightmare on wheels': every car brand reviewed by mozilla – including Ford, Volkswagen and Toyota – flunks

near sensitive areas such as military facilities, government sites or other critical infrastructures that can be combined to map visits and patterns near those facilities.[83]

Additionally, the high-risk supplier scenarios are greatly amplified in combination with another top scenario (RS_82), where an attacker manipulates over-the-air (OTA) update to deliver a malicious software, patch or configuration.

Finally, the identified risks show that these concerns do not apply exclusively to full CAVs manufactured by high-risk suppliers but also to components, to the extent that they can be used as an attack vector for the scenarios described in this section.

Existing measures

Risks stemming from high-risk suppliers are currently insufficiently addressed. Remote control capabilities are a regular feature of modern vehicles, with various pathways available to manufacturers to activate such features. While legal consequences and reputational damage provide an effective barrier to keep manufacturers from abusing such functionalities, these mitigation measures are inadequate where it pertains to high-risk suppliers who may be coerced by military or government bodies. Moreover, espionage and illegal data collection can be carried out over extended periods of time while avoiding detection, as such activities are obfuscated by regular exchanges of data.

Regarding risks to data stemming from high-risk suppliers, the General Data Protection Regulation (GDPR) remains the primary safeguard for personal data, requiring consent for collection and processing, and enforcing data minimisation and transfer restrictions. However, much of the data generated by vehicles, including grid analytics, traffic flows, or aggregated technical metrics, can fall outside its definition of personal data. There currently is no comprehensive framework for cross-border transfers of such data and the GDPR's safeguards for data sent to countries without an adequacy decision do not cover industrial and operational data.

privacy test. https://www.mozillafoundation.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/

[83] Alam (2024) *Data privacy and security in autonomous connected vehicles in smart city environment*. https://www.mdpi.com/2504-2289/8/9/95

Another control on data are user consent forms. However, current consent mechanisms are found to be inadequate due to their complexity and opacity and users are largely unaware of the extent to which data on them is generated and collected by the manufacturer.[84] Moreover, consent is usually bundled with vehicle use, leaving users with little real choice, and privacy policies are typically difficult to access or understand.

[84] European Commission (2023) *Study on the provision of information to consumers about the processing of vehicle-generated data.* https://commission.europa.eu/system/files/2023-03/study%20on%20the%20provision%20of%20information%20to%20consumers-DS0523007ENN.pdf

3 Conclusions

This risk assessment has identified 107 unique risks pertaining to CAVs. Of those, 14 risks were collectively assigned the highest occurring impact score ('critical') and likelihood score ('medium') by the experts. The previous sections have addressed these top risk scenarios in-depth, as well as other closely related scenarios identified by the experts.

The assessment has found that many of the top risks are addressed by the EU's current type-approval rules – provided they are adequately implemented.[85] This includes scenarios where an attacker targets the in-vehicle AI (RS_50) or uses it to gain access to other systems (RS_49); an attacker targets vehicle control systems (RS_04, RS_05, RS_06); an attacker uses the communications and connectivity systems to gain access to other vehicle systems (RS_56); an attacker uses the sensing systems to gain access to other vehicle systems or vice-versa (RS_35, RS_36); an attacker introduces a backdoor in an open-source library (RS_98) or where an attacker manipulates an OTA update (RS_82). However, the existing research and recorded incidents have clearly shown that CAVs can be hacked through various pathways. Such hacks have also been shown to have potentially severe consequences, including the full remote takeovers of vehicles or the leaking large amounts of highly sensitive data.

However, the type-approval regime has mainly been created to ensure traffic safety. New kinds of threats may aim to disturb EU public safety in an organized manner and such actions may potentially have government backing. Resources of public or private companies implementing type-approval regulations are not enough to mitigate these new threads adequately.

Additionally, the cybersecurity of charging infrastructure has been found to be lacking. Several experts raised their concerns and existing studies have revealed a generally low level of cybersecurity in charging infrastructure. In the EU, charging infrastructure cybersecurity falls under the NIS2 Directive, where 'operators of a recharging point that are responsible for the management and operation of a recharging point, which

[85] Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (the Framework Regulation, which replaced Directive 2007/46/EC).

provides a recharging service to end users, including in the name and on behalf of a mobility service provider' are classified as critical entities in the energy sector.[86] It is therefore paramount that charging infrastructure is adequately secured.

Furthermore, the risk assessment has identified a series of top risks pertaining to high-risk suppliers subjected to government or military pressure to implement hidden and malicious hard- or software, updates or configurations in their products (RS_17, RS_20) or changing the functioning of in-vehicle AI (RS_50). A supplier can leverage its (known or hidden) direct access pathways to the vehicle as an attack vector, thereby effectively bypassing many of the controls mandated by the type-approval regulation. Moreover, such attackers can leverage normal over-the-air updates, another top risk scenario identified (RS_82), to prevent immediate detection.

Finally, the risk assessment has identified that the vehicle control systems and processing and decision-making systems are particularly critical asset groups. Attacks on these asset groups has been shown to cause potentially severe consequence that may lead to loss of life or significant damage. Communication and connectivity systems and cloud and backend systems have also been identified as critical assets, as these systems are typical vectors of attack which is in large part due to their public-facing interfaces. Additionally, these systems contain troves of sensitive data which require stringent protection against intentional or unintentional loss. Sensing systems have been identified to be a less likely vector of attack – provided that they only communicate their collected data with the vehicle as intended.

[86] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

4 Recommendations

In order to adequately address the identified risks discussed in the previous sections, several recommendations are set out for the European Commission, national administrations, CAV manufacturers and charging infrastructure operators.

The NIS Cooperation Group recommends that the **European Commission**:

- R_01: Identifies, together with the Member States, proportionate measures to de-risk EU supply chains from high-risk suppliers, especially where it pertains to processing and decision-making systems, communication and connectivity systems and vehicle control systems that can receive remote updates;
- R_02: Develops guidelines for data localisation of sensitive, non-personal data, based on reciprocity.
- R_03: Conducts follow-up research on the potential impact of attacks on the charging infrastructure on the EU grid;
- R_04: Ensures that the findings of this risk assessment are reflected in future EU policies and initiatives, including on EU funding;
- R_05: Communicates the findings of this assessment to international partners;
- R_06: Discusses the follow-up of this risk assessment within the NIS Cooperation Group;
- R_07: Takes into account the lessons learnt for this risk assessment for future NIS Cooperation Group risk assessments;
- R_08: Uses the identified risk in preparation of the risk scenarios in cybersecurity preparedness exercises.

The NIS Cooperation Group recommends that the **Member States**:

- R_09: Apply the recommendations outlined in the EU ICT Supply Chain Security Toolbox in the context of CAVs and related charging infrastructure, including:
    - establishing a common framework for the assessment of critical suppliers,
    - promoting multi-vendor strategies,
    - reducing dependencies on high-risk suppliers,

- ensuring national policies and/or regulations are in place in order to take decisions to restrict or exclude high-risk suppliers from supply chains identified as critical,
- increasing cooperation to exchange information and best practices on vulnerability monitoring and coordinated vulnerability disclosure,
- sharing information on ICT supply chain incidents related to CAV within the NIS Cooperation Group, the European cyber crisis liaison organisation network (EU-CyCLONe) and the CSIRTs network.

R_10: Use the European Vulnerability Database (EUVD) to enhance national cybersecurity and improve risk management;

R_11: Consider information sharing on incidents in CAVs, to timely surface new issues in a rapidly developing hard- and software. To this extend, existing fora such as the CSIRTs Network and the Cooperation Group can be leveraged;

R_12: Share findings and best practices with private stakeholders.

The NIS Cooperation Group recommends that **CAV manufacturers**:

R_13: Consider the risks identified when implementing and maintaining robust risk management systems, following on European and international standards;

R_14: Harden cloud infrastructures[87];

R_15: Improve the provision of information to consumers about the processing of vehicle-generated data, as recommended in the Commission's 2023 study.[88]

The NIS Cooperation Group recommends that **operators of charging infrastructures**:

[87] See for example the guidance laid out by the Cloud Security Alliance: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[88] European Commission (2023) *Study on the provision of information to consumers about the processing of vehicle-generated data.* https://commission.europa.eu/system/files/2023-03/study%20on%20the%20provision%20of%20information%20to%20consumers-DS0523007ENN.pdf

R_16: Swiftly implement the cybersecurity risk management measures set out in Article 21 of the NIS2 Directive[89].

[89] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng