Navigating the road to automotive cybersecurity compliance

Navigating the road to automotive cybersecurity compliance

Franco Oberti[1,2], Fabrizio Abrate[3], Alessandro Savino[1], Filippo Parisi[2], and Stefano Di Carlo[1]
[1]*Control and Computer Eng. Dep., Politecnico di Torino* Torino, Italy
[2]*Dumarey Softronix*, Torino, Italy
[3]*Dumarey Automotive*, Torino, Italy

***Abstract*—Modern vehicles are now part of a complex digital ecosystem, leveraging Artificial Intelligence (AI) and cloud computing for enhanced safety, efficiency, and user experience. However, this digital integration has introduced significant cybersecurity challenges, including data protection, unauthorized access prevention, and user privacy.**

As vehicles become more vulnerable to cyber-attacks, the industry must implement robust cybersecurity measures. Regulations like the UN's UNR155 and UNR156 establish stringent cybersecurity requirements, demanding comprehensive management systems, regular updates, and continuous testing to counter evolving threats. These regulations underscore the importance of cybersecurity in automotive safety.

Future automotive cybersecurity will depend on developing advanced protections and collaboration among manufacturers, policymakers, and cybersecurity experts to ensure innovation and security in an interconnected digital world.

***Index Terms*—Cybersecurity, Automotive Safety, Regulations, Artificial Intelligence, Lifecycle Management**

I. Introduction

The automotive industry, which began in 1908 with the introduction of the Ford Model T, has undergone profound transformations [1], [2]. Today's vehicles are more than mechanical marvels; they incorporate advanced connectivity features that link them to a broad digital ecosystem. This evolution has significantly improved safety, efficiency, and the overall driving experience [3]. However, integrating these technologies introduces new challenges, particularly in cybersecurity.

Modern vehicles boast advanced connectivity, incorporating AI [4] and cloud computing technologies [5]. These features enable vehicles, intelligent infrastructures, and digital systems to communicate, enhancing safety, efficiency, and driving experience. Conversely, vehicles become more integrated and connected and more susceptible to cyber-attacks [6]–[9]. Major cybersecurity challenges include securing data, protecting vehicles, and ensuring privacy [10]–[15].

The fully connected automotive world offers immense benefits but poses significant cybersecurity risks [16]. To ensure these risks do not undermine the benefits, the automotive industry must implement comprehensive and robust cybersecurity strategies [15]. By prioritizing security and fostering collaboration among stakeholders [17], [18], the industry can protect its advancements and continue to innovate securely and effectively. Accordingly, governments and companies have issued numerous regulations and engineering standards focusing on cybersecurity in automotive technology. These standards emphasize continuous innovation and vigilance, stakeholder collaboration, regular updates and testing, and proactive threat mitigation. This paper overviews the regulative effort to address these challenges and the essential role of ongoing compliance to adapt to evolving threats in the automotive sector.

This work was supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU

Authors contacts: {franco.oberti, alessandro.savino, Fabrizio Abrate, stefano.dicarlo}@polito.it and filippo.parisi@dumarey.com

II. Automotive Cybersecurity Legislation

In Europe and partner markets such as Korea and Japan, evolving regulations focus on cybersecurity for road vehicles. Two crucial regulations are United Nations Regulation No. 155 (UNR155) and United Nations Regulation No. 156 (UNR156).

A. United Nations Regulation No. 155

UNR155 [19] addresses cybersecurity management systems for vehicles, aiming to mitigate the increasing threats of cyber attacks in the automotive sector. Adopted by the United Nations Economic Commission for Europe (UNECE), it became effective in January 2021. This regulation mandates that all new vehicle types must comply starting from July 2022, and all vehicles produced must comply by July 2024. The Technical Assessment (TA) process under UNR155 involves a thorough evaluation of a manufacturer's Cyber Security Management System (CSMS) by an independent authority or recognized technical service. The CSMS must demonstrate the manufacturer's capability to identify, manage, and mitigate cyber risks throughout the vehicle's lifecycle, focusing on threat detection, incident response, and security measures implementation during the design, production, and post-production stages. A crucial requirement is that the CSMS certification is valid for three years, after which re-certification is necessary to ensure continuous compliance and adaptation to evolving cyber threats.

B. United Nations Regulation No. 156

UNR156 [20] complements UNR155 by focusing on software updates and software integrity within vehicles. It ensures

that vehicles remain secure and function correctly throughout their operational life, especially when receiving software updates. Key requirements include the deployment of Software Update Management System (SUMS), secure Over-The-Air (OTA) update processes, and continuous monitoring and validation of software integrity. While both UNR155 and UNR156 emphasize security, UNR156 distinctly focuses on the lifecycle management of vehicle software.

C. Network and Information Systems Directive

The Network and Information Systems Directive (NIS2) [21] expands the scope of cybersecurity beyond just the vehicle to include the infrastructure supporting vehicle manufacturing and services. It aims to enhance the resilience of critical infrastructures within the automotive sector. Key measures include enhanced cybersecurity protocols for industrial control systems, improved incident response capabilities, and mandatory reporting of significant cyber incidents. NIS2 affects a broader spectrum of the automotive industry, targeting supply chains, manufacturing plants, and service networks.

The introduction of UNR155, UNR156, and NIS2 represents a significant advancement in securing the automotive industry against emerging threats. These regional regulations enhance vehicle and infrastructure security and set a precedent for regional regulatory practices. As the industry adapts to these changes, ongoing collaboration and innovation will be crucial to meet the evolving demands of regulatory compliance.

Fig. 1. The figure illustrates the cybersecurity focus areas of UNR-155, NIS2, and UNR-156 within the context of vehicle functionality. UNR-155 primarily covers cybersecurity in the onboard domain, directly addressing the product's security. NIS2 operates in the off-board domain, handling cybersecurity related to the IT infrastructure that supports vehicle functionality. UNR-156 acts across both domains, providing comprehensive cybersecurity coverage for both the onboard systems and the supporting off-board IT infrastructure

In the U.S., the National Highway Traffic Safety Administration (NHTSA) [22] has released an updated version of "Cybersecurity Best Practices for the Safety of Modern Vehicles," improving upon its 2016 edition. This document offers guidance for the automotive industry to enhance vehicle cybersecurity, ensuring safety.

According to the NHTSA, as vehicle technology and connectivity continue to advance, maintaining a strong focus on cybersecurity is imperative for automakers, developers, and operators. The NHTSA remains committed to ensuring the safety of vehicles on the nation's roads, providing updated best practices to help the industry mitigate cybersecurity risks.

Agency research, industry voluntary standards, and recent insights from motor vehicle cybersecurity studies inform the 2022 Cybersecurity Best Practices. Reflecting public feedback received on the draft published in the Federal Register in 2021, this non-binding document encapsulates critical best practices anticipated to significantly influence the industry. The NHTSA routinely assesses cybersecurity risks and best practices, planning to update these guidelines to address the ongoing evolution of motor vehicles and their cybersecurity technologies.

In September 2023, the Technical Committee on Intelligent and Connected Vehicles under China Automotive Technology and Research Center Co., Ltd (CARTAC) [23] completed a technical review of two crucial standards: "Technical Requirements for Vehicle Cybersecurity" and "Intelligent and Connected Vehicle - Data Storage System for Automated Driving." These standards are poised to proceed through Technical Barrier to Trade (TBT) notification stages and are expected to be officially released in the second quarter of 2024. It is anticipated that the implementation of "Technical Requirements for Vehicle Cybersecurity" will occur concurrently with the "General Technical Requirements for Software Update of Vehicles."

The three mandatory standards discussed—pertaining to automotive software updates, cybersecurity, and data storage systems for automated vehicles—are aligned with UN R155, R156, and the draft Data Storage System for Automated Driving (DSSAD). As of October 2023, all have successfully passed technical review.

D. Introduction to the Formulation of Chinese Mandatory Standards

To clarify the process of formulating mandatory standards in China, particularly for "Technical Requirements for Vehicle Cybersecurity," we outline the development timeline following the general procedures in the Management Measures for Mandatory National Standards. Completing the technical review by the committee confirms that the technical specifications of the standard have been finalized, setting the stage for a predicted official release in the second quarter of 2024 based on the timelines of previous standards.

E. Estimated Implementation Date of the Standard

The standards "Technical Requirements for Vehicle Cybersecurity" and "Intelligent and Connected Vehicle - Data Storage System for Automated Driving" are expected to be released in May 2024 and to come into force in November 2024. As per the adoption procedure into the China Compulsory Certification (CCC) rules, Technical Committee TC 114 will evaluate these standards and determine their inclusion

timeline into the CCC. Based on recommendations from the working group, the implementation timeline is expected to be as follows:

- Release in May 2024
- Enter into force in November 2024
- From January 2025, the standards will be integrated into implementation rules for CCC and will apply to new vehicle models
- From January 2026, the standards will apply to all vehicle models

F. Coordination with CCC Implementation

Further regulations are necessary to coordinate the implementation of these standards within the CCC framework. Critical considerations include evaluating compliance certificates for CSMS and SUMS with UN R155 and UN R156, as well as the preparations and resources required for validation testing. Ongoing monitoring of the development of supportive rules is essential.

III. Emerging Challenges under European Regulation

UNR155 represents a significant advancement in automotive cybersecurity, establishing stringent requirements that manufacturers must adhere to. With a phased implementation schedule and mandatory re-certification every three years [24], [25], this regulation ensures that new vehicles will be better equipped to handle cyber threats, fostering a safer and more secure automotive ecosystem.

One of the primary challenges for Original Equipment Manufacturer (OEM)s under UNR155 is communicating cybersecurity needs and instilling a cybersecurity mindset across the entire supply chain. This complex task demands a comprehensive approach to ensure all parties comprehend and implement cybersecurity measures. In this context, Road vehicles — Cybersecurity engineering (ISO-21434) [26] plays a crucial role in supporting OEMs by promoting cybersecurity awareness and practices. While ISO-21434 is an engineering standard and UNR155 is a regulation, designing systems according to the first one provides confidence that they follow the principles that align with the second one's requirements. A similar supportive role is fulfilled by Road vehicles — Software update engineering (ISO-24089) [27], which also complements the framework established by UNR155. These standards collectively form a robust structure for managing automotive cybersecurity.

Despite these comprehensive frameworks, significant challenges persist in the vulnerability disclosure process. When vulnerabilities are identified, it is critical to efficiently disseminate accurate information to OEMs and suppliers to enable them to assess the impact and severity of the threat. However, this process is hindered because the complete vehicle architecture often remains undisclosed, and Threat Analysis and Risk Assessment (TARA) details are not uniformly shared across different entities.

Even though cybersecurity regulations in the automotive domain have been issued recently, ongoing discussions and proposals about changes, updates, and new topics continue. Some automotive suppliers are keen on obtaining a certification of organizational processes, responsibilities, and governance to treat risk associated with cyber threats to gain more autonomy and partially relieve OEMs of their responsibilities through the supply chain. This interest could potentially lead to regulatory updates in the future to accommodate it. Although UNR155 currently applies only to road vehicles (specifically types M and N) and trailers (specifically type O, in case fitted at least with one ECU), other categories, such as agricultural vehicles, are not covered. Likely, all vehicle categories will eventually be regulated, but it is uncertain whether UNR155 will be the framework used. For instance, the agricultural sector might prefer a different regulatory framework, such as the Cyber Resilience Act (CRA), instead of UNR155. However, vehicle categories M and N, currently governed by UNR155, are unlikely to be affected by CRA regulations.

Under UNR155, OEMs are solely responsible for the cybersecurity of the products they manufacture. They must also ensure attack resiliency for each subsystem within the product and guarantee that cybersecurity requirements are met throughout the supply chain.

The CRA is notable because it applies to many products. Under this framework, any manufacturer of systems containing digital elements must perform certification. Therefore, the entity that integrates all subsystems into the final product must ensure that the integration of all certified components remains secure. In a cyber incident, responsibility extends beyond the final manufacturer to include the suppliers.

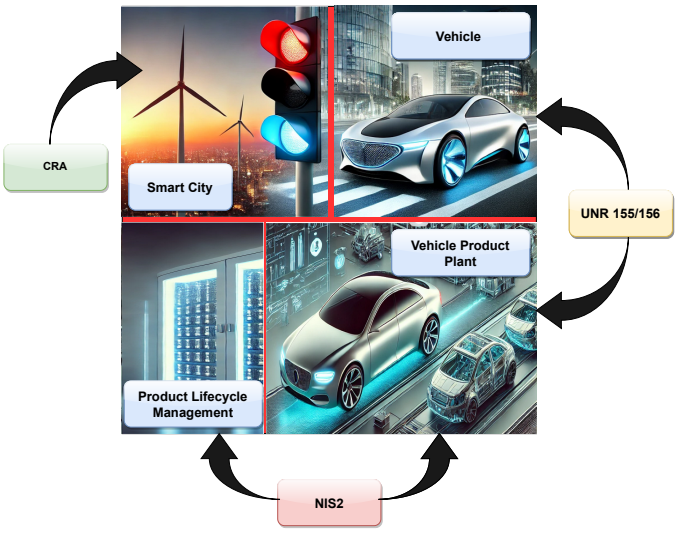

Fig. 2. The figure illustrates the impact of cybersecurity regulations (UNR-155, NIS2, UNR-156, and CRA) on the automotive industry and related sectors.

In situations where a system with digital elements is used in both automotive types M and N, covered under UNR155, and other domains regulated by the CRA, certain challenges

arise. Since several Electronic Control Modules (ECUs) are shared between automotive and other domains, these systems may be subject to requirements from both the vehicle manufacturer (under automotive regulations) and the CRA for other applications (see Figure 2). This necessitates managing the same product under two different governance frameworks simultaneously.

IV. Conclusion

As the automotive industry continues to evolve, cybersecurity is emerging as a fundamental aspect of automotive system value, surpassing even the systems' advanced features. This shift underscores the necessity to integrate cybersecurity from the very inception of the design process, adhering to the 'secure by design' principle. By incorporating security measures at the earliest stages of development, companies can significantly reduce costs and enhance the robustness of their systems.

Moreover, the dynamic nature of cyber threats requires a flexible and adaptive system architecture. This necessitates an agile organizational structure within companies to enable rapid responses to emerging threats. The automotive industry can better protect its assets and sustain consumer trust by fostering an environment that promotes swift adaptability and proactive security measures.

References

[1] K. Alyass, "Cars, gardens, and ruins: Making and remaking the motor city," *SAGE Journals*, 2024, this article reviews three books focusing on the long history and cultural legacy of auto production in Detroit. Available online: SAGE Journals.

[2] J. Battista, "Deindustrialization of detroit: The costs of movement," *Essays in Economic & Business History*, 2024, this article explores the deindustrialization of Detroit and its impact on the automotive industry. Available online: Essays in Economic & Business History.

[3] M. Perner, C. Wagner, and M. Gebhardt, "The key for future vehicles-development of chassis components according to cybersecurity regulations," Google Books, 2024, discusses the development of automotive components with cybersecurity regulations in mind, emphasizing the increasing vulnerability to cyber-attacks. Available online: Google Books.

[4] F. Jamal, "Driving the future: The impact of ai and cloud computing on the automotive industry," *LinkedIn*, 2024. [Online]. Available: https://www.linkedin.com/pulse/driving-future-impact-ai-cloud-computing-automotive-faisal-jamal-vdyee

[5] SYSGO, "Unveiling the role of edge-to-cloud technologies in automotive innovation," *SYSGO Blog*, 2024. [Online]. Available: https://www.sysgo.com/blog/article/unveiling-the-role-of-edge-to-cloud-technologies-in-automotive-innovation

[6] Salesforce, "As automotive sector embraces connected cars and generative ai, cybersecurity is a growing concern," *Salesforce News*, 2023. [Online]. Available: https://www.salesforce.com/news/stories/automotive-industry-security/

[7] J. Zheng, B. Du, H. Du, J. Kang, and D. Niyato, "Energy-efficient resource allocation in generative ai-aided secure semantic mobile networks," in *IEEE*, 2024, explores potential adversarial attacks on automotive market analysis and energy-efficient resource allocation. Available online: IEEE.

[8] S. Kong, K. Wang, C. Feng, and J. Wang, "Smart cities and transportation based vehicle-to-vehicle communication and cyber security analysis using machine learning model in 6g network," Springer, 2024, discusses machine learning models to combat cyber-attacks and address security concerns in contemporary automotive networks. Available online: Springer.

[9] H. Taherdoost, "Insights into cybercrime detection and response: A review of time factor," *MDPI*, 2024, reviews the necessity of minimizing response times for improved cybersecurity in automotive control networks. Available online: MDPI.

[10] A. Karahasanovic and P. Kleberger, "Adapting threat modeling methods for the automotive industry," *Academia.edu*, 2017.

[11] WirelessCar, "What are the greatest challenges of automotive cybersecurity and data privacy for connected cars?" *WirelessCar Blog*, 2023. [Online]. Available: https://www.wirelesscar.com/what-are-the-greatest-challenges-of-automotive-cybersecurity-and-data-privacy-for-connected-cars/

[12] G. Costantino, M. D. Vincenzi, and I. Matteucci, "A vehicle firmware security vulnerability: an ivi exploitation," Springer, 2024, highlights the rise in cyber-attacks on vehicles and the vulnerabilities in connected vehicles, particularly through infotainment systems. Available online: Springer.

[13] L. Moore, "Auto osint," Setu.ie, 2024, discusses the growing threat of cyber-attacks to automotive cybersecurity and the importance of timely information gathering. Available online: Setu.ie.

[14] O. Burkacky, "Cybersecurity in automotive," McKinsey Report, 2020, discusses trends, drivers, and defense strategies against cyber threats in the automotive industry. Available online: McKinsey Report.

[15] M. Singh and M. Singh, "Cybersecurity in automotive technology," Springer, 2021, discusses automotive cybersecurity challenges due to the increasing connectivity and autonomy of vehicles. Available online: Springer.

[16] S. Kim and R. Shrestha, "Introduction to automotive cybersecurity," Springer, 2020, examines the changes and opportunities in automotive cybersecurity due to digital transformation. Available online: Springer.

[17] F. Sommer, J. Dürrwang, and R. Kriesten, "Survey and classification of automotive security attacks," *MDPI*, 2019, reviews automotive security attacks, highlighting the increased attack surface due to connectivity.

[18] D. Nilsson and U. Larson, "A roadmap for securing vehicles against cyber attacks," ResearchGate, 2008, suggests designing security solutions for vehicles based on the defense-in-depth principle. Available online: ResearchGate.

[19] U. N. E. C. for Europe, "United nations regulation no. 155 (unr155): Cybersecurity and cyber security management system," 2021. [Online]. Available: https://unece.org/transportvehicle-regulations/wp29regulations2020-2024

[20] ——, "United nations regulation no. 156 (unr156): Software update management system," 2021. [Online]. Available: https://unece.org/transportvehicle-regulations/wp29regulations2020-2024

[21] E. Union, "Directive (eu) 2016/1148 on security of network and information systems (nis directive)," 2018. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[22] National Highway Traffic Safety Administration (NHTSA), "Cybersecurity Best Practices for Modern Vehicles," 2022. [Online]. Available: https://www.nhtsa.gov

[23] China Automotive Technology and Research Center Co., Ltd (CARTAC), "Technical Committee on Intelligent and Connected Vehicles Review," 2023, technical review of standards on vehicle cybersecurity and data storage systems. [Online]. Available: https://www.cartac.com.cn

[24] "Un regulation no 155 – uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system," EUR-Lex - Access to European Union Law, 2021, available online: https://eur-lex.europa.eu.

[25] M. Sandler, "Un regulation no 155: What you need to know about un r155," *Cyres Consulting Blog*, June 2022, available online: https://www.cyres-consulting.com.

[26] "Road vehicles — Cybersecurity engineering (ISO21434)," International Organization for Standardization, 2021. [Online]. Available: https://www.iso.org/standard/70918.html

[27] "Information and documentation – Archives/records management (ISO24089)," International Organization for Standardization, 2020. [Online]. Available: https://www.iso.org/standard/73339.html