ISSN: 2664-9640

Research on the Status Quo of Cybersecurity Laws and Standards of ICV

Xia Liu[1, a], Jinchao Zhang[1,b], Yihong Qin[1,c], Baizheng Wang[1,d]

[1]CATARC Software Testing (Tianjin)Co.,Ltd., Tianjin 300300, China

[a]castc_liuxia@163.com, [b]zhangjinchao@catarc.ac.cn, [c]qinyihong@catarc.ac.cn, [d]wangbaizheng@catarc.ac.cn

Abstract

In 2015, Fiat Chrysler recalled 1.4 million vehicles due to cyber security problems, which triggered the global attention to the cyber security of intelligent connected vehicles (ICV). With the rapid development of ICV, people will face more and more vehicle cyber security risks, these risks will affect the property security, privacy security and personal safety of users, and even may cause social and national harm. This paper introduces the development background of ICV industry, reviews the current situation of laws, regulations and standards related to ICV cyber security at home and abroad, and finally puts forward the development trend and suggestions of ICV.

Keywords

Intelligent Connected Vehicle,Cybersecurity,Laws and Standards.

1. Introduction

With the popularization of the new four technologies (Electrified, Connected, Intelligent and Sharing) of ICV, people are facing many incidents caused by vehicle cybersecurity issues while enjoying convenience. According to the latest report of Upstream [1], since 2010, there have been more than 900 incidents of cyber security attacks against ICVs reported publicly, and the number of incidents in 2021 alone has increased by more than 225% compared with 2018.

Governments and industries of all countries attach great importance to this. Developed countries and regions such as Europe, the United States and Japan have carried out a series of research work and industry layout on the cybersecurity of ICVs.Since 2015, China has actively promoted information security research in the relevant industries of ICV. From laws, regulations, policies, standards, industry reports to consulting, testing, certification, and products, an industrial chain development trend has been gradually formed, which is led by the government and industry alliance, and actively promoted by vehicle cybersecurity enterprises [2].

2. Status quo of ICV Cybersecurity Laws and Regulations

2.1. Foreign Laws and Regulations Related to ICV Cybersecurity.

In recent years, many countries around the world have promulgated relevant laws and regulations to strictly regulate and guide issues related to the ICV cybersecurity. At the planning and strategic level, the United States has supported the development of technologies and industries related to ICVs through the implementation of the "Intelligent Transportation System (ITS)" project since the early 1990s.

In 2016, the National Highway Traffic Safety Administration （NHTSA） put forward the Cybersecurity Best Practices for Modern Vehicles, which guides the enterprises to improve the vehicle cybersecurity internally, helps manufacturers and other stakeholders to mitigate

ISSN: 2664-9640

cybersecurity risks based on risk management methods, and puts forward seven specific suggestions[3]. The new version was released in September 2022, which is an update of the 2016 version, taking full account of the current standards and research content related to cybersecurity in the automotive industry.

In May 2017, Germany issued the first law on intelligent vehicle, the Road Traffic Act (Eighth Amendment), which initially cleared the legal obstacles for intelligent vehicle to land in Germany [4].

In August 2017, the British government released the Key Principles of Cyber Security for Connected and Automated Vehicles, which are divided into eight principles, and run through the entire vehicle industry, Connected-Automated Vehicle (CAV), ITS and their supply chains.

In May 2018, the General Data Protection Regulation(GDPR) issued by the European Union officially came into force in member countries. The regulation's protection and supervision of personal information has reached an unprecedented height, which can be called the most stringent data protection act in history. Violators will be required to submit a huge fine.

In June 2020, the United Nations World Forum for Harmonization of Vehicle Regulations (UN/WP. 29) released three regulations related to ICVs. They are UN Regulation No.155-cyber security and cyber security management system, UN Regulation No.156-software update and software updates management system, and UN Regulation No.157-Automated Lane Keeping Systems. R155 is the world's first mandatory regulation on automotive information security, and its content framework is shown in Figure 1 [5].

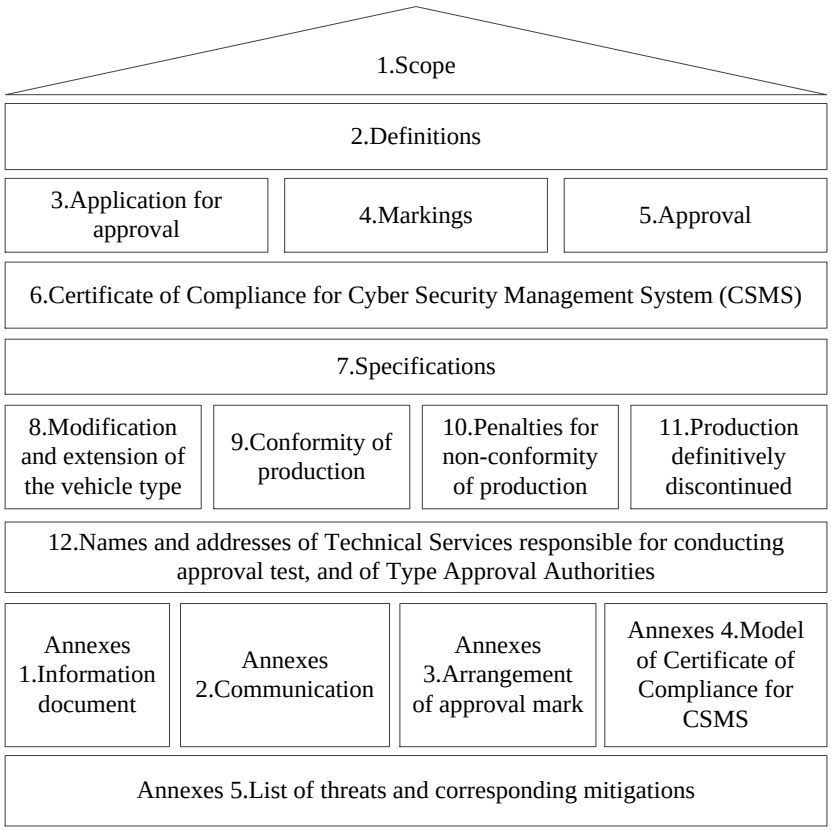

Fig. 1 R155 Framework

2.2. Laws Related to ICV Cyber Security in China.

As a mobile information carrier that can communicate in real time, ICV involves many public privacy and important national information, such as user privacy information, national geographic location information, road distribution, network distribution of communication

ISSN: 2664-9640

operators, etc. in today's big data era. Once obtained and used by criminals, these data may become a social hazard or even a national security problem.

On July 1, 2015, the 15th session of the Standing Committee of the 12th National People's Congress(the NPC Standing Committee) adopted the National Security Law of the People's Republic of China(PRC), which clarifies the security tasks of the state in 11 fields and proposes that the state build a network and information security guarantee system to improve the capacity of network and information security protection. We will ensure the security and controllability of core network and information technologies, key infrastructure, and information systems and data in important fields.

To ensure cyber security, the 24th Session of the 12th NPC Standing Committee of the PRC adopted the Cyber Security Law of the People's Republic of China on November 7, 2016, which is a law designed to safeguard sovereignty and national security in cyberspace, social and public interests, protect the legitimate rights and interests of citizens, legal persons and other organizations, , and promote the healthy development of economic and social informatization.

In order to regulate the application and management of cryptography, promote the development of cryptography, and ensure network and cyber security, the 14th session of the 13th NPC Standing Committee of the PRC adopted a comprehensive and fundamental law in the field of cryptography, namely Cryptography Law of the People's Republic of China, on October 26, 2019.

The Data Security Law of the People's Republic of China, adopted at the 29th session of 13th NPC Standing Committee of the PRC on June 10, 2021, includes provisions related to vehicle cyber security, and sets forth requirements for the development, research, risk monitoring, processing, collection and trading of ICV data activities.

2.3. Regulations and Rules Related to ICV Cyber Security in China.

In May 2015, The State Council issued "Made in China 2025", in which the car was classified as one of the ten "breakthrough development in key areas of strong push", which clearly put forward the development direction of low-carbon vehicle, informatization and intelligent, and will link intelligent cyber vehicles and energy-saving vehicles, China will master the overall technology and key technologies of automatic driving. It is necessary to establish a relatively complete independent research and development system, production supporting system and industrial cluster of ICVs, and basically complete the transformation and upgrading of the vehicle industry [6]. In order to fully implement "Made in China 2025", promote the transformation and upgrading of related industries, vigorously foster new drivers, and give full play to the top-level design and leading role of standards in the ecological environment construction of the Internet of Vehicles industry, the Ministry of Industry and Information Technology (MIIT) and Standardization Administration of the People's Republic of China (SAC) jointly organized the formulation of a series of documents titled "Guidelines for the Construction of National Internet of Vehicles Industry Standard System". Among them, the National Industrial Standard System Construction Guide for Internet of Vehicles (Intelligent Connected Vehicles) was revised and improved in 2022, and its content framework is shown in Figure 2.

For China's vehicle industry, 2025 is a key year. Eleven ministries and commissions, including the National Development and Reform Commission, the MIIT, and the Ministry of Science and Technology, jointly issued the Intelligent Vehicle Innovation and Development Strategy, which proposes that by 2025, China's standard intelligent vehicle technology innovation, industry dynamics, infrastructure, regulations and standards, product supervision and cybersecurity systems will be basically formed [7]. The MIIT issued the Guidelines for the Construction of Internet of Vehicles Network Security and Data Security Standard System, proposing to form a

ISSN: 2664-9640

relatively complete Internet of Vehicles(IoVs) cyber security and data security standard system by 2025.

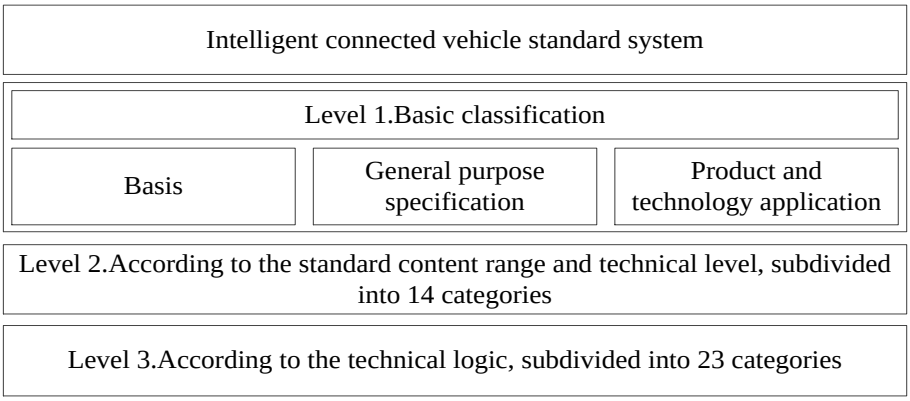

Fig. 2 ICV standard system framework

3. Status quo of ICV Cybersecurity Standard

3.1. Foreign Standards and Specifications Related to ICV Cybersecurity.

The Society of Automotive Engineers(SAE) took in launching cybersecurity-related standard SAE J3061_202112 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems in 2016 [8]. The standard provides a process framework and guidance for vehicle cybersecurity throughout the vehicle life cycle, from concept to production, operation, maintenance and obsolescence. The standard has been updated in 2021 to replace the 2016 version. ISO/SAE 21434-2021 Road vehicles - Cybersecurity engineering based on SAE J3061 provides an cybersecurity framework for the vehicle industry [9]. Refer to the V-shaped model development process, mainly from the risk assessment management, product development, operation or maintenance, process audit and other four aspects to ensure the development of vehicle cybersecurity engineering work. British Standards Institute(BSI) issued ISO/PAS 5112-2022 Road vehicles - Guidelines for auditing cybersecurity engineering, applied to the vehicle field in the construction of cybersecurity management system, support ISO/SAE 21434 audit. BS PAS 1885-2018 The fundamental principles of automotive cyber security aims to set an industry standard for organizations working on autonomous vehicle technology. This standard will help all parties in the vehicle lifecycle and ecosystem better understand how to improve and maintain vehicle cyber security and the safety of intelligent transportation systems [10]. This makes the UK the first country to publish such standards.

Verband der Automobilindustrie (VDA) launched the updated version of Information Security Assessment(VDA-ISA) Trusted Information Security Assessment Exchange(TISAX) at the end of 2017. TISAX involves authorized audit services, automotive oems, and numerous suppliers (service providers), as well as potentially interested third parties. It mainly consists of general cybersecurity requirements, prototype protection, third party contact and data protection.

3.2. Standard System Related to ICV Cyber Security in China.

Subcommittee 34 on Intelligent and Connected Vehicle of National Technical Committee 114 on Road Vehicles of Standardization Administration of China(SAC/TC114/SC34) is responsible for the construction of national standards related to vehicle cyber security. At present, four standards have been implemented on May 1, 2022. Table 1 shows the progress of some standards related to vehicle cyber security.

ISSN: 2664-9640

Table 1 Progress of TC114 ICV cyber security related standards

Number	Standard name	Standard state
1	GB/T 40855-2021 Technical requirements and test methods for cybersecurity of remote service and management system for electric vehicles	Implementation
2	GB/T 40856-2021 Technical requirements and test methods for cybersecurity of on-board information interactive system	Implementation
3	GB/T 40857-2021 Technical Requirements and Test Methods for Cybersecurity of Vehicle Gateway	Implementation
4	GB/T 40861-2021 General Technical Requirements for Vehicle Cybersecurity	Implementation
5	GB/T 41578-2022 Technical Requirements and Test Methods for Cybersecurity of Electric Vehicle Charging System	Release
6	Technical requirements for Vehicle Cybersecurity	Soliciting opinions
7	General technical requirements for software update of vehicles	Soliciting opinions
8	Cybersecurity requirements for vehicle diagnostic interface	Soliciting opinions
9	Intelligent and connected vehicles — General requirement of data	Soliciting opinions
10	GB 15740 Protective device against unauthorized use of motor vehicles	Soliciting opinions
11	Vehicles Cybersecurity incident response management guideline	Submit to TC for approva
12	Intelligent and Connected Vehicle--Terms and Definitions	Submit to the competent authority for approval

National Technical Committee 260 on Information Technology Security of Standardization Administration of China（SAC/TC260）is a technical organization engaged in information security standardization within the professional field of information security technology. To be responsible for organizing and carrying out standardization technical work related to domestic information security. Table 2 shows the progress of some standards related to vehicle cyber security.

Table 2 Progress of TC260 ICV cyber security related standards

Number	Standard name	Standard state
1	GB/T 38628-2020 Information Security Technology — Cybersecurity Guide for Automotive Electronics Systems	Implementation

ISSN: 2664-9640

2	GB/T 41871-2022 Information security technology-Security requirements for processing of motor vehicle data	Release
3	Information security technology-Security requirements for automotive electronic chips	In research

National Technical Committee 485 on Communication of Standardization Administration of China（SAC/TC485) is under the supervision of the Standardization Administration, with the MIIT as the operational guidance unit. China Communication Standardization Association (CCSA) as the secretariat to undertake the unit. Table 3 shows the progress of some standards related to vehicle cyber security.

Table 3 Progress of TC485 ICV cyber security related standards

Number	Standard name	Standard state
1	YD/T3751-2020 Technology specification for data security of Internet of vehicle information service	Implementation
2	YD/T3746-2020 Specification of Internet of vehicle information service- User personal information protection	Implementation
3	YD/T 3752-2020 Technology specification of Internet of vehicle information service platform security	Implementation
4	YD/T 3750-2020 Security guideline of Internet of vehicle wireless communication	Implementation
5	YD/T3594-2019 General technical requirements of Security for Vehicular Communication based on LTE	Implementation

In order to meet the development needs of standardization in the field of cryptography and carry out standardization work in the field of cryptography, the Cryptography Standardization Technical Committee (CSTC) was established in October 2011 with the approval of the Standardization Administration and the National Cryptography Administration.

Including random number, cryptography algorithm SM2, SM3, SM4 related detection, cryptography protocol including SS, IPSec and corresponding gateway detection, related to the cryptography module detection technology and detection specifications, as well as information system cryptography application detection specifications.

In addition, some of the standards put together by the Ministry of Ecology and Environment (MEE) are related to vehicle cyber security. GB 17691-2018 puts the cyber security test of heavy-duty diesel vehicles' on-board terminals into the standard for the first time. It describes the cyber security requirements of on-board terminals that meet National Standard VI, such as: intrusion detection, proper use of asymmetric encryption algorithm, normal on-board terminals sending messages and receiving instructions, as shown in Table 4 [11].

ISSN: 2664-9640

Table 4 Progress of MEE ICV cyber security related standards

Number	Standard name	Standard state
1	GB 17691-2018 Limits and measurement methods for emissions from diesel fuelled heavy-duty vehicles(CHINA VI) Appendix Q.4 Security Strategy	Implementation
2	HJ 1014-2020 Emissions control technical requirements of non-road diesel mobile machinery Appendix H Technical requirements for On-board terminal	Implementation
3	HJ 1239.1-2021 Technical specification for emission remote supervision system of heavy-duty vehicles PART1 On-board terminal Appendix B Data Security	Implementation

4. Development trend and suggestions of ICV Cyber Security

Establish the ICV cyber security basis to guide it related enterprises to accurately master the development progress, focus and weakness of vehicle cyber security and testing technology, scientifically measure the comprehensive development level of Chinese vehicle cyber security, and strengthen the statistical analysis of the application of IoV security. Support government departments to accurately grasp the development trend and law of IoV safety, accurately judge the contribution of it safety development to the transformation and upgrading of the vehicle industry, and timely grasp the operation of the national economy, so as to provide reference for the formulation and implementation of highly targeted and operable industrial policies. In order to form a good industrial ecology, timely guide relevant enterprises to carry out supply and demand docking and technical capacity coordination, and rapidly promote industrial development.

While learning from the experience of relevant international laws and regulations, combined with the industry characteristics and technical attributes of ICV cyber security, to promote the formulation and implementation of China's vehicle cyber security policies and regulations. In addition, based on the basic content of ICV cyber security to coordinate the development of relevant national and organization standards, and provide overall standardization support for the development of vehicle cyber security industry.

References

[1] Upstream. Global Automotive Cybersecurity Report, 2022.

[2] China Industry Innovation Alliance for the Intelligent and Connected Vehicles. Intelligent Connected Vehicle Cybersecurity Evaluation White Paper, 2019.

[3] T.L. Zhang and Y.Y. Jiang. Review of Intelligent Vehicle Legislation and Revision of Road Traffic Law in Germany, Deutschland-Studien, vol. 3 (2017), p. 68-80.

[4] National Highway Traffic Safety Administration. Cybersecurity Best Practices for Modern Vehicles, 2022.

[5] UN/WP29. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021.

[6] Information on http://www.gov.cn

[7] National Development and Reform Commission, Ministry of Industry and Information Technology, and Ministry of Science and Technology, et al. Intelligent Vehicle Innovation and Development Strategy, 2020.

ISSN: 2664-9640

[8] Vehicle Electrical System Security Committee. SAE J3061—2016 cybersecurity guidebook for cyber-physical automotive systems, 2016.

[9] International Organization for Standardization. ISO/SAE 21434-2021 Road vehicles - Cybersecurity engineering, 2021.

[10] British Standards Institute. PAS 1885-2018 The fundamental principles of automotive cyber security, 2018.

[11] Ministry of Ecology and Environment. GB 17691-2018 Limits and measurement methods for emissions from diesel fuelled heavy-duty vehicles(CHINA VI), 2018.