DOI 10.15302/J-SSCAE-2019.03.006

Implementation Countermeasures for Information Security Management of Intelligent Connected Vehicles

Zhao Shijia[1], **Xu Ke**[1], **Xue Xiaoqing**[2 3], **Qiao Yingjun**[4]

1. Ministry of Industry and Information Technology Equipment Industry Development Center, Beijing 100846, China
2. China Software Test Center, Beijing 100048, China
3. School of Vehicle and Mobility, Tsinghua University, Beijing 100084, China
4. Center for Strategic Studies, CAE, Beijing 100088, China

Abstract: Industrial development has accelerated the integration of modern technology within the automotive field. Intelligent connected vehicles (ICVs) provide consumers with convenient transportation and a safe driving environment. At the same time, however, multiple risks are brought about with respect to information security by intelligentization and networking. In recent years, hacker attacks have become more and more frequent. Indeed, this is problematic since comprised information security not only affects driving safety and user data, but national security as well. Accordingly, information security issues have attracted attention from governments all over the world, with developed countries, such as the United States, Europe, and Japan, taking actions to safeguard information security. In this context, China should promote the development and management of information security with respect to ICVs, taking appropriate active measures in the process.

Keywords: intelligent connected vehicles; information security; automotive industry; management

1 Introduction

With the advent of the smart digital age, intelligent connected vehicles (ICVs) are becoming increasingly integrated in the automotive industry. Accordingly, automobiles are no longer isolated units, but important carriers and nodes for intelligent transportation, intelligent energy, and smart city. In essence, they are mobile intelligent network terminals. With the development of artificial intelligence, information and communication technology, and cross-border integration, the means of interaction between ICV and the outside are constantly enriched. With the integration of ICVs, problems inevitably arise with respect to information security. In 2015, two hackers appropriated the remote control of a Cherokee and, using the Uconnect vehicle system, took control of the vehicle. Fiat Chrysler recalled the 1.4 million cars affected in the United States, which was the first vehicle-recall incident in the world. The National Highway Traffic Safety Administration (NHTSA) was highly concerned about this incident and worked alongside Chrysler to solve the problem. Moreover, in 2016, vulnerabilities associated with the service security of the Nissan Leaf were brought to light, and, in 2017, loop holes were exposed in the remote information-processing control units of enterprises such as Ford, BMW, Infiniti, and Nissan. Indeed, it is becoming more and more difficult to predict, and protect users from, malicious ICV attacks.

ICV information-security threats endanger personal privacy and can result in economic losses; moreover, they can result in more serious consequences, such as vehicle destruction, death, and national public-security problems

Received date: May 6, 2019; **Revised date:** May 9, 2019

Corresponding author: Qiao Yingjun, engineer from Center for Strategic Studies, Chinese Academy of Engineering. Major research field is automotive development strategy. E-mail: qiaoyj@cae.com

Chinese version: Strategic Study of CAE 2019, 21 (3): 108–113

Cited item: Zhao Shijia. Implementation Countermeasures for Information Security Management of Intelligent Connected Vehicles. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2019.03.006

[1,2]. According to the Ponemon Institute, an independent research institute in the United States, 60%–70% of vehicles will be recalled due to information-security vulnerabilities in the future. In other words, the threat of information-security attacks with respect to ICVs is gradually increasing [3]. Accordingly, ICV information security has become the main focus of the automotive industry, as well as society in general. For instance, according to statistics, 56% of consumers said that information security and privacy protection are the main factors taken into account when buying vehicles [4].

At present, automotive electrification, intellectualization, networking, and sharing are important developmental trends in the global automotive industry. Accordingly, developed countries as well as multinational automotive enterprises are increasingly developing, and investing in, ICVs. Moreover, China is currently concerned with ICV development, regarding it as an important breakthrough in the construction of a powerful automotive country [5]. However, if said developments are to take place, then China urgently needs to upgrade its automotive information security and align it with national network security; moreover, it must attach importance to the associated information-security risks, accelerate the research and development (and application) of relevant information-security technology, establish standards and regulations, formulate corresponding test specifications, effectively realize the coordination mechanism, and achieve the all-round development of safety protections.

2 ICVs face multiple information-security risks

At present, the information-security risks associated with ICVs mainly come from "cloud–pipe–end–external links"; that is, cloud platforms, network transmissions, vehicles and associated external devices, as shown in Fig. 1.

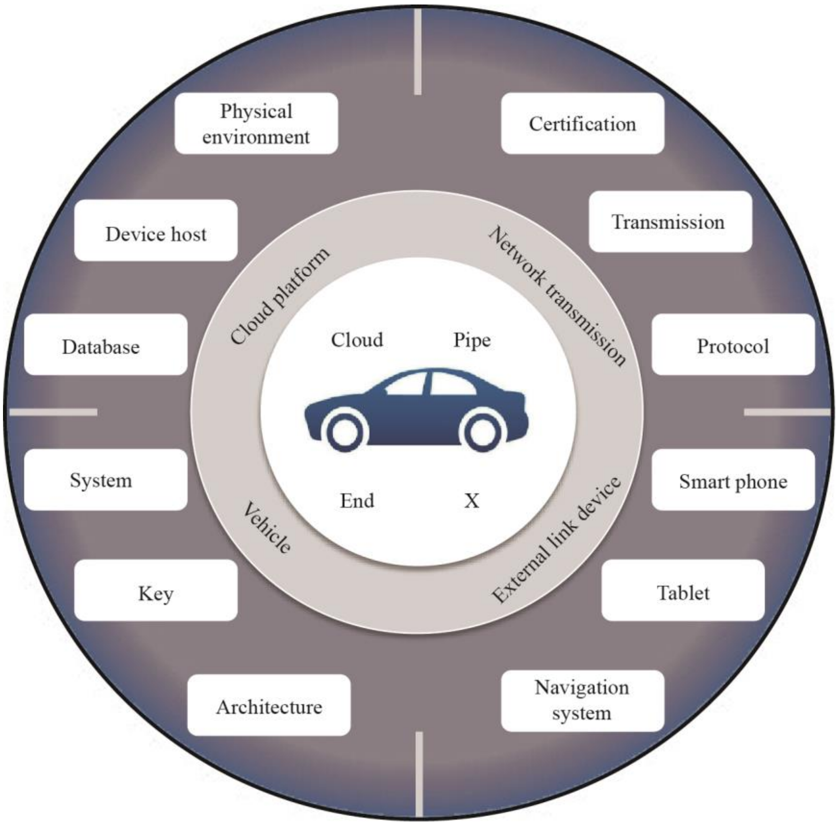

Fig. 1. ICV information-security risk architecture.

2.1 Vehicle-safety risk

The vehicle is mainly regarded as an intelligent terminal in the system. As the level of ICV intelligentization and networking increases, the number of associated information-security problems also increases. These are outlined below.

The first problem is associated with system security, which itself consists of software and hardware security. On the one hand, with software gradually being incorporated into more and more vehicles, software security faces increasing risk challenges, such as over the air (OTA) upgrading. On the other hand, hardware security is associated with autonomous driving and automatic-cruise systems; therefore, by interfering with the millimeter-wave radar,

DOI 10.15302/J-SSCAE-2019.03.006

hackers can interfere with the vehicle or take control by virtue of an ultrasonic device used to send ultrasonic waves of the same cycle and frequency.

The second problem is associated with key security. Data encryption is usually used to protect data privacy. Once the key is compromised, the encrypted data is no longer secure. For example, by recording the car key signal, door opening can be realized. More specifically, the attacker in question obtains the control information and then reversely analyzes it by instrumentation debugging, thereby obtaining the control flow and using the script to control the vehicle through the Bluetooth key.

The third problem is associated with architecture security. The relatively closed network environment inside the vehicle is vulnerable to attack. Moreover, since ICV defense abilities are weak against external attacks, many features are also vulnerable, such as the on-board diagnostics (OBD) interface, the Media Oriented Systems Transport bus, the Controller Area Network (CAN) bus, the Local Interconnect Network bus, and the tire-pressure monitoring system [6]. For instance, since the CAN bus uses a clear-text communication mechanism, the relevant electronic control unit can be controlled by attacking the CAN network, which would result in serious consequences.

2.2 Cloud-platform security risk

The cloud platform is an important part of ICVs, the functions of which are becoming increasingly more comprehensive and complicated. These include the following: providing entertainment services, remote diagnosis of faults to remotely control vehicle, OTA upgrading, and information services underlying vehicle control. The security of the cloud platform mainly includes the physical environment, device host, interface, database, and application security. Accordingly, the cloud platform has a variety of protection mechanisms, such as virus protection, access-control protection, and data-security protection, which prevent the loss and theft of cloud data. At present, the majority of vehicle network data is stored using distributed technology. The main security threats include the access, stealing and tampering of sensitive data by hackers. These must be addressed since, in the future, the cloud will responsible for tracking and managing vehicles across the fleet. According to QYResearch, by 2024, 30% of vehicles sold will be equipped with network-security cloud services, the revenue of which will reach $558 million. Indeed, with the continuous development of ICVs, associated data-security and access-control threats will gradually increase. Accordingly, attention must be given to the relevant security risks of the cloud platform.

2.3 Network-transmission security risk

V2X refers to the external communication connection involved in ICVs, which is mainly based on Long Term Evolution and 5G. At present, the government is also increasing efforts to promote the development of communication technologies and standards. At the same time, dedicated short-rage communication, as a mature technology, has its own advantages with respect to vehicles communication. The security of communication mainly includes maintaining communication integrity, ensuring that sent and received messages are legitimate and not illegally tampered with, preventing camouflage attacks, man-in-the-middle attacks, and flood attacks, as well as ensuring the performance and availability of communications.

There are three major security problems involved network transmissions. The first problem is associated with authentication risks, wherein hackers steal information by identity forgery and dynamic hijacking. The second problem is associated with transmissions risks, wherein vehicle transmission information is vulnerable to attack if it is not sufficiently encrypted. The third problem is associated with agreement risks, wherein malicious protocol masquerades as legitimate protocol. Obviously, these three risks are interconnected. For example, since communications at the protocol link layer are not encrypted, vehicle positioning can be hijacked by grabbing the link-layer identifier. With respect to automatic driving, the car formulates the driving route according to the V2X communication content, and the attacker induces the vehicle through a pseudo message. Misjudgment occurs accordingly and affects vehicle control [7].

2.4 External-link-device security risk

With the increasing functions of ICV, the frequent access to vehicles by external components will bring new security risks. Indeed, consumers are at risk of external virus-intrusion attacks when purchasing and installing externally linked products for their vehicles. First of all, portable devices are mixed with a large number of imitation products and malicious code applications. These outreach device components are cheap but have insufficient security-protection capabilities. Secondly, the charging piles of vehicles have security risks. For example, the charging-pile control module is connected to the management system through an Ethernet. Accordingly, there is no protection inside the network and it can be hijacked through the Internet, where the charging voltage and charging amount can be tampered with. At the same time, charging apps related to mobile payment can be hijacked by means of a Trojan in the mobile phone, which can result in stolen information, among other things. Indeed, the existing vehicle design does not sufficiently consider information security, such as OBD boxes and car machines in the aftermarket, which results in potential risks. In summary, in the vehicle research and development process, automotive companies must focus on information-security attacks caused by external devices [9].

3 Countries strengthen ICV information-security management

The hidden dangers of ICVs have grabbed the attention of world governments. The United States, Europe, and Japan and other countries and regions are actively promoting the formulation of relevant standards and technical norms with respect to information security, thereby accelerating the formation of ICV information-security management requirements.

3.1 US develops comprehensive information-security regulations

The United States has raised automobile information security to the level of national security. The relevant government departments are guiding the industry to speed up the development of information security by formulating policies, promoting legislation, and issuing safety practices. In terms of policy, in September of 2016, the NHTSA officially issued the *Federal Automated Vehicles Policy*. The HAV evaluation includes 15 safety performance items, including privacy, vehicle network security and associated content. In terms of regulations, in March of 2017, the United States Congress passed the *Safety and Privacy in Your Car Study Act*, instructing the NHTSA to enact regulations for motor-vehicle network security, wherein a requirement was set that motor vehicles sold in the United States must prevent unauthorized intrusion, including electronic control, driving data, and data-transmission security. The United States House of Representatives passed the *Future Deployment and Research Safety Act*, requiring automotive companies to develop detailed network-security plans. This prevents automotive companies from manufacturing, selling, or importing intelligent networked automotive systems and vehicles if they have not developed the requisite plans. In terms of standards, the United States took the lead in formulating SAE J3061 *Automotive System Network Security Guidelines* and other standards based on ISO 26262, covering the level of automobile information-security integrity, testing methods, and testing tools in order to ensure that automobiles have effective information-security protection, as well as to provide relevant suggestions for automotive enterprises and automotive-parts suppliers. At the same time, SAE and ISO/TC22 Road Vehicle Technical Committee of the United States set up a working group on automobile information security to formalize international standards and regulations at the ISO level. In 2016, the NHTSA released the *Best Practices of Modern Automobile Information Security*, which addresses the rapid development of intelligent networks in the field of automobile information-security and privacy protection. Indeed, the automotive industry is currently strengthening its information-security protection mechanisms through various means. Moreover, many automotive enterprises, such as General Motors and Tesla, are addressing the associated problems by openly recruiting security personnel or cooperating with security agencies.

3.2 Europe enhances the safety of automotive parts and network communication

The European Network and Information Security Agency has marked ICVs as important with respect to the Internet of Things (IoT) security. At the same time, since 2008, Europe has carried out a number of projects, such as the E-Safety Vehicle Intrusion Protected Application (EVITA) project, the Open Vehicular Secure Platform project, and the Preparing Secure Vehicle-to-X Communication Systems project. Herein, technical specifications and solutions are put forward from aspects of automotive hardware security, network transmission, and communication security. Due to these projects, some technical achievements have been industrialized. For example, the EVITA project provides information "attack" scenarios for automobile network security. Volvo and Chalmers University of Technology cooperated with the Healing Vulnerabilities to Enhance Software Security and Safety project to conduct network risk assessment. Moreover, the Continental Group acquired Argus, an Israeli security company, with a view to further strengthen and improve its vehicle network-security capabilities. Cerberus, a British company, has developed RISC V open source core and customized encryption and password management units to design security chips, which improves the network security defense capabilities of driverless vehicles and IoT devices. In addition, the European Telecommunication Standards Association has formulated a series of information security standards for intelligent transport systems (ITS), including service security and communication security architecture, in order to strengthen the standardization and guidance of the development of information security for ITS.

DOI 10.15302/J-SSCAE-2019.03.006

3.3 Japan carries out vehicle lifecycle information security protection measures

Japan's Network Security Strategy clearly includes automobiles in the field of IoT system security. From the point of view of automobile reliability, Japan's Information Technology Promotion Agency (IPA) defines the automobile information security model by analyzing the possible means of attacking automobile security. The threats to information security include accidental threats caused by user error and malicious threats caused by attackers. In order to address these threats, information encryption is proposed to determine the legitimacy of user programs, as well as to access control management and policies associated with user rights and communication [10]. At the same time, the IPA has formulated a safety management policy in accordance with ICV life cycle. The design stage implements budget allocation according to the importance of various functions with respect to safety. The development stage adopts a security code against loopholes according to the relevant coding standard, establishes a contact feedback mechanism for consumers to respond to information security in the use stage, and provides an information deletion function in the abandonment stage. This is shown in Fig. 2. Moreover, Risa Electronics Japan launched the Automotive Functional Safety and Network Safety Support Plan, which contributes to the realization of driver safety by simplifying the design complexity of sophisticated automotive systems.

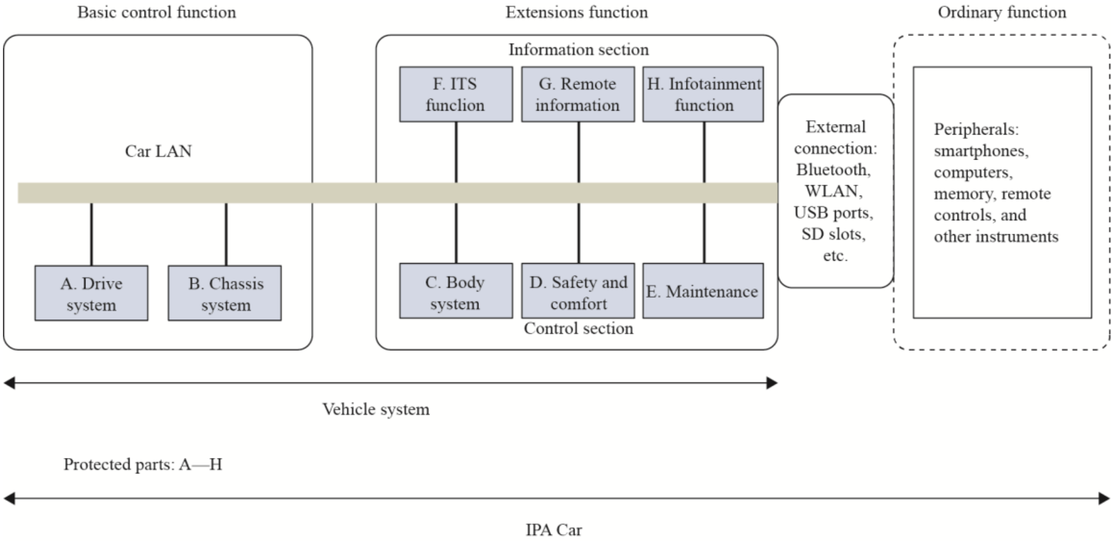

Fig. 2. Japan automotive information-security model IPA car [10].

4 Implementing countermeasures for ICV information security management in China

In recent years, with the frequent occurrence of information security incidents, the Chinese government has gradually strengthened the protection of information security. Accordingly, policy support has been continuously improved. Moreover, network security has become the key construction direction of the 13th Five-Year Plan. Several policies, such as the *National Network Space Security Strategy* and the *Guidance Catalogue of Key Products and Services in Strategic Emerging Industries*, have been implemented to accelerate the demand for information security products. Moreover, the implementation of the *Network Security Law* has further developed network security. Indeed, China's information security industry has been expanding for a number of years, increasing from 15.726 billion yuan in 2012 to 34.172 billion yuan in 2016, with an average annual compound growth rate of 21.41% over five years.

In April 2016, the sub-technical committee of ICVs under the National Automobile Standardization Technical Committee established the Working Group on Automobile Information Security, which is responsible for furthering international standardizations and formulating a standard system of domestic ICV information security. Indeed, the medium-term and long-term development plan of the automobile industry takes ICV information security as an important goal. However, in China, awareness of information security in the automotive industry is still immature. Accordingly, associated demand is currently unclear and the security protection abilities are weak; moreover, the technical requirements and evaluation system of the Intelligent Network Auto Information Security is imperfect; specifically, it does not provide effective guidance for enterprises, nor does it effectively control the quality of products and services. Due to the lack of standardized safety supervision standards and testing processes, the information security management of ICVs is imperfect and, accordingly, it is unable to predict and identify information security risks.

In summary, China urgently needs to strengthen its information security management with respect to ICVs.

4.1 Promoting the development and application of ICV information security technology

The development of ICVs has resulted in new requirements for information security technology. In addition to basic security function requirements, such as defending against network attacks, detecting scanning software vulnerabilities, preventing data tampering, and detecting abnormal behavior in real time, special requirements for vehicle functions are being implemented, including driving safety assurances, vehicle information interaction guarantees, and privacy and information security guarantees. Since traditional vehicles are relatively closed systems, their design is mainly concerned with real-time and functional safety, with less focus placed on information security. However, with the development of vehicle intelligence and networking, the information security field has generated vehicle-related threat risks. Therefore, for the future protection of intelligent network information, it is necessary to consider the addition of information security elements, from design and development to production, as well as to establish a closed loop for information security in order to improve the information security protection capabilities of ICVs. These are further explained below.

First, the top-level design should be strengthened. In order to do this, governments should standardize and guide the industry in formulating policies and issuing guidelines, as well as in establishing an intelligent network-linked automotive information security protection system; moreover, they should support the development and promotion of associated technologies, set up projects, and emphasize departmental collaboration for technical breakthroughs.

Second, intelligent information security protection mechanisms should be strengthened across the entire ICV lifecycle. In order to do this, innovations must be made, such as key chips, software, communication protocols, and system applications; moreover, security and controls should be improved, which includes developing chip encryption technology. Indeed, at the state-level and the enterprise-level for remote monitoring platforms, an information security monitoring module must be introduced as soon as possible in order to conduct real-time monitoring and detect early security risks. These include vehicle and external-link devices, suppressing the spread of malicious attacks on the internal networks, and reporting loopholes or attacks in a timely manner. Indeed, we must not only address security vulnerabilities, but focus on eliminating secondary threats as well.

Third, it is important to collect domestic and international network security incidents and tools, as well as to summarize intelligent network information security issues, and guide front-end enterprises to explore feasible solutions; moreover, the collection and analysis of personal credit records must be strengthened while reducing illegal and untrustworthy behavior and the possibility of attacks. Finally, it is important to build an intelligent network-connected automobile basic-data interaction-management platform, which would promote real-time access to ICV information and service provider platforms, as well as ensure the reliability and stability of supervision services.

4.2 Establishing ICV information security standards and regulations

Since ICV information security is an emerging field, the regulatory bodies are yet to issue corresponding laws, regulations, and procedures. Although the *Network Security Law* has been enacted, the lack of interpretation and detailed rules for industry segments has, in turn, resulted in a lack of legal basis and protection mechanisms for the regulatory measures. Indeed, China should take into account the experiences of the West in developing its automotive information security standards and regulations. The actions that China must take are outlined below.

First, China should strengthen ICV information security legislation, clarify the requirements for automobile enterprises and parts enterprises under the information security framework, and clarify appropriate punishment for harmful consequences caused by the destruction of the information security system.

Second, China should track the dynamics of global ICV information security standardizations, as well as implement the relevant standardization agencies in order to accelerate the development of information security protection standards, including the *General Technical Conditions for Automotive Information Security Protection*, the *Automobile Gateway Information Security Technical Requirements*, the *General Technical Specifications for Automotive Information Security*, the *On-board T-BOX Information Security Technical Requirements*, and the *Electric Vehicle Charging Information Security Protection Specifications*.

Third, China should develop ICV data security technology standards, determine the level of protection by grading the data, and establish a standard framework for cloud security.

DOI 10.15302/J-SSCAE-2019.03.006

4.3 Formulating ICV information security test specifications

The traditional car is more focused and functional, and information security has gradually become the focus of ICV. ICV information-security tests can effectively measure whether the information security protection measures meet the associated protection requirements. Accordingly, the tests can be used to identify information security risks and weak links, which, in turn, can greatly improve security protection capabilities.

First, establish and improve the technical requirements and evaluation standards system of ICV information-security, and build an ICV detection and evaluation platform. Second, analyze the information security threat surface and risk level of the ICVs according to the application scenarios, establish a vehicle information security threat model under different intelligent levels, and conduct security tests on potential defects or weaknesses by relying on third-party evaluation agencie. Third, promote voluntary certification for low-level ICVs through the national information certification system, and implement mandatory security certification for high-level ICVs.

References

[1] Zhong Z H, Qiao Y J, Wang J Q, et al. Summary of strategy research on automobile power in new era (I) [J]. Strategic Study of CAE, 2018, 20(1): 1–10. Chinese.

[2] Zhong Z H, Qiao Y J, Wang J Q, et al. Summary of strategy research on automobile power in new era (II) [J]. Strategic Study of CAE, 2018, 20(1): 11–19. Chinese.

[3] Ponemon Institute. Car cybersecurity: What do the automakers really think? [R]. Traverse City: Ponemon Institute, 2015.

[4] IBM Business Value Research Institute. Accelerating vehicle information security: Winning vehicle integrity and data privacy competition [R]. Beijing: IBM Business Value Research Institute, 2017. Chinese.

[5] Zhao F Q, Liu Z W, Hao H, et al. Analysis of China's strategy for a stronger automotive country and its implementation pathway [J]. Forum on Science and Technology in China, 2016 (8): 45–51. Chinese.

[6] Yu H. Research on connected vehicle cyber security and anomaly detection technology for in-vehicle CAN Bus [D]. Jilin: Jilin University (Doctoral dissertation), 2016. Chinese.

[7] Li Y H. Research of the information security gateway of electric vehicle and research on wolfSSL protocol [D]. Hefei: University of Science and Technology of China (Master's thesis), 2017. Chinese.

[8] Zhao S J, Zhao F Q, Hao H, et al. The current situation and countermeasures in Chinese charging infrastructure of new energy vehicles [J]. Forum on Science and Technology in China, 2017 (10): 97–104. Chinese.

[9] Feng Z J, He M, Li B, et al. Research on car information security attack and protection technology [J]. Journal of Cyber Security, 2017, 2(2): 1–14. Chinese.

[10] Yin X, Wei D, Huang W Q, et al. Current situation and analysis of information security of vehicle networking in Japan [J]. China Information Security, 2017 (1): 98–101. Chinese.