Medicon Engineering Themes
Volume 3 Issue 1 July 2022
Review Article

Ensure Automotive Cyber Security with Management

Wenbo Jia, Haijun Wang*, Yingyi Yao, Jing Liu, Yanxin Wu, Xu Liu and Shubin Tao

Automotive Data of China (Tianjin) Co., Ltd., Tianjin 300393, China

***Corresponding Author:** Haijun Wang, Automotive Data of China (Tianjin) Co., Ltd., Tianjin 300393, China.

Received: May 30, 2022; **Published:** June 10, 2022

Abstract

With the automotive industry's continuous development of electrification, connectivity, intelligentization, sharing, automotive cyber security issues are becoming increasingly serious. How to effectively guarantee the cyber security of automotive products has become one of the urgent problems to be solved in the whole automotive industry. According to current situation of the industry, this paper argues that strengthening the cyber security management is very important, and according to the domestic and foreign automotive cyber security related laws, regulations and standards' requirements, proposes the construction route, evaluation and optimization focus of automotive cyber security management system based on the risk management of the whole automotive product life cycle, which provides reference for enterprises to ensure the cyber security of automotive products.

Keywords: Intelligent Connected Vehicles; Cyber Security Management System; System Evaluation and Optimization

Automotive Cyber Security Background

Development Status of Automotive Industry

In recent years, with the automotive industry's continuous development of electrification, connectivity, intelligentization, sharing, accelerated deep fusion of automotive and electronics, communication, network and other areas, automotive industry's technology innovation has become increasingly active, its industry scale expands unceasingly, the intelligent connected vehicle arises at the historic moment and develops rapidly [1]. In the process of realizing the mission of "replacing people to operate", the intelligent connected vehicle gradually possesses the intelligent connected functions such as environment perception, intelligent decision, collaborative control and entertainment communication through the highly integrated end device carrying and information interaction with wide radiation. At the same time, it also increases the probability of automotive cyber security vulnerabilities and the risk of automotive cyber security incidents [2].

According to the survey data of relevant institutions, the penetration rate of new vehicles equipped with intelligent connected functions in the global market is about 45% at present, and it is expected to reach nearly 60% of the market size by 2025 [3]. With the increase of end-mounted devices and the improvement of network connectivity, vehicle software's code has nearly 100 million lines, which is 10 times more than 10 years ago, and in the future it could reach 300-500 million. The rapid increase of code volume and complexity is bound to lead to the existence of automotive cyber security vulnerabilities, bringing potential automotive cyber security risks to the vehicle.

In addition, the increasingly rich industry ecology and increasingly complex supply chain, not only realize the intelligent connected functions, but also increase the channel of information interaction and the main body mastering information, providing more interfaces and objects for automotive cyber security attacks, which also greatly increase the threat to automotive cyber security.

In July 2015, Fiat Chrysler USA announced to recall about 1.4 million vehicles with software vulnerabilities [4], becoming the first vehicle manufacturer to recall vehicles due to hacker risk. Since then, the automotive industry has opened a new era of intelligent connected vehicles' cyber security. According to statistics, since 2010, there have been more than 900 public reports of automotive cyber security incidents. Compared with 2018, the number of incidents in 2021 has increased by more than 225% [5]. The overall number of security incidents is rising year by year, and the harm of security incidents is getting worse.

Therefore, the automotive cyber security has become the main constraint factor of the intelligent connected vehicle in the vehicle's connectivity and intelligentization, how to ensure the automotive cyber security has become one of the urgent problems to be solved by the major automotive manufacturers.

Status of International Regulatory Policies

In order to better deal with the automotive cyber security problems brought by the development of the industry, various international organizations have issued regulations and standards related to automotive cyber security, strengthening the supervision of automotive product cyber security with regulations and standards. On June 25, 2020, UN/WP29 issued the *Regulation No. 155 Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System* [6], which clearly puts forward the cyber security requirements for automotive manufacturers and automotive products. The EU has also introduced new requirements for all new models entering the EU market to comply with R155 requirement by July 2022, and all models in Europe by July 2024.

Status of China's Regulatory Policies

In view of the increasingly complex regulatory environment of automotive cyber security, China has constantly issued relevant regulatory policies. Among them, published in 2021 *Opinions on Strengthening the Access Management of the Intelligent Connected Vehicle Manufacturers and Products* [7], clearly put forward to strengthen enterprises' cyber security ability. Enterprises should set up cyber security management system, implement the cyber security level protection system and real-name registration management requirements for connected vehicles' cards in accordance with the law, clear responsibility, head of the department of cyber security. Enterprises also should have the technical measures to protect the automotive electronic and electrical systems, components and functions from cyber threats, and have the technical conditions to detect and dispose of automotive cyber security risks and cyber security defects and vulnerabilities to ensure that the vehicles and their functions are protected and ensure the safe operation of the vehicles.

To sum up, cyber security has become a major issue that cannot be ignored in the automotive industry. Major automotive manufacturers and relevant suppliers should actively respond to this development situation to ensure products' cyber security.

Importance of Cyber Security Management

In the field of security, the industry generally believes that the management decides 70%, the technology decides 30% [8]. For enterprises, to ensure the automotive cyber security of products, it is necessary not only to have corresponding cyber security technology strategy and means, but also to have security management measures. Only by paying equal attention to technology and management, can enterprises ensure that the cyber security risks of products are minimized, achieve the cyber security goals of enterprises and products, provide reliable services, and ensure the normal operation of products. So the cyber security management has become the top priority of the enterprise to ensure the cyber security, and the cyber security management is also one of the important ways to ensure that security technical means plays a normal role. The fundamental purpose of cyber security management is to standardize and constrain related cyber security activities, implement the requirements of cyber security strategy, so as to give play to the role of cyber security technology. The specific form of cyber security management is the introduction, publicity, implementation, supervision and inspection of cyber security management norms and systems. Therefore, the establishment of cyber security management system is an indispensable and important management means to ensure products' cyber security.

In addition, the construction of the cyber security management system is also the emphasis and publicity of the concept of "automotive cyber security" in the enterprise level, which also helps enterprises to deepen the concept of "automotive cyber security" at the level of consciousness, create an atmosphere of "automotive cyber security", and ensure products' cyber security in the source.

Cyber Security Management System

Basic Contents of Cyber Security Management System

Based on the requirements of I*SO/SAE 21434 Road Vehicles - Cyber security Engineering [9], UN/WP.29 R155, Opinions on Strengthening the Access Management of the Intelligent Connected Vehicle Manufacturers and Products, and Regulations on the Management of Security Vulnerabilities in Network Products* [10], we propose an automotive cyber security management system based on the cyber security risk management of the whole life cycle of automotive products. As shown in the Fig. 1, it mainly covers organizational management and product life cycle management two parts.

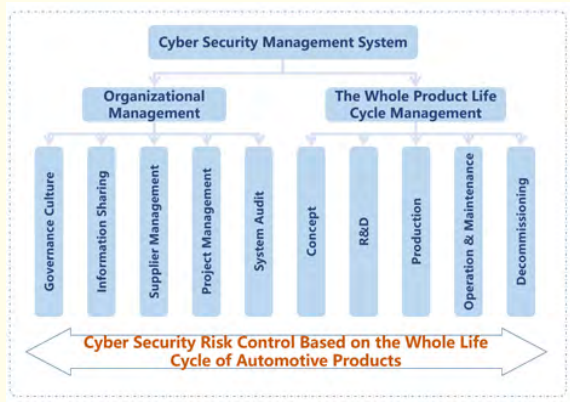

Figure 1: Overall framework of automotive cyber security management system.

Organizational management includes governance culture, information sharing, supplier management, project management and system audit five parts. Its specific content includes:

Governance culture: define the organizational structure of automotive cyber security management, clarify the objectives of automotive cyber security management system, formulate management system guidelines and strategies;

Information sharing: define the management scope of cyber security information, clarify the classification standards of cyber security information, control information application, information approval, information release, information deletion and other links to ensure the confidentiality and security of shared information;

Supplier management: establish supplier cyber security management system, strengthen the cyber security management requirements of relevant suppliers;

Project management: clear responsibility allocation of various activities, develop cyber security activity plans, define tailoring principles and so on;

System audit: establish the management process of internal audit and management review of cyber security management system, clarify the specific inspection content, inspection items and inspection methods of internal audit, and ensure the suitability, adequacy and effectiveness of the operation of the cyber security management system.

The whole product life cycle management includes concept, research and development, production, operation and maintenance, and decommission stages, including:

Concept phase & research and development phase: establish a cyber security development management process that integrates with the existing development process, clear personnel responsibilities and division of labor, match valve nodes, define input and output, integrate items identification, risk assessment, cyber security goals and concept formulation, integration and verification, validation and other cyber security activities;

Production stage: formulate and implement the cyber security production control plan to ensure that the cyber security requirements in post-development are applicable to the items or components, and ensure that no vulnerabilities can be introduced in the production process;

Operation and maintenance stage: establish a comprehensive cyber security operation and maintenance system, clarify the monitoring sources of cyber security intelligence, and screen cyber security problems. The establishment of automotive cyber security problem grading standards, analysis process, vulnerability notification, emergency management and other systems can accurately analyze, quickly respond to the occurrence of automotive cyber security problems, take appropriate disposal measures;

Decommissioning phase: establish a communication mechanism for the termination of cyber security support services, and ensure that components or systems involved in cyber security can be safely decommissioned.

The whole system takes the automotive product as the core, takes the cyber security as the goal, establishes the enterprise management system in the enterprise management level and the product management level, guarantees the automotive products' cyber security.

Basic Methods of Establishing Cyber Security Management System

The construction of the automotive cyber security management system can follow the PDCA process model, and the enterprise can complete the system construction through the three links of research and gap analysis, construction implementation and evaluation optimization.

In order to enhance enterprises' understanding of the automotive cyber security management system and improve the effectiveness of the implementation of the management system, gap analysis is usually carried out through research in the early stage of system construction.

In the research and gap analysis stage, we can first understand the overall situation of enterprise cyber security management through the survey questionnaire, such as organizational structure, internal documents, original management related documents, security services, cyber security training and so on. Then we can organize relevant personnel to hold interviews, in-depth understanding of the current situation of enterprise's cyber security, comb the existing enterprise cyber security management system framework and the corresponding management documents. Finally through the review of the existing cyber security management related documents, we can clear the enterprise existing cyber security management content, at the same time, communicate and discuss with relevant personnel on the framework of cyber security management system and the content of management documents, formulate the implementation plan of cyber security management system, and provide basis and guidance for the establishment of cyber security management system.

In construction implementation stage, the enterprise needs to focus on management roles, time nodes, specific activities, input and output related to activities and interaction relationship between all the parts, carry out the system from the organization management and the product whole life cycle management, formulate corresponding management process, forming automotive cyber security system relevant documents. The documents are divided into four levels. The first document is the policy strategy, which is the general policy of enterprise automotive cyber security management; The second documents are the standard procedure, are the core of the

system documents, contain the corresponding management requirements; The third level documents are the guide manual, are the specific process of carrying out activities formed according to the actual situation; The fourth documents are record forms, which provide record template documents for the actual operation results of the system.

After the establishment of the cyber security management system, according to the control requirements of the management system specification document, the enterprise should publish and implement the cyber security management system documents, enter the trial operation stage, and carry out the evaluation and optimization related activities. In the early stage of system operation, the enterprise should carry out the operation and promotion of the cyber security management system, and fully do a good job in the trial operation of the system and the publicity and implementation of the knowledge related to automotive cyber security management. In the trial operation stage of the system, the enterprise should timely find the problems existing in the system documents by deducting, simulating and selecting suitable models, find out the root causes of the problems, improve the corresponding processes and documents, and ensure the effectiveness and suitability of the system.

In addition, if the enterprise has established a quality management system (QMS) or information security management system (ISMS), the enterprise can associate the automotive cyber security management system with QMS and ISMS, reduce redundant processes and procedures, release enterprise management resources, and reduce cost and increase efficiency while ensuring product cyber security.

Evaluation and Optimization of Cyber Security Management System

After the establishment of the cyber security management system, the enterprise also needs to improve and optimize it, in order to ensure the advancement, suitability and effectiveness of the enterprise cyber security management system. Therefore, with the popularity of the cyber security management system in the industry, as an important input to optimize the cyber security management system, the evaluation of the cyber security management system has become the focus of the industry. At present, *Automotive Cybersecurity Management System Audit* [11] issued by VDA (Verband der Automobilindustrie) and the international standard *ISO PAS 5112 Road Vehicles - Guidelines for Auditing Cybersecurity Engineering* [12] can provide reference guidance for the evaluation of the cyber security management system.

VDA Automotive Cybersecurity Management System Audit

The main evaluation methods of *Automotive Cybersecurity Management System Audit* for the automotive cyber security management system include the rating of individual questions and the overall rating, in which the rating results of individual questions as the basis of the overall rating.

The rating of individual questions mainly evaluates the risk level of each individual question, judges the compliance degree of related work through the evaluation of each individual question, and divides the rating results into three levels: OK, minor non-conformity and major non-conformity. After completing the rating of individual questions, the overall rating result can be output according to the rating results of individual questions, and the operation status of the enterprise's cyber security management system can be divided into three states: audit passed, audit failed; measures must be defined, audit failed.

Besides, VDA *Automotive Cybersecurity Management System Audit* also explains the key points of cyber security management, risk identification and risk assessment, risk management, the product whole life cycle of the cyber security management and supplier cyber security management, provides support for the rating of individual questions. For the overall rating, VDA *Automotive Cybersecurity Management System Audit* proposed that the automotive cyber security management system re-audit must consider the results of the last audit. Any measures passed in the last audit but not implemented or insufficiently implemented will have a negative impact on the results of the current audit.

ISO PAS 5112 Road Vehicles - Guidelines for Auditing Cybersecurity Engineering

ISO PAS 5112 Road Vehicles - Guidelines for Auditing Cybersecurity Engineering issued on March 31, 2022 provides an example of the audit questionnaire for the requirements of ISO/SAE 21434 standard in Annex A, audits and evaluates cyber security management system in the aspects of cyber security management, cyber security activities, risk assessment and methods, concept and product development stages, post-development stage, distributed cyber security activities and so on. This standard also provides a powerful reference for the evaluation and optimization of automotive cyber security management system.

Suggestions on Key Points of Automotive Cyber Security Management System Evaluation

By reviewing domestic and foreign standards, regulations and industry practice experience, we believe that the review and evaluation of cyber security management system should focus on the following aspects:

Organizational cyber security management: whether the measures related to automotive product cyber security at the organizational level are sufficient and in place. Such as the provision of relevant resources, the establishment of cyber security culture, the corresponding organizational structure, related training and publicity and so on.

Supply chain cyber security management: the assessment of suppliers' cyber security capabilities, the control of the cyber security level of products provided by suppliers and the division of responsibilities with suppliers on cyber security, etc.

Product cyber security development management: related cyber security development work from concept to pre-SOP, covering threat analysis and risk assessment, system and component security design, testing, verification and validation, etc.

Product cyber security production management: methods for enterprises to implement cyber security requirements in the post-development stage.

Product cyber security operation and maintenance management: product cyber security risk continuous monitoring, product cyber security vulnerability management, product cyber security emergency response, etc.

To sum up, enterprises should focus on the above evaluation dimensions after establishing the automotive cyber security management system, and conduct a comprehensive evaluation of the effectiveness and adequacy of the system in terms of the completeness of the system, the suitability of the process, the adequacy of the personnel ability, the integrity and consistency of the document record and so on, then optimize and continuously improve the system.

Summary

To sum up, in order to ensure the cyber security of automotive products, enterprises should not only have the technical measures to protect the automotive electronic and electrical systems, components and functions from cyber threats, the technical conditions for the detection and disposal of cyber security risk monitoring, cyber security defects and vulnerabilities, etc. More importantly, enterprises should strengthen the management of automotive cyber security from the awareness level, implementation level and continuous optimization level, standardize and restrict the relevant automotive cyber security activities in terms of personnel awareness, process system, supervision and improvement, so as to ensure that all the technical measures of automotive cyber security are implemented and effective.

References

1. Jiatong Zhang. "Analysis on Information Security and Development Suggestions of Intelligent Connected Vehicle". China Informatization 07 (2021): 70-71.
2. ZhenGuo, ChaoMa, Guoliang Wang and Tianyu Liu. "Development Status and Prospect of Intelligent Vehicle CyberSecurity Technology". Automotive Parts 02 (2021): 115-121.

3. Jingjing Hao., et al. "Challenges and Development of Information Security of Intelligent Connected Vehicles". Proceedings of the 14th China Intelligent Transportation Annual Conference (2019): 1-8.
4. Yanxin Wu and WenboJia. "Automotive Cyber Security Issues Development Status". Automotive Information Security 30 (2020): 382.
5. Upstream Security Global Automotive Cybersecurity Report 2021. Upstream Security Ltd (2022).
6. UN ECE/WP.29. Regulation No. 155 Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System (2021).
7. Ministry of Industry and Information Technology, PRC. Opinions on Strengthening the Access Management of the Intelligent Connected Vehicle Manufacturers and Products (2021).
8. Zhengyan Zhong and Yi Wei. "Design and Research of Enterprise Information Security Guarantee System". Modern information science and technology 4.10 (2020): 139-141.
9. International Organization for Standardization. ISO/SAE 21434: 2021 Road Vehicles - Cybersecurity Engineering [S]. International Organization for Standardization (2021).
10. Ministry of Industry and Information Technology, PRC. Regulations on the Management of Security Vulnerabilities in Network Products (2021).
11. Verband der Automobilindustrie. Automotive Cybersecurity Management System Audit. Berlin: Verband der Automobilindustrie (2020).
12. International Organization for Standardization.ISO PAS 5112 Road Vehicles - Guidelines for Auditing Cybersecurity Engineering. International Organization for Standardization (2022).

Volume 3 Issue 1 July 2022