Cybersecurity Management Strategy of Automobile Supply Chain

Xu Liu(✉), Haijun Wang, and Shubin Tao

China Automotive Technology and Research Center Co., Ltd, Tianjin, China
{liuxu2021,wanghaijun2019,taoshubin}@catarc.ac.cn

Abstract. In recent years, the development of intelligent and networked vehicles has been accelerated, innovative technologies have been evolving, and industrial transformation has continued to deepen. At the same time, automobile cybersecurity problems are becoming increasingly prominent, and many risks and hazards caused by automobile cybersecurity incidents have aroused the focus of the regulatory authorities, the industry and the public. As the supply chain of intelligent connected vehicles is long, the main body is diversified and complex, and the cybersecurity protection involves many links, it is easy to form a security gap and capacity shortcomings. From the perspective of industry demand, supplier cybersecurity management is an indispensable link in the construction of automobile cybersecurity management system by automobile manufacturers. At the same time, in order to effectively meet the cybersecurity needs of automobile manufacturers, enterprises in all links of the supply chain need to strengthen their own cybersecurity capacity building. Therefore, in order to improve the overall security level of the industry and promote the healthy development of the industry, it is very necessary to strengthen the cybersecurity guarantee ability of the whole supply chain of intelligent connected vehicles and build a cybersecurity guarantee system covering the whole life cycle of intelligent connected vehicles.

Keywords: Intelligent connected vehicle · cybersecurity supply chain · cybersecurity system

1 Introduction

As the supply chain of intelligent connected vehicles is long, the main body is diversified and complex, and the cybersecurity protection involves many links, it is easy to form a security gap and the ability of the short board. Therefore, it is of great significance to enhance the overall security level of the industry and promote the healthy development of the industry to strengthen the cybersecurity guarantee ability of the whole supply chain of intelligent connected vehicles and build a cybersecurity guarantee system covering the whole life cycle of intelligent connected vehicles.In view of the current situation and challenges of automobile supply chain cybersecurity, based on the requirements of current domestic and foreign regulatory standards, this paper expounds the practical points of automobile manufacturers' supply chain cybersecurity management, analyzes

S. Kadry et al. (Eds.): BDEIM 2022, AEBMR 233, pp. 276–283, 2023.
https://doi.org/10.2991/978-94-6463-124-1_33

the key elements of automobile suppliers' cybersecurity ability from the perspective of management system and key technologies, and systematically reviews the evaluation and certification system suitable for automobile supply chain cybersecurity. Put forward measures and suggestions to promote the development of automobile supply chain cybersecurity.

2 Automotive Supply Chain Cybersecurity Issues and Challenges

Under the development trend of automobile intelligence and network connection, the industrial structure and supply and demand relationship are integrated and staggered, which constitute multiple subjects, involve many links, and the level of cybersecurity capability is uneven. Inevitably, there are gaps and weak links in cybersecurity protection. At the same time, as software and system gradually become the core competitiveness of automobiles, the integration and application of cross-field technologies are deepening gradually, and the complexity of technical system is increasing several times. As a result, it is more difficult to ensure the overall design and coordination of cybersecurity protection, which leads to huge risks of supply chain cybersecurity (Fig. 1).

From the perspective of automobile suppliers, appropriate cybersecurity capabilities should be established to meet the cybersecurity requirements delegated and assigned by automobile manufacturers or superior suppliers, so as to ensure opportunities in market competition. However, as the current supplier management system of automobile manufacturers is not perfect and relevant requirements are not clear enough, suppliers at all levels of the industrial chain are generally lacking in the awareness and ability of cybersecurity management. Specific problems include: lack of organizational level cybersecurity management system; Lack of cybersecurity management process covering the whole life cycle of products; Lack of cybersecurity technology design and testing verification for core products; Lack of their own cybersecurity ability level of effective proof means (Fig. 2).

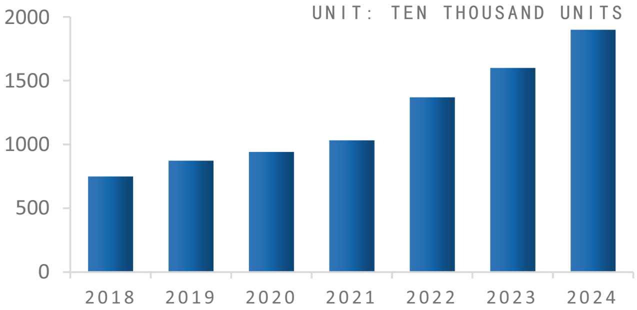

Fig. 1. Market size of China's intelligent connected vehicles [Since the draw]

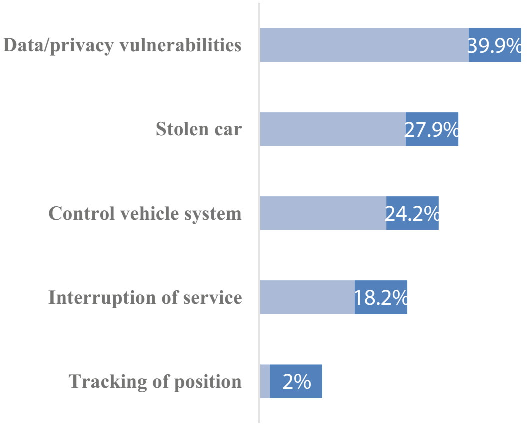

Fig. 2. Classification of cybersecurity events [Since the draw]

3 Manufacturer Supply Chain Cybersecurity Management

3.1 Supply Chain Cybersecurity Assessment and Access

Cybersecurity assessment of suppliers mainly includes management and technology. In terms of management, it can comprehensively refer to ISO/SAE 21434 standard and other relevant standards, and combine with the manufacturer's internal supplier management requirements for cutting [1]. As a typical second-party audit activity, supplier evaluation can refer to ISO/PAS 5112 standard in terms of audit procedures and operation specifications. In terms of technology, the technical department can independently complete the technical evaluation work by referring to the existing technical evaluation process of potential suppliers of automobile manufacturers, and add the evaluation of the relevant dimensions of cybersecurity technical capability during the evaluation [2].

Automakers can ask potential suppliers for records and evidence of their cybersecurity capabilities, Including but not limited to development, post-development, governance, quality and information security in the field of cybersecurity best practices, sustainable cybersecurity activities, cybersecurity incident response evidence, third party provided cybersecurity evaluation reports, ISO/SAE 21434 certificate and other cybersecurity related certificates or process management documents.

3.2 Supervision and Administration Before the Appointment

In the process of inquiry for the designated supplier, the automobile manufacturer shall make the following formal requirements:

- Require potential suppliers to comply with the relevant requirements for assessment access and ensure that they provide no less capability and resources than demonstrated in the assessment process;
- Require potential suppliers to strictly fulfill the cybersecurity responsibilities in the mutually agreed security agreement;

- Clarify relevant cybersecurity objectives and cybersecurity requirements for the products or services quoted by potential suppliers.

Automobile manufacturers should develop and sign security agreements with designated suppliers to clarify the distribution of responsibilities between manufacturers and suppliers regarding cybersecurity activities and form constraints. Security protocols can include:

- Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select "1 Column" from the selection palette. The manufacturer and supplier shall each provide personnel who meet the requirements related to cybersecurity as a contact person, who shall communicate and confirm the work items, progress and responsibilities (ISO/SAE is recommended for reference 21434 Appendix C.2);
- Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select "1 Column" from the selection palette. Information sharing mechanism between manufacturers and suppliers, confirming information and work results to be shared, sharing methods and tools to be used, etc.;
- Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select "1 Column" from the selection palette. Cybersecurity activities at each time point of the project of the supplier, namely cybersecurity plan, such as: based on the schedule plan of the model project to clarify the output time of the deliverables, the acceptance of the deliverables and other conditions.

3.3 Post-designated Supervision and Management

Regular Audit

In the process of development, the supplier's work implementation (cybersecurity) was reviewed and evaluated according to the supplier's daily performance evaluation standards [3].

Interim Audit

An interim audit process shall be initiated when:

- Cybersecurity events caused by cybersecurity vulnerabilities of parts and components;
- When cybersecurity issues occur during the delivery phase;
- When the components are known to have cybersecurity vulnerabilities through other means.

Regular Project Meeting

Determine the frequency of regular project meetings, synchronize the progress of cybersecurity work, synchronize cybersecurity vulnerabilities, etc.

Cybersecurity Archive Management

The collection of cybersecurity archive contents includes but is not limited to the following aspects:

- Schedule node of component development, name of cybersecurity output of each node;
- Time, participants, conclusion (meeting minutes) of each regular project/technical meeting;
- The actual completion and output of cybersecurity during mass production of nodes;
- Vulnerability analysis report, cybersecurity risk mitigation measures, etc.

Suppliers
A security agreement should be signed with the next level supplier (if any).

Security Vulnerability Repair
Within the time agreed in the contract, the auto supplier shall always respond to the occurrence of cybersecurity vulnerabilities/events, and unconditionally repair the cybersecurity vulnerabilities caused by itself [4].

4 Automobile Supplier Cybersecurity Management System

At present, the UN/WP.29 R155, the most widely recognized international regulation, Cybersecurity and Cybersecurity Management System, puts forward relevant requirements for the supplier management of automobile manufacturers [5]. That is, vehicle manufacturers should be required to indicate how their cybersecurity management systems will manage the degree of compliance that may exist in sub-organizations of contract suppliers, service providers or manufacturers with the requirements of Section 7.2.2.2 of the R155 regulation. For suppliers, they should consider the requirements to support the compliance and access of automobile manufacturers, and consider their cybersecurity management system from multiple aspects, such as cybersecurity organization management and cybersecurity process management.

5 Cybersecurity Organization Management

Cybersecurity organization management is defined for the "process of management process", including the organization management process, asset management, cultural awareness management, configuration management, document management, tool management, change management. Group of middle the asset management in weave management is included in the whole product lifecycle process, and its cybersecurity attributes can be compromised can cause security incidents; Cybersecurity management of the means of production, mainly for its authority management; At the same time, it is necessary to consider cybersecurity related topics in the existing configuration management, file management, tool management and change management, and integrate cybersecurity into the existing management process [6].

Cybersecurity project management refers to the planning and development of cybersecurity related work items at the project level. Including the definition of the cybersecurity plan, cybersecurity examples, cybersecurity assessment and design approval. In addition to the time plan, the cybersecurity plan should also consider the resources, manpower and management plan of cybersecurity activities in the cybersecurity project, and define the input and output of each cybersecurity activity. The output should be corresponding to the cybersecurity example, so as to provide the corresponding materials for the integrity and correctness evaluation when the design is approved [7].

6 Cybersecurity Process Management

6.1 Cybersecurity Concept Stage

The purpose of this phase is to derive cybersecurity objectives and concepts through threat analysis and risk assessment. This stage is especially important for parts suppliers belonging to the type of “out-of-context”, because there is no existing demand for this type of supplier. Based on the assumption of the environment, it is necessary to analyze its assets, damage, threat and risk from the perspective of the vehicle, and deduce the safety objectives and concepts for the parts themselves. And carry out subsequent development work with this goal and concept. Therefore, for suppliers of “out-of-context” type, this part of the process cannot be cut [8].

6.2 Cybersecurity Development Stage

The development stage mainly refines the actual landing plan for the cybersecurity concept, including cybersecurity system design, cybersecurity related hardware and software design, vulnerability analysis, code audit, cybersecurity testing, etc. In the process of cybersecurity development, vulnerability analysis can not be ignored. Its main role is to optimize the existing software and hardware architecture by analyzing the possible vulnerability of components, so as to better achieve the top-level cybersecurity objectives and concepts [9]. Code audit report and cybersecurity test report can not be ignored, they are used as the docking file with the upper demand party to prove that the product has not introduced medium and high risk vulnerabilities in the development.

6.3 The Post-development Stage of Cybersecurity

The cybersecurity post-development phase focuses on activities related to production, operations, and closing support processes. For the production stage, it is necessary to consider the production related requirements that may be introduced in this stage, including key filling, cybersecurity information configuration, etc., which should be added to the existing production control plan for unified management [10]. The operation and maintenance stage mainly focuses on the emergency response process after the occurrence of cybersecurity incidents related to parts. What should not be neglected is the information synchronization and process docking between parts suppliers and stakeholders, especially the demand side. Its own processes should be able to avoid the impact of major security incidents in a timely manner; The end of the support phase needs to consider the cybersecurity declaration and data processing process description related to the features of the cybersecurity parts.

7 Conclusion

The automobile industry is characterized by many aspects, complex systems and high integration. Cybersecurity problems occurring in any link may spread risks to the entire supply chain, thus producing more far-reaching impacts. In the future, with the further improvement of automobile intelligence and network connectivity, the role of the industrial chain will be more abundant, and the information flow and data flow interaction between various entities will be more frequent. Strengthening the cybersecurity management of the entire automobile supply chain, making overall planning, coordination and orderly promotion will also play an increasingly important role in ensuring the cybersecurity of the automobile industry, and will become the focus of increasing attention from all sectors of the industry [11].

At present, the regulatory authorities have focused on cybersecurity as a key issue in the development of the automobile industry. With the improvement of the regulatory system and the gradual landing of regulatory requirements, regulatory authorities will begin to carry out more specific and in-depth regulatory work in each subdivision of automotive cybersecurity, and promote the implementation of a series of regulatory means, including the issuance of management rules, the implementation of special review, the organization of pilot demonstration, and the issuance of standard development requirements. As an important part of the automotive supply chain cybersecurity management, the relevant standard requirements will continue to be refined, and the regulatory measures will be continuously strengthened.

Therefore, the following suggestions are proposed for automobile supply chain cybersecurity management:

1. Automobile manufacturers should build and improve the cybersecurity management system and implement supplier cybersecurity management principle of action.
2. Auto suppliers should pay timely attention to regulatory trends and customer needs, and make forward-looking deployment of cybersecurity capability construction.
3. Third-party institutions should strengthen capacity building and provide multi-dimensional evaluation and certification services for the industrial chain.

References

1. ISO/SAE 21434 Road vehicles — Cybersecurity engineering,2021
2. ISO/PAS 5112 Road vehicles — Guidelines for auditing cybersecurity engineering,2022
3. Automotive supply chain Cybersecurity Management White Paper,2022
4. UNECE R155 Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system,2021
5. Axalta Unveils Global Automotive Color Popularity Report [J] Focus on Powder Coatings, 2021, 2021(2)
6. Cybersecurity of Intelligent Vehicle [J]. Zhang Liping. Telecom Express. 2015(11)
7. Current Situation and Development Suggestions of Chinese Intelligent Networked Automobile Information Security Laws and Regulations System [J]. Wang Jinming, Liu Yu, Zhang Yifan. Automobile Aspect. 2020(10)

8. Automotive Cybersecurity - Efficient Risk Management for the Entire Life Cycle of Vehicles [J] ATZelektronik worldwideVolume 15, Issue 11. 2020. PP 18–22
9. A brief analysis on the cybersecurity of intelligent connected vehicles[J]. Li Rui, Yan Han. Industrial Information Security. 2022(03)
10. Development Status and Trend of Intelligent Connected Vehicle (ICV) Technology [J]. He Zhiyong, Li Jianying. Agricultural Machinery Use and Maintenance. 2022(09)
11. An Overview of Intelligent Networked Vehicle Information Security [J]. Song Haochen, Yang Lin, Xu Huawei, Yang Junjie, HU Jianyao, Chen Chaoying. Information Security and Communication Security. 2020(07)