Road vehicles Cybersecurity system evaluation method

Hao Shan, Kexun He, Baizheng Wang, Xiyu Fang
No.68, Xianfeng Road, Dongli District, Tianjin, China.
shanhao@catarc.ac.cn

Abstract. With the continuous improvement of automobile intelligence and networking, automobile cybersecurity has gradually become the focus of attention from enterprises and research institutions. Whether it is domestic or international, there are many organizations and institutions in the Internet of vehicles cybersecurity is widely concerned, ISO 21434 road vehicle network security project, is an international automotive network security standard, which covers the entire life cycle of automotive products (from design to retirement), is currently in the development. From the perspective of ISO 21434 cybersecurity system requirements, this paper proposes an cybersecurity system evaluation method for automobile companies, in order to evaluate whether or to what extent each automobile company meets the cybersecurity status of ISO 21434 standard.

1. Introduction
With the interconnection and intelligence of cars, cars are no longer isolated, but more and more integrated into the Internet. At the same time, cars have gradually become potential network attack targets [1-2], and the network security of cars has become the basis of vehicle security, attracting more and more attention [3-6]. How to realize automobile network security, the automobile industry has made a lot of exploration and achieved a lot of results. In order to reduce the cost and improve the quality, it is imperative to standardize the existing results.

In the process of formulating standards [7-9], China has referred to the standard formulation situation of foreign countries with mature automobile industry, such as developed countries such as the United States and Japan, as well as the standard formulation progress of more authoritative organizations and societies such as ISO/TC22 and SAE. From an international perspective, SAE J3061 is the first to be mentioned in terms of norms and standards for the entire life cycle of enterprises, organizations and products. SAE J3061 is a standard for the entire life cycle of a vehicle, which provides a process framework and guidance for vehicle network security that takes into account the entire life cycle of the vehicle, from concept to production, operation, maintenance and scrap. SAE J3061 is designed to help businesses identify and assess cyber security threats, and to import cyber security into the entire vehicle development process. The main contents of SAE J3061 are:

- Defines the complete lifecycle process framework. Enterprises can tailor and utilize this framework to import network security into vehicle development process, including concept to production, operation, maintenance and scrap
- Provides guidelines
- Provides vehicle network security related tools and methodologies

Based on SAE J3061, ISO 21434 is a standard for the entire life cycle of a vehicle. The standard is being developed and is scheduled for release in 2020. ISO 21434 mainly guarantees the development of automotive cybersecurity engineering from four aspects: risk assessment management, product...
development, operation/maintenance, and process audit. The goal is that the products designed, produced and tested by the standard have certain cybersecurity protection capabilities [10].

2. Introduction of ISO 21434

ISO 21434[11] specifies requirements for the concept, development, production, operation, maintenance, and disposal of engineering-related cybersecurity risk management for road vehicle electrical and electronic systems and their components and interfaces. The standard defines a framework that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risks. This standard applies to electrical and electronic systems for mass production road vehicles, including components and interfaces developed or modified after the date of publication of this standard.

The main elements of ISO 21434 include:

➢ Terms and definitions relating to cybersecurity
➢ Enterprise level cybersecurity management
➢ Project level cybersecurity management
➢ Continuous improvement of cybersecurity management
➢ Risk assessment of cybersecurity management
➢ Cybersecurity related product concept development
➢ Cybersecurity related product system development
➢ Cybersecurity management operation and maintenance requirements
➢ After the design stage (production, operation and maintenance, decommissioning, scrapping, etc.) cybersecurity management

It is through these dimensions that the standard ensures the development of automotive cybersecurity engineering design and process system. However, the standard does not mention how to evaluate and evaluate the best practices of automobile cybersecurity conducted by automobile companies according to the standard. In this paper, from the perspective of best practice requirements mentioned in the standard, test and evaluation methods will be proposed to determine whether or to what extent automobile companies have implemented the best practices of automobile cybersecurity in accordance with the standard.

3. System evaluation method

ISO 21434 puts forward corresponding requirements for cybersecurity management content in each chapter, for example, the requirements are numbered as rq-xx-yy, XX represents the chapter, YY represents the entries in this chapter. For specific items, this paper proposes an cybersecurity evaluation method for this item. Generally, there are 5 items, and each item is awarded one point. There are 36 items in total and 180 points in total. The final score of more than 126 points (including) of the automobile companies, that can be evaluated to meet the cybersecurity requirements of ISO 21434 standard.

| ID       | requirements                                                                 | Evaluation method                                                                 |
|----------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| RQ-05-01 | The organization shall define a cybersecurity policy                         | 1. The organization has a clear policy on network security, which is formally publicized and implemented by all staff; |
|          |                                                                                | 2. Confirmation of road vehicle network security risks;                           |
|          |                                                                                | 3. The commitment of the top management to manage the corresponding risks;        |
|          |                                                                                | 4. The policy should include the attitude the organization will take after an cybersecurity incident; |
|          |                                                                                | 5. The change of policy should record the time, version and other information     |

Table 1. The corresponding relationship between the Evaluation method and ID requirements
| RQ-05-02 | The organization shall establish and maintain rules and procedures at the organizational level to support the implementation of the requirements of this international standard and the implementation of the corresponding activities | 1. The specific steps of the rules and procedures of the organization are recorded in the electronic system; 2. Have clear measures to deal with those who do not follow the rules and procedures of the organization; 3. Rules and procedures shall be reviewed and revised as the company develops; 4. There should be clear guidance documents for the complex technical procedures involved in the rules and procedures; 5. The organization's rules and procedures require the approval of the relevant leaders before they can take effect. |
| --- | --- | --- |
| RQ-05-03 | The organization shall assign and communicate responsibilities for achieving and maintaining network security; And grant the appropriate permissions | 1. Organize a special cybersecurity department to take charge of cybersecurity matters; 2. The cybersecurity department is independent of any other department of the organization; 3. The cybersecurity department has the authority to obtain the information resources it needs; 4. The organization shall publicize the status of its cybersecurity department internally; 5. The organization shall ensure the execution of the cybersecurity team in its work. |
| RQ-05-04 | The organization should provide the resources needed to address cybersecurity issues | 1. The organization shall purchase system equipment required for network security; 2. The organization shall provide the necessary funds for network security; 3. The cybersecurity department shall have a special cybersecurity incident management team; 4. The organization should make good public relations for the cybersecurity team; Organizations should have a cybersecurity red team. |
| RQ-05-05 | The organization shall identify areas of expertise related to or interacting with cyber security and establish and maintain channels of communication between these areas of expertise in order to A) determine whether to integrate network security into existing processes and how to do so; B) coordinate the exchange of relevant information. | 1. The organization shall identify areas of expertise related to cyber security including information technology security, functional security, data protection and privacy protection; 2. Regularly communicate with the cybersecurity department in relevant professional fields (information technology security, functional security, data protection and privacy protection); 3. The cybersecurity department tries to integrate cybersecurity into the existing professional processes; 4. Relevant information includes threat scenarios and hazard information, network security objectives and functional security objectives, or where there may be conflicts between network security requirements and functional security requirements; 5. Coordination includes the identification of Shared cybersecurity services and reuse of cybersecurity policies and tools across professional domains. |
| RQ-05-06 | The organization should define risk values (1 to 5) in a risk matrix | 1. The organization shall conduct its own qualitative risk assessment;  
2. The organization shall identify its significant assets;  
3. Organizations can define appropriate risk matrices according to their specific needs and purposes;  
4. Determine the priority of risk disposal;  
5. Determine how to handle the risk. |
| RQ-05-07 | The organization shall establish and maintain a network security culture | 1. People in charge of cybersecurity projects set an example that others can trust and follow.  
2. Procedures are in place to ensure that network security decisions are traceable.  
3. Give top priority to network security and functional security when making design and development decisions.  
4. The reward system supports and encourages effective results in cyber security, while punishing those who harm cyber security in order to take shortcuts.  
5. Positive attitude towards network security, such as:  
- can discover and solve network security problems in the early stage of the product life cycle (network security is designed);  
- the organization is ready to respond quickly to vulnerabilities and cyber security incidents that occur during user use. |
| RQ-05-08 | The organization shall ensure that the personnel involved in network security within the organization have the corresponding capabilities and awareness to perform their duties | 1. Personnel involved in network security are familiar with the organization's network security rules and procedures, including network security risk management;  
2. The personnel involved in network security are familiar with the rules and procedures of the organization in the professional fields related to network security, such as functional security and privacy protection;  
3. Personnel involved in network security are familiar with methods, tools and guidelines related to network security;  
4. Personnel involved in network security are familiar with known attack means and network security controls;  
5. Network security personnel are familiar with the general handling of emergency security incidents. |
| RQ-05-09 | The organization shall establish and maintain a continuous improvement process | 1. Learn from historical network security business experience, including experience gained from on-site monitoring and internal and external information observation;  
2. Learn from the information of similar products in the industry;  
3. Get the improvement items that need to be implemented in the network security activities of the follow-up projects;  
4. Communicate lessons learned to appropriate personnel;  
5. Make its cybersecurity-related issues more and more efficient. |
| RQ-05-10 | Network security risk management shall comply with ISO 31000 | 1. The organization can maintain the consistency of network security risk management and enterprise risk management; 2. Risk management is a part of the decision-making of senior management; 3. Risk management explicitly expresses uncertainty; 4. Risk management shall be adjusted according to the situation of the organization; 5. Risk management should be dynamic, repeatable, and adaptable to change. |
|---|---|---|
| RQ-05-11 | A network security audit shall be conducted to independently determine whether the organization's processes are meeting the objectives of this standard | 1. The cybersecurity audit may be included in or integrated with other audits that meet the quality management system standards 2. The person performing the audit may be from within or outside the organization 3. To ensure that the organization's processes are always applicable to network security, audits can be performed periodically 4. Auditors or departments should be independent of the rest of the organization 5. Auditors have access to the resources they need. |
| RQ-05-12 | The organization should define the environmental conditions, taking into account the internal and external aspects of the organization, what sharing is necessary and allowed, and what is prohibited | 1. List of Shared network security information types; 2. Approval process for sharing; 3. Information editing and desensitization requirements; 4. Rules for the traceability of Shared information; 5. Types of counseling and communication allowed. |
| RQ-05-13 | The organization shall establish and maintain a quality management system in accordance with international standards or equivalent standards to support network security projects | 1. Change management; 2. Document management; 3. Configuration management; 4. Demand management; 5. Incident management. |
| RQ-05-14 | The network security configuration information of the mass production product shall remain available until the product is terminated for maintenance | 1. Bill of materials 2. Binary code 3. A network security management system for the manufacturing process shall be developed 4. Change management 5. Configuration management |
| RQ-05-15 | Tools that can affect related items, systems, and components should be managed | 1. Use the tool correctly according to the user's manual with erratum; 2. Protect against unexpected use and operation; 3. Access control for tool users; 4. Verify the tool. 5. Use the minimum permission principle |
| RQ-06-01 | Responsibilities related to the project's network security activities shall be communicated and assigned | 1. Organize a special cybersecurity department to take charge of cybersecurity matters;  
2. The cybersecurity department is independent of any other department of the organization;  
3. The cybersecurity department has the authority to obtain the information resources it needs;  
4. The organization shall publicize the status of its cybersecurity department internally;  
5. The organization shall ensure the execution of the cybersecurity team in its work. |
| RQ-06-06 | Cyber security plans should include | 1. Dependence or preconditions on other activities or information  
2. The purpose and person in charge of the activity  
3. Start node or stop node and expected duration  
4. Summary of results  
5. Scope of cyber security activities |
| RQ-06-07 | The network security plan should be updated when the activities under way are determined to change or refine | 1. Risk assessment should be made according to changes in activities  
2. Make corresponding network security changes to the changed parts  
3. There should be relevant process to control the change  
4. If the change fails, there should be a rollback mechanism to ensure business continuity  
5. Assess the risks if changes are not made. |
| RQ-06-10 | The cybersecurity plan and the work resulting from the cybersecurity activities defined in the cybersecurity plan | 1. Change management;  
2. Document management;  
3. Configuration management;  
4. Demand management;  
5. Incident management. |
| RQ-06-18 | A network security case should be created to provide evidence supported by the results of the work to demonstrate the extent to which network security has been achieved | 1. The company has sound network security rules and regulations  
2. The company will conduct regular network security awareness training for employees  
3. The company will monitor employees' activities in the company by technical means, such as anti-virus and online behavior management  
4. The company meets the requirements of network security level protection  
5. The company meets specific industry laws and regulations. |
| RQ-06-25 | The scope of network security assessment should include | 1. The cybersecurity plan and all deliverables required by the cybersecurity plan;  
2. Rationality and effectiveness of implemented or implemented network security technology or process control;  
3. Evidence that relevant objectives have been achieved;  
4. Basic principles of dealing with network security risks;  
5. Network security requirements after development. |
| RQ-08-02 | The assets with network security attributes that will lead to loss scenarios after being attacked should be listed | 1. Disclosure of sensitive information stored in IVI  
2. Function failure of ECU or domain controller after being hacked  
3. Information leakage and waste of computing resources will occur after the cloud platform is attacked by hackers  
4. When OTA upgrade system is attacked, it will cause illegal software downloading  
5. When the car-controlling APP is attacked, the vehicle will be maliciously controlled. |
| RQ-08-12 | The results that affect the category, attack path, and risk determination should be considered to help determine the options for risk handling | 1. To avoid risks by eliminating sources of risk or by deciding not to initiate or continue activities that cause risks;  
2. Mitigate risks by means of safety control;  
3. Share or transfer risks (e.g. through a contract, or by buying insurance);  
4. Accept residual risks after disposal;  
   Accept risk. |
| RQ-10-01 | Network security requirements should be optimized based on the following conditions | 1. Higher level assigned cybersecurity requirements  
2. Higher level architecture design  
3. Abnormal detection of network security control function  
4. Systems with security event logging mechanisms require secure communication with external systems to achieve log data collection  
5. Optimized cybersecurity requirements may also include technical implementations of higher-level cybersecurity requirements from external sources. |
| RQ-10-02 | The architecture design should be optimized for the development level based on the following conditions | 1. Initial architectural design  
2. Network security control  
3. Optimized network security requirements;  
4. Higher level architecture design  
   Operating environment. |
| RQ-10-10 | The identified vulnerabilities should be managed | 1. Functional isolation;  
2. Use of encryption;  
3. Secure storage;  
4. Anonymization of personal information;  
5. Fix bugs |
| RQ-10-12 | The testing needs to ensure that the execution of the design and the integration of the components meet the following requirements | 1. Includes vehicle system-level integration and testing.  
2. Process the results of hardware and software tests at the system level.  
3. The test includes updated regression test and retest after bug repair.  
4. The test method can be used as a baseline as part of the standard engineering of the quality management system.  
5. Testing should be done in cycles, or after major changes to the product. |
| **RQ-10-15** | Test case coverage should use test coverage metrics defined in relation to cybersecurity to determine the integrity of the test methodology |
|----------------|--------------------------------------------------------------------------------|
| **1.** | Test coverage can be determined by using appropriate software tools. |
| **2.** | Under full test coverage is acceptable if justified. |
| **3.** | Test coverage is only used to determine whether all requirements are translated into execution and implementation |
| **4.** | Test common defects (incorrect sequence of operations, insufficient authentication). |
| **5.** | Analysis of test coverage can reveal weaknesses such as require-based test cases, inadequate requirements, dead code, dead code, or unexpected functionality. |

| **RQ-10-19** | When choosing a design, modeling, or programming language, consider the following |
|----------------|--------------------------------------------------------------------------------|
| **1.** | Grammatically and semantically clear and comprehensible definitions; |
| **2.** | Support the realization of modularization, abstraction and encapsulation; |
| **3.** | Support the use of structured structures; |
| **4.** | Support the use of security design and coding techniques; |
| **5.** | Portability |

| **RQ-11-04** | In accordance with the rationale, project validation should ensure that all risks identified during the concept and product development phases have been accepted or have been disposed of as such risks have been accepted |
|----------------|--------------------------------------------------------------------------------|
| **1.** | Risk mitigation options; |
| **2.** | Decided to hedge some risks; |
| **3.** | Some risks can be transferred by buying insurance, etc. |
| **4.** | Accept the remaining residual risk |
| **Step 5 accept risk** |

| **RQ-12-01** | A production control plan for cybersecurity requirements for the post-development phase shall be created |
|----------------|--------------------------------------------------------------------------------|
| **1.** | Once the relevant item or component is produced, its development-time access shall be removed immediately |
| **2.** | Physical access security precautions include avoiding physical access to the production server running the software. |
| **3.** | Logical access security protection measures include the application of cryptography technology [12-14] and access control policies. |
| **4.** | Carry out version management, change management and configuration management for the production system |
| **5.** | The production environment is completely isolated from the test environment. |

| **RQ-13-01** | For a network security emergency event, the network security emergency response plan created should include |
|----------------|--------------------------------------------------------------------------------|
| **1.** | Remedial measures for network security emergencies |
| **2.** | Communication mechanism during emergency response (including internal and external communication partners) |
| **3.** | Assign responsibility for remedial action |
| **4.** | Method of judging process |
| **5.** | Emergency response termination conditions and termination actions |
RQ-13-02 | Track the status of network emergency incident recovery | 1. Have clear responsibility for network security emergency response  
2. Perfect processing procedures and methods  
3. Regular progress report after the emergency  
4. Experience and lessons learned after the event  
5. The cause of the incident

RQ-13-03 | Information related to network security emergency events should be related to emergency events | 1. Affected assets (e.g. part number, system description and number of affected assets);  
2. Relevant emergencies and vulnerabilities;  
3. Investigate forensics information such as log data and crash data;  
4. Feedback from end users.  
5. Emergency measures

RQ-15-01 | For distributed activities, this standard shall be used to evaluate the ability of the supplier to perform relevant activities during, if applicable, and after development | 1. Evidence used to demonstrate an organization's cybersecurity capabilities (e.g., cybersecurity best practices in development, post-development, governance, quality, and cybersecurity);  
2. Evidence used to prove that an organization can carry out sustainable cybersecurity activities;  
3. Summary of past network security assessment;  
4. Audit results at the organizational level;  
5. Proof of cybersecurity management system;

RQ-15-03 | Customers and suppliers should specify their own network security activities in the network security work interface | 1. Appoint contacts for cybersecurity customers and suppliers  
2. Identify network security activities that need to be performed by customers and suppliers respectively  
3. Relevant information and work results shall be Shared, including distribution, review and feedback mechanism in case of network security problems  
4. Set milestones for customer and supplier cybersecurity activities  
5. Define the termination of network security support for related items or components.

4. Summary
By studying the ISO 21434 standard, this paper analyzes the requirements of road vehicle information safety system, and puts forward the evaluation method to judge whether the automobile company meets the requirements of this information safety system. The cybersecurity evaluation system based on ISO 21434 standard also provides an important reference for the analysis of the cybersecurity system of road vehicles.

References
[1] Chen.C, Han.WL, Wang.X; VANET overview of security technology[J]; A small microcomputer system, 2011,32(5):896-904.
[2] Suchen Jiang, Research on the development trend of intelligent automobile enterprises[J]. engineering technology: The full version, 2016(11): 00318-00318
[3] Tian.M, Wang.S, Cai.L, Research on vehicle network security protection[J], Computer knowledge and technology: academic exchange, 2017, 13(6): 72-75.
[4] Miller C, Valasek C. Adventures in automotive networks and control units[J]. Black Hat USA, 2013, 21: 260-264.
[5] Miller C, Valasek C. A survey of remote automotive attack surfaces[J]. Black Hat USA, 2014.
[6] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle[J]. Black Hat USA, 2015.

[7] Liu XM, Yu GC, Chen SY. Study on safety regulation strategy and standard of vehicle network[J]. Information and communication technology and policy, 2018(8): 51-53.

[8] Sun YP, Tian HR. Research progress on the standardization of network security of Internet of vehicles[J]. Telegraph communication network technology, 2017(6): 18-21.

[9] Sun H, Xie HG, Wang Z. The construction of intelligent network automobile information security standard system and industrial policy research[J]. China automobile, 2018(12): 38-43.

[10] CESI. White paper on standardization of automotive electronic network security (2018 edition). http://www.cesi.ac.cn/201804/3790.html, 2018-04-16.

[11] ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering, ICS: 43.040.15 Car informatics. On board computer systems.

[12] D. Nilesh, M. Nagle. The new cryptography algorithm with high throughput. Computer Communication and Informatics, 2014 International Conference on, IEEE, 2014. 1~5

[13] A. M. Atteya, A. H. Madian. A hybrid Chaos-AES encryption algorithm and its impelmention based on FPGA. New Circuits and Systems Conference, IEEE, 2014. 217~220

[14] V. Kaul, P. Choudhari, S. K. Narayankhedkar. Security enhancement for data transmission in 4G networks. 5th International Conference on Confluence the Next Generation Information Technology Summit, IEEE, 2014. 373~378