On the Criteria for Cybersecurity and Risk Assessment Based on ISO/SAE 21434 for the Application of Autonomous Vehicle

Cybersecurity for the Application of Autonomous Vehicle

Yi Liu[1, a], Xuezhu Yang[1, b], Muxi Li[1, c*], Miao Wu[1, d], Chengrui Sun[1, e], Shiying Zhou[2, f]

[1]E&E Research Department of Intelligent Connected Vehicle Development Institute, FAW, China
[2]General Research and Development Institute, FAW, China

[a]liuyi7@faw.com.cn
[b]yangxuezhu@faw.com.cn
[c]limuxi@faw.com.cn
[d]wumiao@faw.com.cn
[e]sunchengrui@faw.com.cn
[f]zhoushiying@faw.com.cn

Abstract. Recently, as research on autonomous driving technology progresses, the supply of vehicles having various autonomous driving functions is increasing, and autonomous vehicles represented by V2V (Vehicle to Vehicle) and V2X (Vehicle to Everything) are emerging. For the era of autonomous driving, connectivity between vehicles and vehicles, vehicles and the surrounding environment is required based on information and communication technologies such as LTE, 5G, and WiFi. Advances in autonomous driving technology also face new challenges, with security emerging as a top concern as it can become a prime target for cyberattacks as the vehicle's external networks and connections increase. Therefore, it is necessary to derive the defense requirements in software to respond to such malicious attacks, and it is necessary to apply the verified security coding standard during software development. Recently, the ISO/SAE 21434 international standard replacing SAE J3061 has been established and published in relation to cyber security. In this paper, we propose criteria for cybersecurity and risk assessment methods. In addition, a case study confirms the suitability of the risk level determination according to the proposed evaluation factors and criteria.

Keywords: ISO/SAE 21434; Cyber Security; Autonomous Vehicle; Functional Safety; Risk Assessment

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 134–143, 2022.
https://doi.org/10.2991/978-94-6463-108-1_16

1 Introduction

Today, automobiles depend on electric/electronic products due to the introduction of autonomous driving and connected vehicles. As communication technology develops, vehicle systems, vehicles and vehicles, and vehicles and infrastructure have begun to be connected as shown in Figure 1, and the use of connection functions and information sharing for various functions such as vehicle maintenance and traffic safety is increasing.

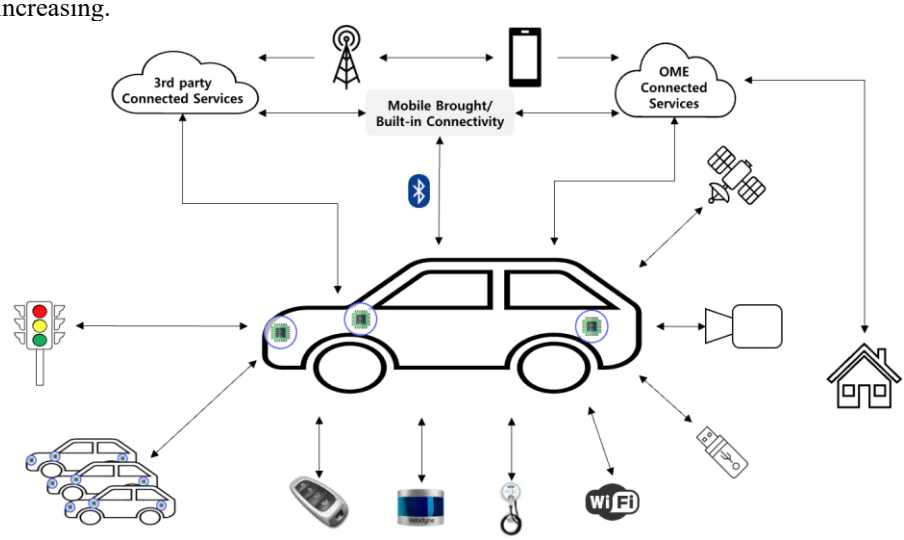

Fig. 1. Connectivity between vehicles and various infrastructures

However, this increase in vehicle connectivity has a vulnerability to cyber attacks. For example, in 2005, at the White Hacker Conference called Blackhat & DEFCON, a remote hacking of a car was demonstrated to abnormally operate the wiper and stop the engine [1]. As the connectivity of vehicles increases, the threat caused by cyber attacks increases, and the need for security is also recognized naturally.

A systematic mapping study was performed to identify the existing software security approaches used in the software development life cycle and to identify key studies on the use of software security technologies [2]. Various methods of attacking and defending autonomous vehicles were constructed and discussed, and to better classify each a comprehensive attack and defense taxonomy was proposed. This has provided a better understanding of the deployment of targeted defenses against targeted attacks [3].

An attack surface assessment focusing on the attack feasibility rating that conforms to the ISO/SAE 21434 standard was presented and introduced the attack potential rating for assets and the application of this rating to common use cases [4]. A comprehensive literature review was performed on the existing research on cyber-physical system security, and a systematic study was conducted. In addition, we proposed a method to explore general CPS functions through a framework consisting of three orthogonal

coordinates: a security perspective, a CPS component perspective, and a CPS system perspective [5].

A review of the draft of ISO/SAE 21434 was performed and a position was provided for discussion of the recommendations presented in the analysis methods and standards [6]. It describes the ISO 21434 standard and security engineering approach to enhance vehicle security in response to the increasing adoption of ICT in vehicles, and suggests several research directions for realizing the proposed approach in operational environments [7]. Based on a model-based approach, a method for performing cybersecurity risk analysis in automotive areas compliant with ISO 21343 standards was presented and a rich goal-oriented meta-model to capture automotive asset and system characteristics, estimate the impact of damage scenarios, identify threats, and evaluate feasibility was proposed [8].

It was argued that connected and autonomous vehicles can be subjected to various attacks that pose a serious risk to safety by malicious attackers, and a comprehensive investigation on cyber security was conducted to solve these security problems [9]. An investigation was conducted to see if there is a cybersecurity vulnerability in autonomous and unmanned vehicle systems, and development guidelines and mitigation strategies to be used in the development of autonomous and unmanned vehicle systems by identifying and classifying threats and attacks exploiting the vulnerability [10]. A systematic study was conducted on the security threats surrounding autonomous driving from the angle of vehicle perception, navigation and control, and the corresponding defense strategies were presented along with an in-depth overview of the threats [11]. A blockchain-based security and distributed CAV architecture was proposed as a method to solve the weak security and privacy problems of CAV against various cyber attacks [12].

In this paper, standards for cyber security and risk assessment methods are presented, and a study was conducted to confirm the suitability of risk level determination according to the proposed assessment factors and standards through case analysis.

2 Functional safety and cybersecurity at the vehicle level

ISO/SAE 21434 “Road Vehicles – Cybersecurity Engineering” is the automotive security standard of the future and is important to automotive product development and all related processes. It can be said that the target of cyber security in the automotive field is not only major OEMs, but also all related partners (parts, systems, subsystems, SW, related infrastructure, etc.) that develop vehicles or are involved in the entire vehicle lifecycle [13]. The scope of ISO/SAE 21434 covers electrical/electronic systems of road vehicles, hardware and software, interfaces, as well as systems that are connected (or connected to) external equipment and networks.

2.1 Analysis for Deriving Security Goals

One of the most important outputs of ISO 26262 is the Safety Goal and ASIL, and cybersecurity also requires activities to establish the Security Goal in a similar context. Just as in ISO 26262, ASIL is determined through HARA, in ISO 21434, securi-

ty goals can be derived through TARA. Figure 2 shows the relationship between ISO 26262 and ISO 21434 on cybersecurity.

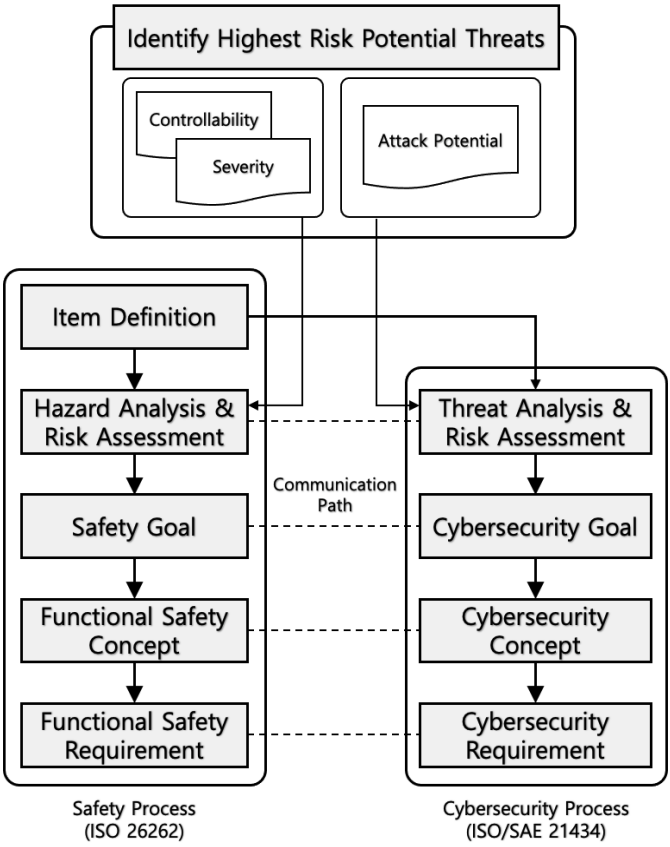

Fig. 2. Relationship between ISO 26262 and ISO 21434 on Cybersecurity

As mentioned in the figure, the derivation of the Security Goal and the Safety Goal is carried out in the form of paralleling the Safety Process and the Security Process, and the relationship shown in Figure 3 is shown. The security requirements are derived from the security objectives, and the security objectives identified in the risk analysis contribute to the safety objectives.

In other words, ISO/SAE 21434 aims to define the process and activity requirements required for evaluation from the cybersecurity perspective of automotive electrical/electronic systems, and to establish electrical and electronic engineering measures to prepare for various attack techniques and new attack technologies through a risk-based approach.

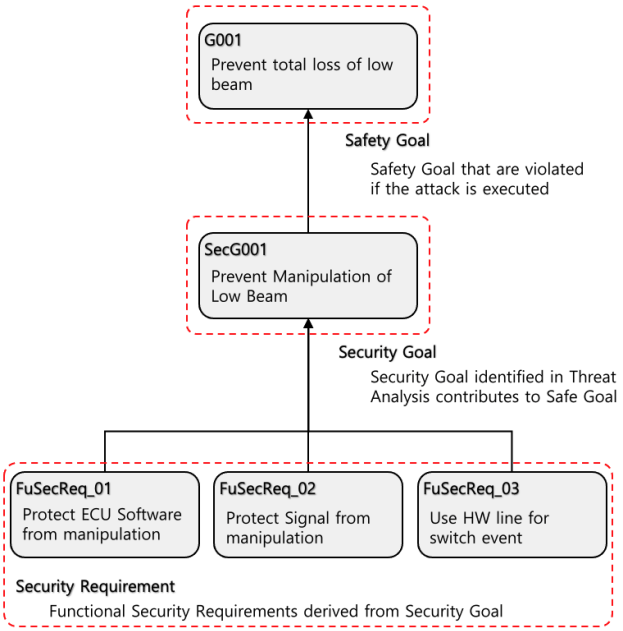

Fig. 3. Relationship between Safety Goal and Security Goal

2.2 Risk Assessment

Figure 4 shows the procedures for risk analysis and risk assessment methods required by ISO 21434. First, an item is defined to define the scope of the component, and the assets of the system are identified by referring to the defined scope. Based on the identified assets, it defines risk scenarios that can affect it from various perspectives and analyzes paths that can be attacked by malicious attackers. Based on the results from attack path analysis, the likelihood of attack and the impact of the attack are determined, and the risk level is finally determined.

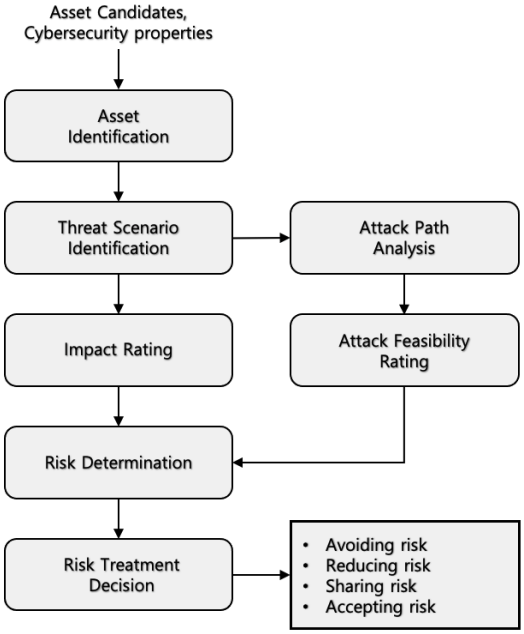

Fig. 4. Relationship between Safety Goal and Security Goal

The following five evaluation factors are applied to assess the risk of cyberattacks.

- Elapsed time
- Attacker expertise
- System knowledge required
- Window of opportunity
- Equipment required

Based on the above five evaluation factors regarding information provision, security risks are determined from a matrix with two inputs:

- Attack Probability – exposure, likehood
- Impact – environemental, financial, safety, operational consequences

Table 1. Risk level Scale based on impact ratings and potential attacks

		Attack Possibility			
		Very Low	***Low***	***Medium***	***High***
Impact	***Negligible***	A	A	A	B
	Moderate	A	A	B	C
	Serious	A	B	C	D
	Severe	B	C	D	D

Based on the score criteria assigned to the evaluation factors, the potential attack risk and attack potential are calculated, and then the risk level is determined as shown

in the table. Table 1 shows that the risk level increases from A to D. Depending on the determined risk level, risk treatment measures can be planned and implemented.

3 Feasibility evaluation using vehicle power supply system

Based on the previously proposed risk assessment factors and evaluation criteria, we verify the suitability by applying risk level determination to DC voltage conversion controllers applied to real vehicles. Figure 5 shows the configuration of the DC voltage conversion controller environment.

The main function of the DC voltage conversion controller is to convert a high voltage of a battery cell into a 12 V voltage and supply operating power to the controller. If the DC voltage conversion controller is attacked by a malicious attacker, it may not perform normal functions or perform incorrect functions, causing the vehicle to lose its power source, which could endanger the driver while driving.

To verify the risk level scale defined in Table 1, the experiment was performed with the following procedure.

1) Identify risk scenarios caused by cyber attacks
2) Grading by impact rating and attack frequency for each identified scenario
3) Measurement of risk level scale according to impact rating and attack potential

As a method of attacking the DC voltage conversion controller, it is possible to use unauthorized equipment to tamper with software programs, or to insert malicious code or tamper with programs directly in the process of development or mass production by internal employees. In addition, it is possible to attack by disguising the Gateway and TCU and delivering an incorrect message to the DC conversion controller. Table 2 shows the level of risk determined based on the severity of damage and the probability of occurrence of these attacks. As shown in Table 2, as the connectivity of vehicles increases, the impact of attacks that transmit wrong messages through the network is severe, and the frequency of occurrence is also not low, confirming that the risk level scale is high. In addition, attacks that modulate SW programs by directly connecting equipment have a serious impact, but the frequency of attacks is low, indicating that the risk level scale is relatively low.

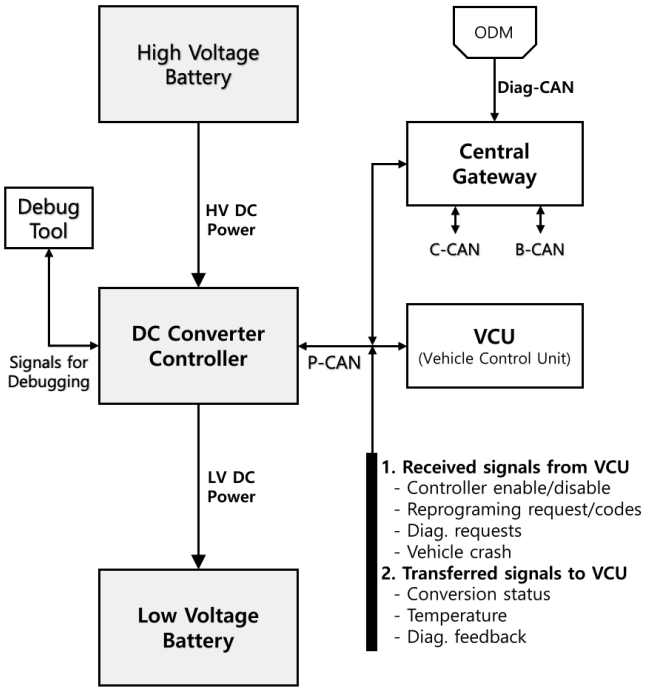

Fig. 5. DC voltage conversion controller environment

Table 2. Risk Level Scale Application Results

Attack Methods	Impact	Attack Possibility	Security Risk
Modulating the S/W Program of the controller using unauthorized equipment	Serious	Low	B
Physically direct connection to insert malicious code and modulate the S/W program	Serious	Very Low	A
Unauthorized personnel use the Debugging Tool to insert malicious code and modulate the S/W program	Serious	Low	B
Incorrect message transmitted to DC voltage converter via unauthorized Gateway and TCU spoofing	Severe	Medium	D
Unauthorized user access through externally exposed JTAG port	Severe	Very Low	B

4 Conclusion

The development of communication technology and autonomous driving technology has expanded the connectivity of automobiles, thereby increasing the possibility of external attacks. ISO/SAE 21434 international standard, which replaces the existing SAE J3061, was established and published to establish cyber security goals and requirements suitable for automobiles. The ISO/SAE 21434 standard is recommended not only for major OEMs in the automotive sector, but also for all relevant partners that develop vehicles or are involved in the entire vehicle lifecycle.

In this study, we analyzed cyber security at the vehicle level and presented a scale for evaluating the risk level based on potential attack risk and attack potential in relation to cyber attacks. The suitability was verified by applying the method of deriving the risk level scale presented in this paper to the method of attacking the DC voltage conversion controller.

References

1. Miller, C., & Valasek, C. “Remote exploitation of an unaltered passenger vehicle”, Black Hat USA, 2015.
2. Mohammed, N. M., Niazi, M., Alshayeb, M., & Mahmood, S. “Exploring software security approaches in software development lifecycle: A systematic mapping study.” Computer Standards & Interfaces, 50, pp. 107-115, 2017.
3. Thing, V. L., & Wu, J. “Autonomous vehicle security: A taxonomy of attacks and defences.” In 2016 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata), IEEE, pp. 164-170, 2016.
4. Plappert, C., Zelle, D., Gadacz, H., Rieke, R., Scheuermann, D., & Krauß, C. “Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain.” In 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, pp. 266-275, 2021.
5. Humayed, A., Lin, J., Li, F., & Luo, B. “Cyber-physical systems security—A survey.” IEEE Internet of Things Journal, 4(6), pp. 1802-1831, 2017.
6. Macher, G., Schmittner, C., Veledar, O., & Brenner, E. “ISO/SAE DIS 21434 automotive cybersecurity standard-in a nutshell.” In International Conference on Computer Safety, Reliability, and Security, Springer, Cham, pp. 123-135, 2020.
7. Dantas, Y. G., Nigam, V., & Ruess, H. “Security engineering for ISO 21434.” *arXiv preprint arXiv:2012.15080*, 2020
8. Ponsard, C., Ramon, V., & Deprez, J. C. “Goal and Threat Modelling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO/SAE 21434.” In SECRYPT, pp. 833-838, 2021.
9. Sun, X., Yu, F. R., & Zhang, P. "A survey on cyber-security of connected and autonomous vehicles (CAVs)." IEEE Transactions on Intelligent Transportation Systems, 2021.
10. Yağdereli, E., Gemci, C., & Aktaş, A. Z. "A study on cyber-security of autonomous and unmanned vehicles." The Journal of Defense Modeling and Simulation, 12(4), pp. 369-381, 2015.

11. Ren, K., Wang, Q., Wang, C., Qin, Z., & Lin, X. “The security of autonomous driving: Threats, defenses, and future directions.” Proceedings of the IEEE, 108(2), pp. 357-372, 2019.
12. Gupta, R., Kumari, A., & Tanwar, S. “A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles.” Transactions on Emerging Telecommunications Technologies, 32(6), e4009, 2021.
13. ISO - International Organization for Standardization. ISO/SAE DIS 21434 Road Vehicles - Cybersecurity engineering, 2020.