Wireless Networks (2024) 30:4591–4605
https://doi.org/10.1007/s11276-022-03084-9

PIER: cyber-resilient risk assessment model for connected and autonomous vehicles

Seunghyun Park[1] · Hyunhee Park[2]

Accepted: 11 July 2022 / Published online: 10 August 2022

Abstract

As more vehicles are being connected to the Internet and equipped with autonomous driving features, more robust safety and security measures are required for connected and autonomous vehicles (CAVs). Therefore, threat analysis and risk assessment are essential to prepare against cybersecurity risks for CAVs. Although prior studies have measured the possibility of attack and damage from attack as risk assessment indices, they have not analyzed the expanding attack surface or risk assessment indices that rely upon real-time resilience. This study proposes the PIER method to evaluate the cybersecurity risks of CAVs. We implemented cyber resilience for CAVs by presenting new criteria, such as exposure and recovery, in addition to probability and impact, as indices for the threat analysis and risk assessment of vehicles. To verify its effectiveness, the PIER method was evaluated with respect to software update over-the-air and collision avoidance features. Furthermore, we found that implementing security requirements that mitigate serious risks successfully diminishes the risk indices. Using the risk assessment matrix, the PIER method can shorten the risk determination time through high-risk coverage and a simple process.

Keywords Risk assessment · Cyber-resilience · Connected and autonomous vehicles (CAVs) · PIER

1 Introduction

As vehicles are evolving into large smart devices connected to the Internet, the autonomous features they are equipped with dramatically change the mobility of vehicle users [1]. However, behind this convenience, new security threats that have not been considered in conventional vehicles have emerged. More specifically, the connectivity of Internet-equipped vehicles leaves them open to public allowing hackers to exploit malicious attempts [2–4]. In particular, the security vulnerabilities of the IT environment, such as those of computer systems and networks, are becoming major threats for connected vehicles. Furthermore, fully autonomous vehicles require higher safety and security measures because even minor security flaws or malfunctions can cause accidents involving many human casualties.

Current vehicle security-related regulations and standards [5–7] define cybersecurity threat analysis and risk assessment (TARA) for vehicles as important processes. However, they do not provide important criteria or evaluation standards that should be considered in each step of actual TARA. Therefore, they rely on the policies and capabilities of manufacturers and suppliers. The e-safety vehicle intrusion protected applications project (EVITA), jointly developed by European automobile manufacturers and suppliers, presents a reliable security framework for vehicle communication using the in-vehicle network (IVN), which is an on-board system. Remote attackers can take control of a vehicle by accessing connected vehicles through the wireless network, taking over the rights, and manipulating control software or messages. It implies that there is difficulty in sufficiently analyzing and evaluating

✉ Hyunhee Park
hhpark@mju.ac.kr

Seunghyun Park
sp@hansung.ac.kr

[1] Division of Computer Engineering, Hansung University, 116, Samseongyo-ro 16-gil, Seongbuk-gu, Seoul 02876, South Korea

[2] Department of Information and Communication, Myongji University, 116, Myongji-ro, Cheoin-gu, Yongin-si 17058, Gyonggi-do, South Korea

cybersecurity threats and risks [8–12] in the interaction between connected vehicles and external entities.

Existing research on vehicle cybersecurity [13–21] focused on preventing unauthorized external access to the internal network by setting a boundary section [22]. However, these methods differ from the paradigm shift of cybersecurity to fast detection and recovery against advanced cyber-attack technologies in a rapidly developing IT environment. Instead of operating in a closed environment, vehicle networks are now connected to external cloud infrastructure, smart devices, grids, and other connected and autonomous vehicles (CAVs) for interaction. Thus, the fundamental defense strategy against the IVN is no longer valid [23]. According to the actual cases of vehicle cyber incidents [24–26], attackers remotely analyze the external communication of vehicles for a period of one year or longer and manipulate software through the network. Moreover, they seek vulnerabilities of the IVN or control software by injecting messages to gain unauthorized access. If an incident occurs as a result of long-term analysis, defenders need strategies and methods for fast recovery based on real-time analysis and actions so that these attacks do not lead to personal injury or financial loss [27].

Considering the changing cybersecurity paradigm of IVN, this study defines four criteria for the risk assessment of CAVs: probability, impact, exposure, and recovery. In particular, this study considers exposure items to prevent cyber incidents and recovery criteria to measure rapid resilience, in addition to the widely-used probability and impact. Cyber resilience is reflected in the safety and security of vehicles by evaluating the prevention of cyber threats and real-time follow-up measures for CAVs according to these criteria. Furthermore, we propose evaluation items and metrics based on these criteria and derive evaluation indices to reinforce security by assigning weights to controllable items. In addition, the target scope is expanded to communication and infrastructure to derive security requirements of the vehicle, communication, and infrastructure linkage areas, which could not be derived in prior studies.

The rest of this paper is organized as follows. Section 2 summarizes related studies of various conventional methods for security risk assessment in-vehicle environments. Section 3 introduces the PIER method, the risk assessment method proposed in this study, and explains the four primary criteria: attack probability, impact, exposure, and recovery, and evaluation metrics presented in this method. In particular, cyberattack response levels can be improved by weighting the controllable factors for security in CAVs and creating indices to remove threats and enhance resilience in advance. In Sect. 4, the cybersecurity risks for CAVs are evaluated by applying the proposed PIER method to automotive over-the-air (OTA) software update and collision avoidance, which are two significant features of connected vehicles (CVs) and autonomous vehicles (AVs). In Sect. 5, risk mitigation is verified by suggesting and re-evaluating security requirements that can reduce risk indices for major threats and risks derived from the previous cyber risk assessment. In addition, the proposed method is validated by comparing its coverage and performance with those of conventional methods. Finally, Sect. 6 presents the core security control factors for CVs and AVs derived in this study as key findings and summarizes the proposed method.

2 Related work

This section examines and compares the major characteristics of prior studies on the risk assessments of CVs, AVs, and CAVs.

Cui and Zhang [28] proposed the VeRA model to perform a simplified risk assessment for AVs, characterized by including human control in the risk assessment criteria and attack probability and severity. Probability was defined in three levels by combining the attacker's knowledge and the equipment usage, whereas severity was defined as in SAE J3061 [7]. This index is similar to the impact index in other existing studies. The authors newly defined human control based on the automation level and human capacity of AVs, as defined in SAE J3016 [29]. However, objective criteria for measuring the driver's ability in three levels are insufficient.

ISO/SAE 21434 [6] presents the metrics of attack impact and feasibility and an example to derive the risk value from the TARA methods. Four major attributes, that is, safety, financial, operational, and privacy damage, were used to assess impact according to four damage scenarios. The impact ratings of each attribute were classified into four grades according to each criterion. For attack feasibility, attack potential, common vulnerability scoring system, and attack vector were used. For each sub-attribute, the impact was evaluated according to different criteria from one to five. This assessment scheme is meaningful as it refers to standards related to each attribute. However, the process is complex and challenging to quickly apply because the various indices required by each standard must be evaluated in advance, as mentioned by Cui and Zhang [28].

Kelarestaghi et al. [30] proposed an impact-oriented risk assessment for IVN in the security of intelligent transport systems. Their proposal applied the risk model defined in the National Institute of Standards and Technology Special Publication 800-30 [31]. Risks that can influence a damaged IVN are classified into seven risk categories and subcategorized further to indicate the negative impact on the transportation network. This method uses five levels of likelihood and impact as a matrix to classify risk assessment into five risk clusters. However, the criteria (very low, low, moderate, high, and very high) of impact and likelihood ratings for each element are unclear, and results may differ depending on the situation or analyst.

Strandberg et al. [32] proposed start, predict, mitigate, and test (SPMT) as a method to predict and mitigate the vulnerabilities of vehicles for the analysis of vehicle security. SPMT consists of four phases, and the actual risk assessment is performed in the predictive phase. Predictions are made in accordance with the Common Vulnerabilities and Exposures database and STRIDE threat model, and risk is calculated by multiplying the prediction result by its probability. The SPMT process has a virtuous cycle that predicts threats in each phase, mitigates them, and reassesses them. However, the six measures calculated by a simple product of the two indices have limitations when a detailed assessment is required, as they are significantly simplified.

Kong et al. [33] suggested a framework for evaluating smart car security by calculating the risk of three grades through the arithmetic product of asset, threat, and vulnerability analysis. The asset index partly transformed the severity evaluation of the EVITA project, and the asset value is determined by considering the highest impact among the three categories of safety, privacy, and operationality. The threat is calculated from the attack tree, and vulnerability is calculated using the probability of vulnerability and event occurring in a way similar to that performed for threat calculation. Unlike in prior methods, impact and probability are inherent in these indices. However, this framework assumes an equal possibility for every threat without environmental and technical limitations for every case of vulnerability specified in the attack tree. Thus, this method has limitations in realistic risk classification and evaluation.

Prior studies evaluating vehicle security commonly utilized the probability of attack and the resulting impact as factors in risk assessment. However, existing evaluation criteria do not sufficiently apply the connectivity property of CVs that allows attackers to access the IVN using an open wireless channel or the autonomous property of AVs that analyzes the driving context and determines vehicle control by merging various sensing data. This study proposes the PIER method, which performs threat analysis by considering exposure for reliable internal and external connections, and recovery for immediate detection of and restoration from attacks, as risk assessment factors, in addition to the existing indices for probability and impact.

3 PIER method

The quantitative risk and resilience assessment method proposed in this study evaluates the vulnerability of CAVs to threats, the probability of attack by such threats, the impact of results derived when an attack occurs, and the recovery method for returning a risk state to a normal state.

3.1 Process

The overall process performs risk assessment by applying risk factors and PIER criteria to analyze the CAVs functionalities, as depicted in Fig. 1. The main functionalities of CAVs include automotive OTA and collision avoidance, as shown in Fig. 1(a). In-vehicle components interact with the external entities and can be exposed as attack surfaces from the connectivity properties. In Fig. 1(b), the PIER methodology presented in this study is applied to the main functionalities that require risk assessments. This method evaluates risk criteria based on the risk factors in each risk category: probability, impact, exposure, and recovery. Section 3.2 describes these major risk categories composing the risk matrix in four subsections. Each risk criteria is covered in detail in Table 1 of Sect. 3.3. Risk factors that cause high risk derive security requirements to mitigate them as countermeasures, as shown in Fig. 1(c). The PIER method finally determines the risk level by applying the previously derived security requirements to the main functionalities in the risk assessment stage again in Fig. 1(d).

3.2 Risk categories

3.2.1 Probability: *P*

Probability is the likelihood of actual attack occurrence according to the attacker's effort and the defender's proactive action. This is closely related to the skills required for the attack, the preparation cost, and the configuration of the defense system. Attackers can attempt an assault with little effort and time if an attack using known techniques is valid. When the hurdles to an attack are low, an easily attempted valid attack makes an incident. This is a considerable risk to the target system.

The PIER model measures the probability using the following Eq. (1) based on the required skill, preparation time, and essential defense system.

$$Probability = \min_{\alpha} \max_{\beta} \left[\sum_{i}^{n} \eta_i \cdot \left(\frac{P_i}{n} \right)^2 \right], \tag{1}$$

where the measurement items, n, mean the number of risk factors P_i in each risk category P. The risk factor is

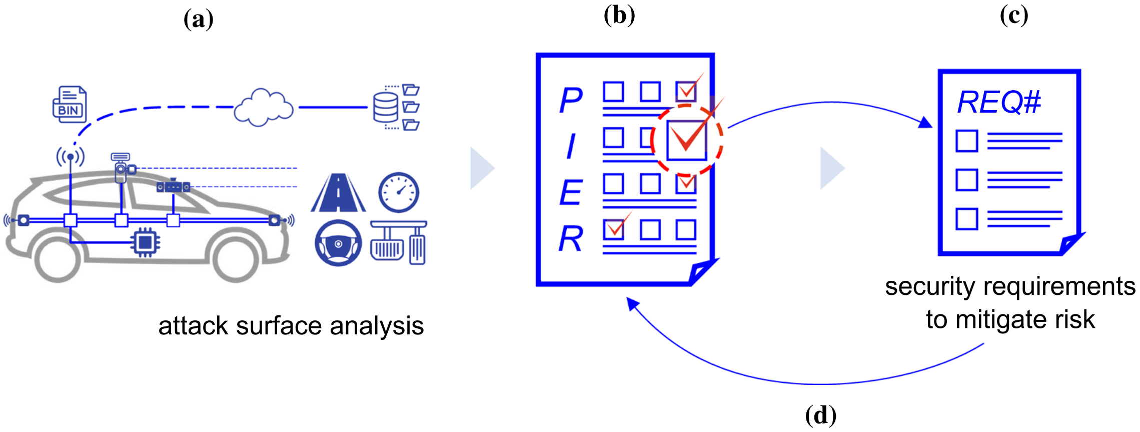


Fig. 1 The overall process of PIER method: **a** automotive software update over-the-air (OTA) and collision avoidance as main functionalities of a connected and autonomous vehicle, **b** PIER risk assessment based on the risk categories, risk factors, and each criterion, **c** security requirements to mitigate the risk as countermeasures, and **d** reassessment risk to determine the final security risk

evaluated as low, medium, or high. A predefined weight matrix η_i is applied to the controllable factor $\exists P_i^*$.

The PIER method sets the minimum value α of the risk level to one and the maximum value β to three to rate all risk categories into three levels of classes, respectively. Also, it is applied the weight of 1.5 by multiplying the weight vector in each risk category. For example, the weight vector η becomes $[1, 1, 1.5]$ in the case of the probability factors for P_1, P_2, and P_3^*, when P_3^* is a controllable weighted factor.

3.2.2 Impact: *I*

Impact refers to the damage caused by an attack. A CAV is a safety-critical and mission-critical system simultaneously. If a remote attack directly affects the driveline of a moving CAV, the driver may lose control of the vehicle with unintentional acceleration, braking, or steering. The impact of this loss of driveline control caused by cyber attacks is more severe than the simple inconvenience caused by malfunctions in the audio or air conditioning systems. The impact of potential harm is high if the result of a cyberattack is directly connected to the safety of passengers or other road users. Furthermore, even when a cyberattack does not directly affect the passengers' safety, it may still have a critical impact on business, especially when the recovery process consumes more procedures, time, and cost than expected.

The PIER model measures the impact using the following Eq. (2) based on the resulting damage, the target of the damage, and the recovery time from a cyberattack.

$$Impact = \min_{\alpha} \max_{\beta} \left[\sum_{i}^{n} \eta_i \cdot \left(\frac{I_i}{n} \right)^2 \right], \tag{2}$$

where the measurement items, n, mean the number of risk factors I_i in each risk category I. The risk factor is evaluated as low, medium, or high. A predefined weight matrix η_i is applied to the controllable factor $\exists I_i^*$.

3.2.3 Exposure: *E*

Exposure indicates the likelihood that the attack vectors of the CAV are exposed to attackers. Hackers consider the reachability to the target, exploitation of known vulnerabilities, and the possibility of spreading damage when establishing a strategy for an efficient attack.

Reachability refers to the ability of a hacker to connect directly or indirectly to an attack target. An attacker can access the target through network scanning if the target is exposed to the Internet or a public network. Even if the attacker is not connected directly to their target, they can indirectly access the system step by step by gaining authority over an intermediate system through a different network. However, this requires more time and effort than direct access. Therefore, it is crucial to accurately identify possible attack routes and the reachability of the target for effective defense and risk assessment.

Furthermore, known or unsolved vulnerabilities can deteriorate the security of the system. Unlike in conventional IT systems, known vulnerabilities inherent in embedded software provide hackers with attack vectors because of its longer patching cycles and the difficulties of fixing vulnerabilities in real-time. Therefore, carrying a known vulnerability in such an environment means easy exposure of attack vectors to hackers.

The accessibility is evaluated in terms of the perspective of whether an attack conducted by a hacker to take over the authority of a vehicle can be simultaneously applied to a large number of unspecified vehicles at a remote location.

Table 1 Criteria of risk factors

Category	Risk factors	Criteria
Probability	P_1: required skill	Using existing known toolkits
		Modifying attack toolkits to discover new vulnerabilities
		Capable of discovering new categories of vulnerabilities
	P_2: preparation time	Short-term preparation under a week
		Mid-term preparation under a month
		Long-term preparation over a month
	P_3^*: defense system	Monitoring 24 × 365 with vehicle backends required
		Essential security systems
		Non-deployment of security system
Impact	I_1: damage result	Directly related to occupant safety
		Financial loss or compliance violation
		User inconvenience
	I_2: damage target	Drivetrain
		Control devices, e.g., airbag operation and door opening
		Convenience devices, e.g., air conditioning and audio
	I_3^*: recovery time	Response delay over an hour
		Post-recovery within an hour
		Proactive or real-time
Exposure	E_1^*: reachability	Direct access to an unspecified number of vehicles
		Remote access to authorized requests
		Decomposition that requires physical occupancy
	E_2: exploitable vulnerabilities	Publicly disclosed general vulnerabilities
		Disclosed vulnerabilities to automobiles
		Undisclosed vulnerabilities to automobiles
	E_3: accessibility	All unspecified access
		Remote access via network link
		Physical occupancy required
Recovery	R_1^*: ease to detection	Post action after damage
		Real-time response
		Prevent in advance
	R_2: patch means	Manual patching in all cases
		Patching in batch
		Kill chain defense not patching required
	R_3: supply chains	Replacement of the current partnership
		License or coverage extension
		Leverage existing supply chains

The risk factors that the defender can control, i.e., P_3^*, I_3^*, E_1^*, and R_1^* have weights

The risk is extremely high if the server transmitting control commands to remote vehicles are exposed to the Internet and grants permission to hackers because the attack can spread to an unspecified number of CVs. However, the spread risk is low because each new target would require a similar amount of effort to attack if physical possession is assumed or the target vehicle is specified through the network.

The PIER model measures the exposure using the following Eq. (3) based on the reachability to the target, exploitable vulnerabilities, and accessibility to spread damages.

$$Exposure = \min_{\alpha} \max_{\beta} \left[\sum_{i}^{n} \eta_i \cdot \left(\frac{E_i}{n} \right)^2 \right], \tag{3}$$

where the measurement items, n, mean the number of risk factors E_i in each risk category E. The risk factor is evaluated as low, medium, or high. A predefined weight matrix η_i is applied to the controllable factor $\exists E_i^*$.

3.2.4 Recovery: *R*

Recovery refers to the ability to recover a system from damage caused by cyberattacks to a normal state. In a cyberattack, delays in appropriate action increase the degree of damage and loss exponentially. Therefore, it is essential to detect attacks quickly and take appropriate measures. The defender must consider the detection capabilities, patch methods, and supply chain coverages for early detection and fast responses.

Detection capability is determined by the presence of a monitoring system that can recognize threats in advance or in real-time to respond to cyber-attacks immediately. In a conventional IT environment, abnormal access attempts are monitored by mirroring the security system logs such as firewalls and intrusion detection and prevention systems (IDPSs). Even a CAV environment requires the system to detect malicious traffic in network communication and analyze attack behaviors effectively. Ideally, it is necessary to block threats in advance by the analysis result before the actual attack behavior occurs. However, it is realistic for the CAV to establish strategies through real-time detection and immediate response, considering the characteristics of the mission-critical system.

The patch method is evaluated to determine whether it can collectively patch vulnerabilities inherent in CAVs or related systems. An effective defense neutralizes attacks with a preemptive response system that blocks the attackers' intrusion kill chain [34]. Furthermore, it is crucial to quickly prepare and spread a patch to the target systems when vulnerabilities are exploited. When updating the controller software, a conventional automobile requires a physical connection to a diagnostic device. Because these vehicles are manually processed, the spread cycle is significantly longer, and the completion rate of actions is low; thus, vulnerabilities discovered in this system remain risk factors for an unspecified amount of vehicles. CAVs utilize automotive OTA technology [35] for efficiently and simultaneously distributing patched software to multiple CVs.

Supply chain performance [36] evaluates the dependence of the existing supply network and the external entities on the defense against attack and acting on any vulnerabilities. When a vehicle can respond to cyberattacks without requiring additional costs, outside resources, or changes in the supply network, it implies that its defense is relatively fast. However, additional time is required if an additional budget is required for defense or to change the contract, such as a license extension. It may take more time to find the different partnerships beyond the existing supply chain [37]. Therefore, it is essential to manage the supply chain for efficient operation with comprehensive coverage.

The PIER model measures the recovery using the following Eq. (4) based on the attack detection capability, patch methods, and supply chain performance.

$$Recovery = \min_{\alpha} \max_{\beta} \left[\sum_{i}^{n} \eta_i \cdot \left(\frac{R_i}{n} \right)^2 \right], \tag{4}$$

where the measurement items, n, mean the number of risk factors R_i in each risk category R. The risk factor is evaluated as low, medium, or high. A predefined weight matrix η_i is applied to the controllable factor $\exists R_i^*$.

3.3 Risk assessment criteria

The PIER model evaluates risks using four categories: the degree of being exposed to threats of cyber-attack; the probability of actual attacks from these threats; the impact of damage as a result of the attack; and the ability to recover from the damage of the attack. Three major risk factors are defined for each category, and the corresponding response levels are evaluated according to the three criteria of high, medium, and low. In particular, assigning weights to items that allow the defender to control the cybersecurity environment and remove threats in advance improves the defender's cyberattack response level. Table 1 shows the evaluation criteria and weight matrix of the major risk factors.

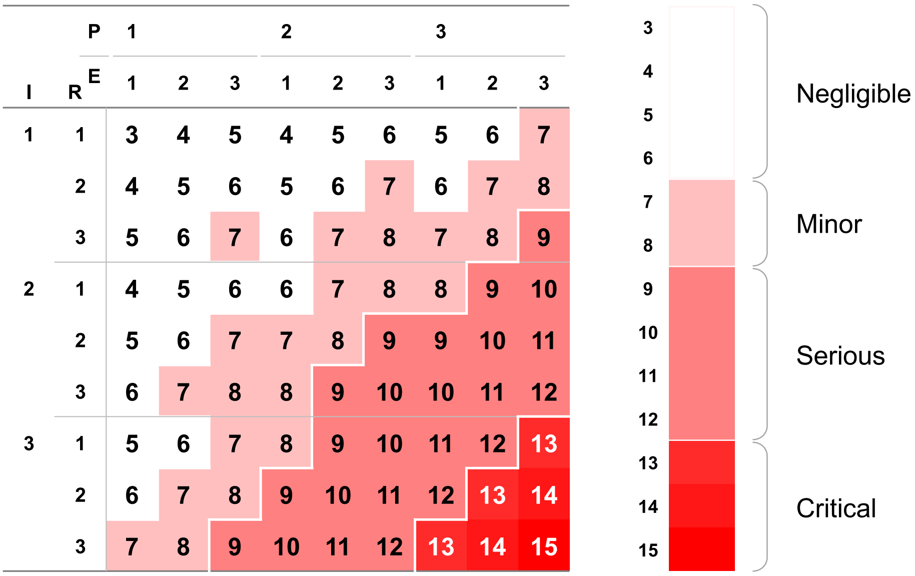
3.4 Risk assessment formula

The following Eq. (5) defines the environmental risk of CAVs when considering the probability, impact, exposure, and recovery described in the previous section.

$$Risk = Probabilty \times Impact + Exposure + Recovery, \tag{5}$$

where $Probabilty \times Impact$ is the impact on damage multiplied by its probability, plus the exposure and recovery create the risk value.

Figure 2 shows a matrix for evaluating the risk using the PIER method. The evaluated risk ranges from three to 15, where a higher value indicates a higher risk. In this study, a PIER risk ranging from three to six is classified as Negligible, seven to eight as Minor, nine to 12 as Serious, and 13 to 15 as Critical.



	P	1			2			3		
I	R E	1	2	3	1	2	3	1	2	3
1	1	3	4	5	4	5	6	5	6	7
	2	4	5	6	5	6	7	6	7	8
	3	5	6	7	6	7	8	7	8	9
2	1	4	5	6	6	7	8	8	9	10
	2	5	6	7	7	8	9	9	10	11
	3	6	7	8	8	9	10	10	11	12
3	1	5	6	7	8	9	10	11	12	13
	2	6	7	8	9	10	11	12	13	14
	3	7	8	9	10	11	12	13	14	15

3
4
5
6
Negligible
7
8
Minor
9
10
11
12
Serious
13
14
15
Critical

Fig. 2 Risk evaluation matrix

4 PIER implementation and evaluation for connected and autonomous vehicles (CAVs)

This section defines the two primary functions of CAVs: automotive OTA and collision avoidance. In addition, the overall risk for CAVs is evaluated from a cybersecurity perspective by analyzing exposure of threats to external entities, attack probability, the impact of the attack, and recovery from the damage.

4.1 Main functions

4.1.1 Automotive over-the-air (OTA) in connected vehicles (CVs)

Automotive software is an essential vehicle component directly related to users' safety on the road. Therefore, vehicle control software requires high reliability and security. That is why the manufacturer, dealer, or authorized maintenance channel manages the automotive software update instead of the user. Updating conventional automotive software requires authorized diagnostic equipment and diagnostic communications over a wired network physically connected to the vehicle. Even when an urgent software update is needed, the owner cannot update the software directly and must visit a repair shop instead. Consequently, it causes the update life cycle of automotive software to be significant long. As a result of these limitations, these cause software vulnerabilities are left unattended, and vulnerabilities in software can be exploited as attack targets or attack surfaces.

Automotive OTA in Fig. 3 is a new alternative to overcome the limitations of a conventional vehicle control software update with a long update cycle and conveniently update the software within a shorter cycle. This method remotely updates the software of a vehicle controller using a cellular or IoT network to which the CAVs are connected. These updates include not only software with a relatively low safety rating, such as automotive infotainment systems, but also software components with a high safety rating, such as drivetrain controller firmware. The automotive OTA ecosystem consists of backend servers, remote repositories, wireless networks, IVNs, electronic control units (ECUs), and software packages.

Automotive OTA reduces the update cycle of vehicle control software using CAVs connectivity. However, this can provide attack surfaces that damage the integrity of the automotive control software [46, 47] because it allows a modification of the vehicle software, which was a barrier to the internal components in the past. Serious security risks can occur if an attacker can affect the lifecycle of on-demand software such as repository, distribution, and installation. Maliciously manipulated software becomes a route for an attacker to remotely control the engine, braking, steering, and infotainment system of moving vehicles. It can be a critical risk that directly affects the safety and lives of users on the road.

4.1.2 Collision avoidance in autonomous vehicles (AVs)

Positioning, perception, judgment, and control are the core technologies required for AVs. Such vehicles use various sensors to recognize the location, road, and surrounding objects of the vehicle while determining the speed, steering, and braking commands for stable driving. Autonomous driving software sends the commands to the drive and steering systems to control the vehicular movement. The

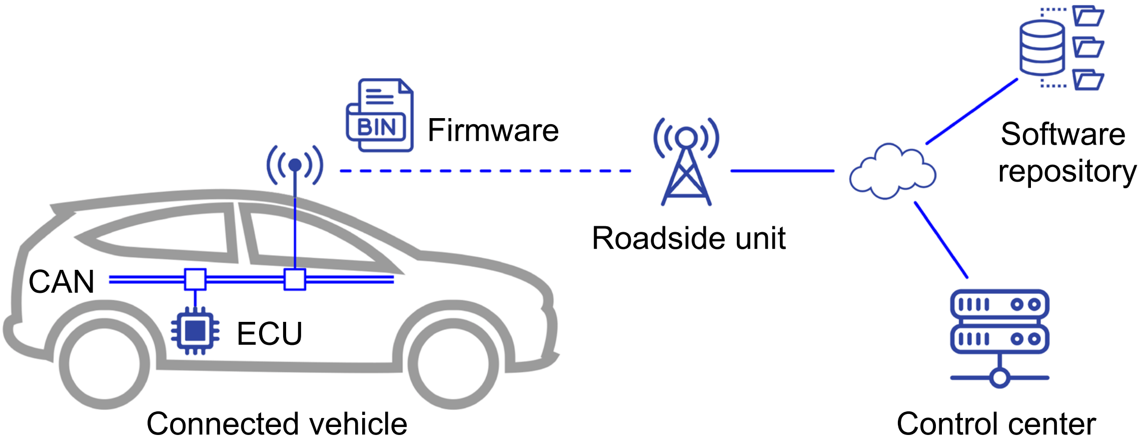


Fig. 3 Automotive OTA architecture in connected vehicles (CVs)

collision avoidance technology of AVs in Fig. 4 is crucial for accident prevention. It requires accurate recognition of various external factors and the internal conditions of the vehicle that can occur in driving contexts on the road.

The driving context of AVs is based on the state of the driving vehicle, the predicted path, and the movement of the surrounding objects. In particular, this context includes not only control information such as vehicle speed, acceleration, driving direction, and the predicted path, but also specific factors that can directly affect the vehicle control pattern, such as high-speed driving, downtown driving, intersection entry or exit, parking and stopping attempts, and emergency braking. In addition, it analyzes the driving interference and collision possibility against moving objects on the driving routes inside and outside by detecting and predicting the movements of the objects.

Severe risks to vehicle safety occur if attackers can intervene while AVs combine and process multiple sensing data or if attackers can interfere while AVs are operating collision avoidance in response to a dangerous situation [48, 49]. For example, the AVs may fail to recognize a collision risk over the front by intense light into the front camera [38] or by reverse-injecting the light detection and ranging wavelength [39] to interrupt the moving object recognition on the road.

4.2 PIER analysis for CAVs

A CAV is a mission-critical system. If the security system of this ecosystem is bypassed and the integrity or availability of the control software is compromised, the guarantee of the safe operation of the drive system cannot be guaranteed due to malicious manipulation. This brings

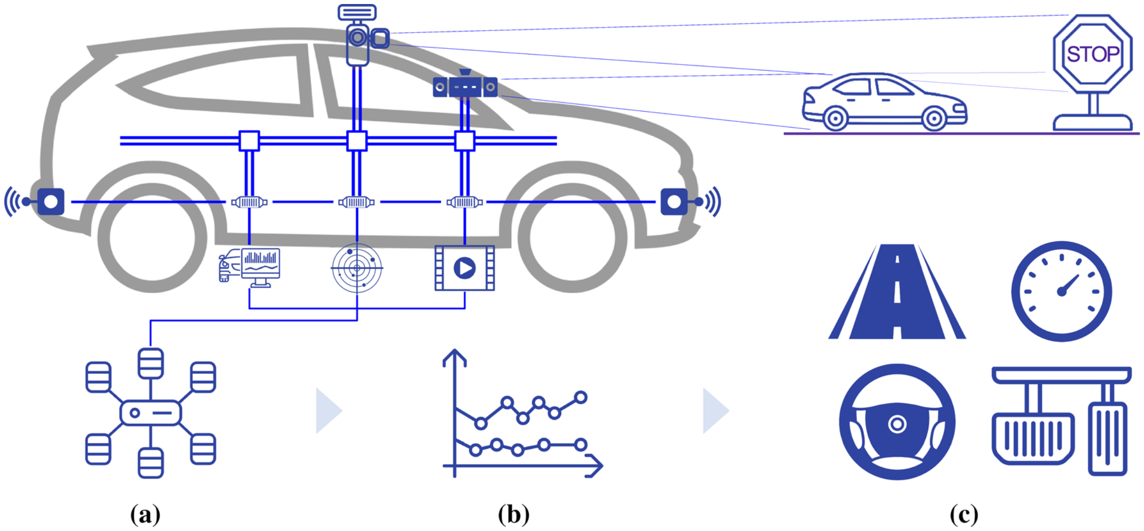


Fig. 4 Collision avoidance in autonomous vehicles (AVs): **a** multiple sensing data fusion, **b** data analysis, and **c** driving control, i.e, steeing, braking, and acceleration of the vehicle

about a high impacted risk because it can cause a critical incident involving the casualties of road users. In particular, the automotive OTA provided by CVs is relatively easy to access externally. Therefore, access should be controlled from the cyber defense perspective, and risk factors should be evaluated with a focus on prevention through monitoring. In contrast, the collision avoidance feature provided by AVs is a factor that places critical importance on a fast recovery, as real-time availability and resulting safety are essential.

4.2.1 PIER analysis of automotive OTA in CVs

Conventional cyber-attacks on vehicles were from hackers forcing an update of manipulated software to the internal controller of the vehicle. However, a vehicle not connected to the Internet has to be physically occupied to tamper with its software. In contrast, a CV connected to a wireless network can update software remotely without physically occupying the vehicle. The repository used for software storage, a wireless network used for distribution, and the process of extracting and patching software changes in an automotive OTA are IT-based components. Therefore, the scope of exploitable vulnerabilities is broad, and the exposure is high in terms of accessibility even without expert knowledge concerning in-vehicle design and control technology. A higher level of security is required in the automotive OTA because attackers can create a path allowing the direct manipulation or remote control of the vehicle simply by taking control of the remote repository server using the security technology of the universal IT environment. Therefore, the monitoring and response to anomalous behaviors are necessary along with a cyber-defense system and the back-end cloud infrastructure to which a vehicle is connected. Table 2 shows the risk assessment for automotive OTA in CVs.

4.2.2 PIER analysis of collision avoidance in AVs

The drivetrain software in AVs applying collision avoidance by analyzing the driving context based on multi-sensing data directly affects the cybersecurity risk. If an analysis error is caused by the interference of sensing signals, manipulated data, or malfunctioning sensors by the attacker, it can cause an accident that may involve human injuries while driving AVs. Direct manipulation of a vehicle's sensing signal or control software requires expert knowledge of the automotive domain and thus can be a barrier to attackers in terms of probability and exposure. However, security threats that adversely affect the driving system during vehicle operation can cause severe damage even in a fleeting moment. Therefore, real-time resilience and prevention systems are considered crucial factors. Table 3 shows the risk assessment for collision avoidance in AVs.

5 Discussion

5.1 Countmeasures to mitigate risk

5.1.1 Security requirements as countermeasure in automotive OTA

The security requirements specified in Table 4 are presented as countermeasures to mitigate the risk in automotive OTA.

First, signatures for known vulnerabilities in an OEM C &C or cloud repository are monitored to prevent the execution of known vulnerabilities on a server and block suspicious behavior when identified [17, 40, 41], thereby lowering the risk of exposure ($E_2 = 3 \rightarrow 2$). In addition, the most significant opportunity for attackers from the exposure perspective is that an attack surface is accessible in the public domain because the server or particular transmission sections are exposed to attackers. To complement this, man-in-the-middle attacks in the transmission section are made more difficult by encrypting the transmission or converting sections into dedicated lines ($E_3 = 2 \rightarrow 1$). Furthermore, it also blocks manipulated software of an attacker containing malicious code by verifying the code signature based on the public key infrastructure [42, 43] whenever installing the software package sent from the endpoint of the vehicle controller ($E_1^* = 2 \rightarrow 1$).

When reliable backend, transmission section, and endpoint are configured by applying these security requirements to automotive OTA, the high risk of exposure is mitigated to low. As a result, the overall risk assessment of automotive OTA lowers from the risk of 13 as Critical to eight as Minor.

5.1.2 Security requirements as countermeasure in collision avoidance

The security requirements specified in Table 5 are presented as countermeasures to mitigate collision risks in AVs.

First, a secure flashing [44] prevents an attacker from arbitrarily manipulating the vehicle's control software. A secure boot [45] is utilized to perform a kill chain defense when such software is installed and prevent misuse of the manipulated software ($R_2 = 3 \rightarrow 1$). In addition, in-vehicle IDPSs prevent the manipulated controller area network (CAN) messages or abnormal behaviors of the control

Table 2 Risk assessment for automotive OTA in CVs

Categories	Risk factors	Level	Description
Probability	P_1: required skill	2	Possible to attack IT infrastructures without vehicle expertise
	P_2: preparation time	1	Taking a lot of time to prepare for an attack due to limited entry points
	P_3^*: defense system	3	Real-time monitoring required with the convergence of vehicle and IT security
	Probability factor	High	$\lceil 18.5/9 \rceil = 3$
Impact	I_1: damage result	3	Direct risk to the occupants' safety from manipulated drivetrain software
	I_2: damage target	3	Taking control of the drivetrain using connected in-vehicle controllers from the remote site
	I_3^*: recovery time	2	Requiring recovery within an hour for 99.99% availability to automotive IT system
	Impact factor	High	$\lceil 24/9 \rceil = 3$
Exposure	E_1^*: reachability	2	Attack entry point as the approved Internet section
	E_2: exploitable vulnerabilities	3	Attack OTA repositories backend and cloud systems using disclosed general vulnerabilities
	E_3: accessibility	2	Convergence of Internet section included in the dedicated and closed network
	Exposure factor	High	$\lceil 19/9 \rceil = 3$
Recovery	R_1^*: ease to detection	1	Pre-detection and prevention the attacks with vehicle and IT security convergence
	R_2: patch means	2	Possible to real-time recovery with batch patching from automotive OTA in a cyber breaches
	R_3: supply chain	1	Utilization of already-established infrastructure and independent operating partnerships
	Recovery factor	Low	$\lceil 6.5/9 \rceil = 1$
Automotive OTA risk assessment		Critical	$3 \times 3 + 3 + 1 = 13$

software in the IVNs. Anti-spoofing and anti-jamming are applied simultaneously to prevent interference, manipulation, and interruption of the sensing data in advance ($R_1^* = 3 \rightarrow 1$). Maintaining up-to-date attack signatures is crucial to detect abnormal behavior or attack routines inside a vehicle accurately. Batch patching is performed using automotive OTA to update detection patterns, and a supply chain system is secured and managed in advance to keep this patch up to date ($R_3 = 3 \rightarrow 2$).

When reliable IVNs and sensing data convergence scheme is configured by applying these security requirements to collision avoidance of AVs, a high-security risk of recovery is mitigated to low. As a result, the overall risk assessment of collision avoidance lowers from the risk of seven as Minor to five as Negligible.

5.2 Performance comparison

In this section, the coverage of the risk criteria used in a risk assessment and the procedure simplicity from the process perspective is compared with existing methodologies to verify the effectiveness of the PIER method proposed in this study.

5.2.1 Risk criteria coverage

Most methodologies employ the attack probability and impact of an attack as criteria for assessing the cybersecurity risk of vehicles. As shown in Table 6, the attack feasibility attribute in ISO/SAE 21434 [6] rates the attack probability, including the elapsed time, specialized expertise, and equipment required for the attack from the capability perspective of attackers. The PIER method quantitatively assesses the attack probability factors by categorizing them into the required skill, preparation time, and defense system level and subdividing it into risk factors under each criterion.

In addition, the VeRA methodology [28] in Table 6 presents human control as an evaluating factor in terms of recovery. The controllability property, which can handle dangerous situations in assessing risk, is a meaningful indicator from the perspective of recovery. Human control is selected according to a pre-configured matrix with a combination of the automation level of AVs and human capability. The six levels of autonomy in SAE J3016 [29] are widely referenced indices for classifying AVs. However, human capability or experience level is difficult to establish as an objective index in interacting with a vehicle. Consequently, this measure may lead to a problem with an item that may lead to underestimated or exaggerated errors in a risk assessment because there are no quantitative

Table 3 Risk assessment for collision avoidance in AVs

Categories	Risk factors	Level	Description
Probability	P_1: required skill	1	Necessary to have expertise in vehicular domain to take control of the software authority, e.g., CAN message metadata, in-vehicle network, and entry points
	P_2: preparation time	1	Long-term information gathering and preparation in advance
	P_3^*: defense system	2	Necessary internal mechanisms to protect vehicular networks and control systems without external support
	Probability factor	Low	$\lceil 8/9 \rceil = 1$
Impact	I_1: damage result	3	Direct risk to the occupants' safety from manipulated drivetrain software
	I_2: damage target	3	Causing malfunction of the drivetrain systems by manipulating the sensing data and analysis based on the autonomous driving mechanism
	I_3^*: recovery time	3	Real-time defense and recovery in milliseconds required to ensure control and safety of a moving vehicle
	Impact factor	High	$\max_{3}(\lceil 31.5/9 \rceil) = 3$
Exposure	E_1^*: reachability	1	Hard to spread attacks due to restricting entry points and the necessity of occupating physical targets
	E_2: exploitable vulnerabilities	1	The necessity of undisclosed vulnerabilities directly related to the target vehicle
	E_3: accessibility	2	Physical access or obstruction in close proximity to manipulate the sensing data
	Exposure factor	Low	$\lceil 6.5/9 \rceil = 1$
Recovery	R_1^*: ease to detection	3	Difficult to detect anomaly behaviors before an incident without connectivity
	R_2: patch means	3	Taking a lot of time due to manually patching from physical maintenance infrastructures without connections
	R_3: supply chain	3	Depending on partnership capabilities and coverage as technology variance and utilization of maintenance infrastructure are deeply related
	Recovery factor	High	$\max_{3}(\lceil 31.5/9 \rceil) = 3$
Collision avoidance risk assessment		Minor	$1 \times 3 + 1 + 3 = 7$

Table 4 Security requirements to mitigate security risk level in automotive OTA

Category	Risk factors	Level	Security requirements
Probability	P_1: required skill	$2 \rightarrow 1$	Required for more advanced preparation and technology to bypass security systems that block malicious actions
	P_2: preparation time	1	Same as Table 2
	P_3^*: defense system	3	Same as Table 2
	Probability factor	Medium	$\lceil 15.5/9 \rceil = 2$
Exposure	E_1^*: reachability	$2 \rightarrow 1$	Verifying the signatures of the vehicle software to block manipulated packages containing malicious codes
	E_2: exploitable vulnerabilities	$3 \rightarrow 2$	Intrusion detection and prevention to block malicious activities caused by known vulnerabilities in the vehicular network
	E_3: accessibility	$2 \rightarrow 1$	Encryption in transit or private network to protect publicly exposed requests and delivery of software packages over-the-air
	Exposure factor	Low	$\lceil 6.5/9 \rceil = 1$
Automotive OTA risk assessment		Minor	$2 \times 3 + 1 + 1 = 8$

criteria for human driving ability or response skills under a critical situation.

The PIER method uses an index that evaluates rapid resilience in a critical situation from a recovery perspective. Resilience is evaluated by the criteria of the quick

Table 5 Security requirements to mitigate security risk level in collision avoidance

Category	Risk factors	Level	Security requirements
Recovery	R_1^*: ease to detection	$3 \rightarrow 1$	Intrusion detection and prevention to block malicious activities caused by message injection to the vehicular network
	R_2: patch means	$3 \rightarrow 1$	Apply secure flash and secure boot with software signature verification to prevent deployment of manipulated software
	R_3: supply chain	$3 \rightarrow 2$	Applying automotive OTA to lower supply chain dependency and shortening the patching software delivery life cycles
	Recovery factor	Low	$\lceil 6.5/9 \rceil = 1$
Collision avoidance risk assessment		Negligible	$1 \times 3 + 1 + 1 = 5$

Table 6 Coverage of risk categories

Risk categories	ISO/SAE 21434 [6]	Cui and Zhang [28]	Kelarestaghi et al. [30]	Strandberg et al. [32]	Ours (PIER)
Probability	O[a]	O	O	O	O
Impact	O	O	O	O	O
Exposure					O
Recovery		O[b]			O

[a] Feasibility

[b] Human control

recognition of a high-risk situation, the patch method applied, the time required, and the coverage of the supply chain as the response capabilities. The crucial elements of the CAVs resilience are the capability to recover the cybersecurity risk immediately by detecting and taking action in advance of dangerous situations, neutralizing the attack through kill chain defense, spreading patches in real-time, and responding with a thorough supply chain.

5.2.2 Conciseness of application steps

It is important to sufficiently assess the risk criteria for each factor to evaluate the risk to CAVs. ISO/SAE 21434 [6] fully describes the steps necessary for a risk assessment. Sufficient review and assessment of risk factors are meaningful when designing and certifying the end-to-end architecture in the development stage of CAVs. However, obstacles may arise in assessing and removing risk factors if the process is too complicated or takes a prolonged time to apply. If cyber-attacks are in progress or while driving CAVs, it is necessary to quickly assess the risk using only core risk factors and establish an appropriate response strategy accordingly.

Table 7 shows the total number of processes required for a risk assessment and tasks to be applied in advance. Annex H of ISO/SAE 21434 provides examples of the TARA method. The TARA method requires seven steps of risk evaluation, including an impact rating and an attack feasibility rating, to determine the risk value of CAVs. The damage scenario of the asset identification stage should precede the impact rating, whereas attack path analysis based on threat scenarios is required to determine the attack feasibility rating. The dependency required at each stage of a risk assessment cause in delay decision-making under situations in which an immediate risk decision and response are required.

The PIER method does not require preparation, and the risk criteria are defined compactly for a fast risk rating. The risk categories, risk factors, weights, and criteria required for a PIER risk assessment are expressed in a single line, as shown in Table 1. The PIER method, a two-step process without prior procedures, can quickly deduce the risk and countermeasures compared to the existing methods described in Table 7.

6 Conclusion and future work

This study proposes the PIER method to evaluate the cybersecurity risk of CAVs. This method uses probability, impact, exposure, and recovery as four risk categories of a risk assessment. It realizes cyber-resilience by adding

Table 7 Process steps

	ISO/SAE 21434 [6]	Cui and Zhang [28]	Kelarestaghi et al. [30]	Strandberg et al. [32]	Ours (PIER)
Number of processes	8	4	5	4	2
Preparation	7, Ref.[a]	2, Ref.[b]	3, Ref.[c]	Start phase[d]	None
Regression cycle	Ref.[e]	None	None	Test phase	Reassessment
Risk matrix, R	$1 + I \times F$	$H + S \times P$	Predefined matrix	$P \times C$	$P \times I + E + R$

[a] Item definition and six tasks of TARA method, i.e., asset identification, impact rating, threat scenario identification, attack path analysis, and attack feasibility rating

[b] Analysis of attack tree and attack defense tree

[c] Adversarial model, threat event, and vulnerability analysis

[d] Threat modeling

[e] Risk treatment decision

exposure and recovery risk factors to the probability and impact indices for the TARA of CAVs. Exposure risk factors provide criteria to evaluate the attack surface for connectivity attributes in CAVs. Recovery risk factors provide criteria to assess the rapid resilience in terms of availability and real-time properties in mission-critical systems, CAVs.

This study applies automotive OTA as a representative function of CVs and collision avoidance as a representative function of AVs to the PIER method to verify the effectiveness of the proposed methodology. It evaluates the risk level in each aspect of CVs and AVs based on the risk categories, risk factors, criteria, and evaluation matrix of the PIER method. Security requirements derived from the factors causing the high risk are important countermeasures to mitigate the risk. Derived security requirements from the case study of automotive OTA in CVs lower the risk from Critical to Minor. Countermeasures from the method in collision avoidance of AVs reduce the risk from Minor to Negligible. Reducing the risk level effectively in the re-evaluation after applying the countermeasures proves the effectiveness of this PIER methodology.

The PIER method has broader coverage in terms of exposure and resilience compared to other studies for risk assessment of CAVs security. In particular, the predefined detailed criteria for each risk factor provide quick assessment and derive countermeasures because it simplifies the risk assessment process without the preparation stage.

The following research aims to refine and propose the key steps for risk assessment considering the cyber-resilience of CAVs to simplify and clarify the TARA method in automotive cybersecurity-related laws, regulations, and standards.

Acknowledgements This research was financially supported by Hansung University for Seunghyun Park. Also, this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT)(No. 2022R1A2C2005705) for Hyunhee Park.

References

1. Bezai, N. E., Medjdoub, B., Al-Habaibeh, A., Chalal, M. L., & Fadli, F. (2021). Future cities and autonomous vehicles: analysis of the barriers to full adoption. *Energy and Built Environment, 2*(1), 65–81. https://doi.org/10.1016/j.enbenv.2020.05.002.
2. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX security symposium* (pp. 77–92).
3. Miller, C., & Valasek, C. (2014). A Survey of Remote Automotive Attack Surfaces. *In Black Hat USA, 2014,* 1–94.
4. Maple, C., Bradbury, M., Le, A. T., & Ghirardello, K. (2019). A connected and autonomous vehicle reference architecture for attack surface analysis. *Applied Sciences, 9*(23), 1–33. https://doi.org/10.3390/app9235101.
5. The United Nations Economic Commission for Europe. (2021). Cyber security and cyber security management system. *UN Regulation No. 155*. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security. Accessed 30 Apr 2022.
6. International Organization for Standardization. (2021). ISO/SAE 21434:2021, Road vehicles—Cybersecurity engineering (pp.

1–81). https://www.iso.org/standard/70918.html. Accessed 30 Apr 2022.

7. SAE International. (2021). J3061, Cybersecurity guidebook for cyber-physical vehicle systems (DEC2021) (pp. 1–128). https://www.sae.org/standards/content/j3061_202112. Accessed 30 Apr 2022.
8. Kim, K., Kim, J. S., Jeong, S., Park, J. H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers and Security, 103*(102150), 1–27. https://doi.org/10.1016/j.cose.2020.102150.
9. Sun, X., Yu, F. R., & Zhang, P. (2021). A Survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems,* 1–20. https://doi.org/10.1109/TITS.2021.3085297
10. Gao, C., Wang, G., Shi, W., Wang, Z., & Chen, Y. (2021). Autonomous driving security: State of the art and challenges. *IEEE Internet of Things Journal,* 1–20. https://doi.org/10.1109/JIOT.2021.3130054
11. Martin, H., Ma, Z., Schmittner, C., Winkler, B., Krammer, M., Schneider, D., et al. (2020). Combined automotive safety and security pattern engineering approach. *Reliability Engineering & System Safety, 198,* 2020. https://doi.org/10.1016/j.ress.2019.106773.
12. Luo, F., Jiang, Y., Zhang, Z., Ren, Y., & Hou, S. (2021). Threat analysis and risk assessment for connected vehicles: A survey. *Security and Communication Networks, 2021*(1263820), 1–19. https://doi.org/10.1155/2021/1263820.
13. Hoppe, T., Kiltz, S., & Dittmann, J. (2009). Applying intrusion detection to automotive it-early insights and remaining challenges. *Journal of Information Assurance and Security, 4*(3), 226–235.
14. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., & Savage, S. (2010). Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy* (pp. 447–462). https://doi.org/10.1109/SP.2010.34
15. Miller, C., & Valasek, C. (2013). Adventures in Automotive Networks and Control Units. In *DEF CON 21* (pp. 1–101).
16. Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things Journal, 1*(1), 10–21. https://doi.org/10.1109/JIOT.2014.2302386.
17. Cho, K.-T., & Shin, K. G. (2016). Fingerprinting electronic control units for vehicle intrusion detection. In *Proceedings of the 25th usenix security symposium* (pp. 911–927).
18. Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network, 31*(5), 50–58. https://doi.org/10.1109/MNET.2017.1600257.
19. Li, X., Yu, Y., Sun, G., & Chen, K. (2018). Connected vehicles' security from the perspective of the in-vehicle network. *IEEE Network, 32*(3), 58–63. https://doi.org/10.1109/MNET.2018.1700319.
20. Marchetti, M., & Stabili, D. (2019). READ: Reverse engineering of automotive data frames. *IEEE Transaction on Information Forensics and Security, 14*(4), 1083–1097. https://doi.org/10.1109/TIFS.2018.2870826.
21. Park, S., & Choi, J.-Y. (2020). Malware detection in self-driving vehicles using machine learning algorithms. *Journal of Advanced Transportation, 2020*(3035741), 1–9. https://doi.org/10.1155/2020/3035741.
22. Chattopadhyay, A., Lam, K.-Y., & Tavva, Y. (2021). Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems, 22*(11), 7015–7029. https://doi.org/10.1109/TITS.2020.3000797.
23. Mahmoud Hashem Eiza, M. H., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine, 12*(2), 45–51. https://doi.org/10.1109/MVT.2017.2669348.
24. Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. In *Black Hat USA 2015* (pp. 1–91).
25. Nie, S., Liu, L., & Du, Y. (2017). Free-fall: Hacking Tesla from wireless to CAN bus. In *Black Hat USA 2017* (pp. 1–16).
26. Cai, Z., Wang, A., & Zhang, W. (2019). 0-days & mitigations: Roadways to exploit and secure connected BMW cars. In *Black Hat USA 2019* (pp. 1–37).
27. Ligo, A. K., Kott, A., & Linkov, I. (2021). How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. *IEEE Engineering Management Review, 49*(2), 89–97. https://doi.org/10.1109/EMR.2021.3074288.
28. Cui, J., & Zhang, B. (2020). VeRA: A simplified security Risk Analysis Method for Autonomous Vehicles. *IEEE Transactions on Vehicular Technology, 69*(10), 10494–10505. https://doi.org/10.1109/TVT.2020.3009165.
29. SAE International. (2021). J3016, Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles (APR2021) (pp. 1–41). https://www.sae.org/standards/content/j3016_202104, Accessed 30 Apr 2022.
30. Kelarestaghi, K. B., Foruhandeh, M., Heaslip, K., & Gerdes, R. (2019). Intelligent transportation system security: Impact-oriented risk assessment of in-vehicle networks. *IEEE Intelligent Transportation Systems Magazine, 13*(2), 91–104. https://doi.org/10.1109/MITS.2018.2889714.
31. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments, SP 800-30 Rev.1 (pp. 1–95). https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. Accessed 30 Apr 2022.
32. Strandberg, K., Olovsson, T., & Jonsson, E. (2018). Securing the connected car: A security-enhancement methodology. *IEEE Vehicular Technology Magazine, 13*(1), 56–65. https://doi.org/10.1109/MVT.2017.2758179.
33. Kong, H. K., Hong, M. K., & Kim, T. S. (2018). Security risk assessment framework for smart car using the attack tree analysis. *Journal of Ambient Intelligence and Humanized Computing, 9,* 531–551. https://doi.org/10.1007/s12652-016-0442-8.
34. Lee, Y., Woo, S., Song, Y., Lee, J., & Lee, D. H. (2020). Practical vulnerability-information-sharing architecture for automotive security-risk analysis. *IEEE Access, 8,* 120009–120018. https://doi.org/10.1109/ACCESS.2020.3004661.
35. Nilsson, D. K., & Larson, U. E. (2008). Secure firmware updates over the air in intelligent vehicles. In *Proceedings of 2008 IEEE international conference on communications workshops* (pp. 380–384). https://doi.org/10.1109/ICCW.2008.78
36. Kamble, S. S., Gunasekaran, A., Subramanian, N., Ghadge, A., Belhadi, A., & Venkatesh, M. (2021). Blockchain technology's impact on supply chain integration and sustainable supply chain performance: evidence from the automotive industry. *Annals of Operations Research,* 1–10. https://doi.org/10.1007/s10479-021-04129-6
37. Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2021). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of*

Things Journal, 8(8), 6222–6246. https://doi.org/10.1109/JIOT.2020.3025775.

38. Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. (2015). Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe, 11*(2015), 995–1017.
39. Shin, H., Kim, D., Kwon, Y., & Kim, Y. (2017). Illusion and Dazzle: adversarial optical channel exploits against lidars for automotive applications. In Fischer, W., & Homma, N. (Eds.), *Proceedings of international conference on cryptographic hardware and embedded systems. Lecture Notes in Computer Science* (Vol. 10529, pp. 445–467). https://doi.org/10.1007/978-3-319-66787-4_22
40. Park, S., & Choi, J.-Y. (2020). Hierarchical anomaly detection model for in-vehicle networks using machine learning algorithms. *Sensors, 20*(14), 1–21. https://doi.org/10.3390/s20143934.
41. Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2020). A survey of intrusion detection for in-vehicle networks. *IEEE Transactions on Intelligent Transportation Systems, 21*(3), 919–933. https://doi.org/10.1109/TITS.2019.2908074.
42. Heng, X., Qin, S., Xiao, Y., Wang, J., Tao, Y., & Zhang, R. (2022). A strong secure V2I authentication scheme from PKI and accumulator. In *Proceedings of 2022 2nd international conference on consumer electronics and computer engineering (ICCECE)* (pp. 98–103). https://doi.org/10.1109/iccece54139.2022.9712701
43. European Telecommunications Standards Institute. (2021). Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2. *ETSI TS 102 940 V2.1.1* (pp. 1–48).
44. Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., & Baccelli, E. (2019). Secure firmware updates for constrained IoT devices using open standards: A reality check. *IEEE Access, 7,* 71907–71920. https://doi.org/10.1109/ACCESS.2019.2919760.
45. Pott, C., Jungklass, P., Csejka, D. J., Eisenbarth, T., & Siebert, M. (2021). Firmware security module. *Journal of Hardware and Systems Security, 5*(2), 103–113. https://doi.org/10.1007/s41635-021-00114-4.
46. Halder, S., Ghosal, A., & Conti, M. (2020). Secure over-the-air software updates in connected vehicles: A survey. *Computer Networks, 178*(1), 1–10. https://doi.org/10.1016/j.comnet.2020.107343.
47. Mahmood, S., Nguyen, H. N., & Shaikh, S. A. (2022). Systematic threat assessment and security testing of automotive over-the-air (OTA) updates. *Vehicular Communications, 35,* 100468. https://doi.org/10.1016/j.vehcom.2022.100468.
48. Haider, S., Abbas, Z. H., Abbas, G., Waqas, M., Tu, S., & Zhao, W. (2020). A novel cross-layer V2V architecture for direction-aware cooperative collision avoidance. *Electronics, 9*(7), 1–22. https://doi.org/10.3390/electronics9071112.
49. Vagale, A., Oucheikh, R., Bye, R. T., Osen, O. L., & Fossen, T. I. (2021). Path planning and collision avoidance for autonomous surface vehicles I: A review. *Journal of Marine Science and Technology, 26*(4), 1292–1306. https://doi.org/10.1007/s00773-020-00787-6.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Prof. Seunghyun Park received his Ph.D. in Cybersecurity from Korea University in 2021. He joined the Faculty of Hansung University in September 2021 and is currently an Assistant Professor in the Division of Computer Engineering. From 2014 to 2021, he worked for Hyundai Motor Company and Kia in connected vehicles and enterprise cybersecurity for security risk assessment, remediation, and incident response. Before that, he was a Senior Researcher at the Advanced Institute of Technology of Korea Telecom Corporation, where he researched media technology and data analytical methods from 2011 to 2014. He also developed mobile software in LG Electronics Inc. from 2008 to 2011. His current research interests focus on automotive cybersecurity and risk assessment, web framework, and data analytics models.

Prof. Jayh (Hyunhee) Park received the Ph.D. degrees in electronics and computer engineering from Korea University, Seoul, South Korea, in 2011. She joined the Faculty of Myongji University, in 2020, where she is currently an associate professor with the department of Information and Communication Engineering. She is currently a supervisor of DAN Lab (Data Analysis and Networking). From March 2017 to February 2020, she has been working the department of computer software as an assistant professor from Korean bible university, Seoul, South Korea. From November 2014, she has been working in LG Electronics as a Senior Researcher for Wi-Fi standardization (IEEE 802.11ax, Wake Up Radio, Wi-Fi Alliance, etc.). From January 2013 to October 2014, she joined INRIA Research Center as a Postdoctoral Researcher where she works in DIONYSOS Research Group and in Telecom Bretagne as a Postdoctoral researcher where she undertakes the system implementation for QoE on wireless networks. From September 2011 to February 2013, she joined Korea University as a Research Professor. She served as the Program Co-Chair for the IMIS 2020, the Organizing Committee for the ICTC2020, ICTC2021, and BWCCA 2021 and the Workshop organizer for FINGNet 2019 and 2020. She is a Guest Editor of the Electronics and Journal of Advanced Transportation. Her research interests include wireless networks, mobile edge/cloud computing, and big data analysis.