Traffic & Transportation

Cybersecurity Threat Analysis and Risk Assessment for Intelligent Connected Vehicles

Huasheng XIE[1], Lie WANG[2]

Original Scientific Paper
Submitted: 19 Jan 2025
Accepted: 4 Apr 2025
Published: 24 Feb 2026

[1] 1571695044@qq.com, School of Computer, Electronics and Information, Guangxi University, Nanning, China
[2] 13977106533@139.com, School of Computer, Electronics and Information, Guangxi University, Nanning, China

Publisher:
Faculty of Transport and Traffic Sciences, University of Zagreb

ABSTRACT
With the rapid development of intelligent connected vehicles, cybersecurity issues have become increasingly prominent, posing significant challenges to vehicle safety and user privacy. This paper conducts a study on threat analysis and risk assessment (TARA) for intelligent connected vehicles based on the ISO/SAE 21434 standard. The research analyses and examines the practical methodologies of the standard from systematic and practical perspectives, constructing a comprehensive risk assessment framework that covers risk identification, analysis, assessment and response strategies. The rationality and effectiveness of the framework are validated through case studies. This study not only provides systematic security guidance for automotive manufacturers and technology developers but also offers empirical evidence for regulatory compliance reviews, thereby promoting the secure development of intelligent connected vehicles.

KEYWORDS
cybersecurity; intelligent connected vehicles; ISO/SAE 21434; TARA; risk assessment.

1. INTRODUCTION

With the rapid development of the automotive industry, intelligent connected vehicles (ICVs), which represent the cutting-edge innovation in automotive technology, have gradually transformed our travel experiences. Thanks to the integrated application of advanced sensors and powerful computing platforms, ICVs can fulfil a variety of functions that are revolutionary to traditional vehicles, such as autonomous driving, real-time traffic information sharing and remote vehicle control, thus bringing users an unprecedented driving and riding experience [1].

Nevertheless, as vehicles become networked, they are exposed to the risks of cyberattacks, including illegal remote control, user data leakage and even traffic accidents [2]. These risks primarily originate from the external threat entry points introduced by vehicle networking, like physical interfaces, near-field wireless communications and remote vehicle-cloud communications. Consequently, assessing and dealing with the cybersecurity risks of intelligent connected vehicles has become an urgent issue that demands immediate attention.

This paper mainly concentrates on the threat analysis and risk assessment during the vehicle design stage. The ISO/SAE 21434 is an international standard that aims to offer a comprehensive framework for vehicle cybersecurity and cover the relevant processes within the product cybersecurity life cycle [3]. Moreover, this standard also provides a significant reference basis for threat analysis and risk assessment [4].

2. INTRODUCTION TO ISO/SAE 21434

Cybersecurity risk assessment, as a proactive defence technology, primarily centres around elements such as system vulnerabilities, external threats and the value of system assets [5]. The ISO/SAE 21434 standard represents a crucial international benchmark for road vehicle cybersecurity. Its key components encompass the establishment of a security management system, the conduct of risk assessments, the formulation of threat models and the implementation of emergency response strategies (depicted in *Figure 1*). This standard is designed to offer a comprehensive security framework for intelligent connected vehicles, enabling manufacturers and suppliers to identify, assess and manage potential cybersecurity risks effectively [3]. The central tenet of this standard lies in the integration of cybersecurity measures throughout all stages of vehicle development and operation, rather than confining security assessment to the post-completion phase of the product. In essence, during the initial design phase, potential security threats must be contemplated to guarantee the establishment of a robust security shield from the outset.

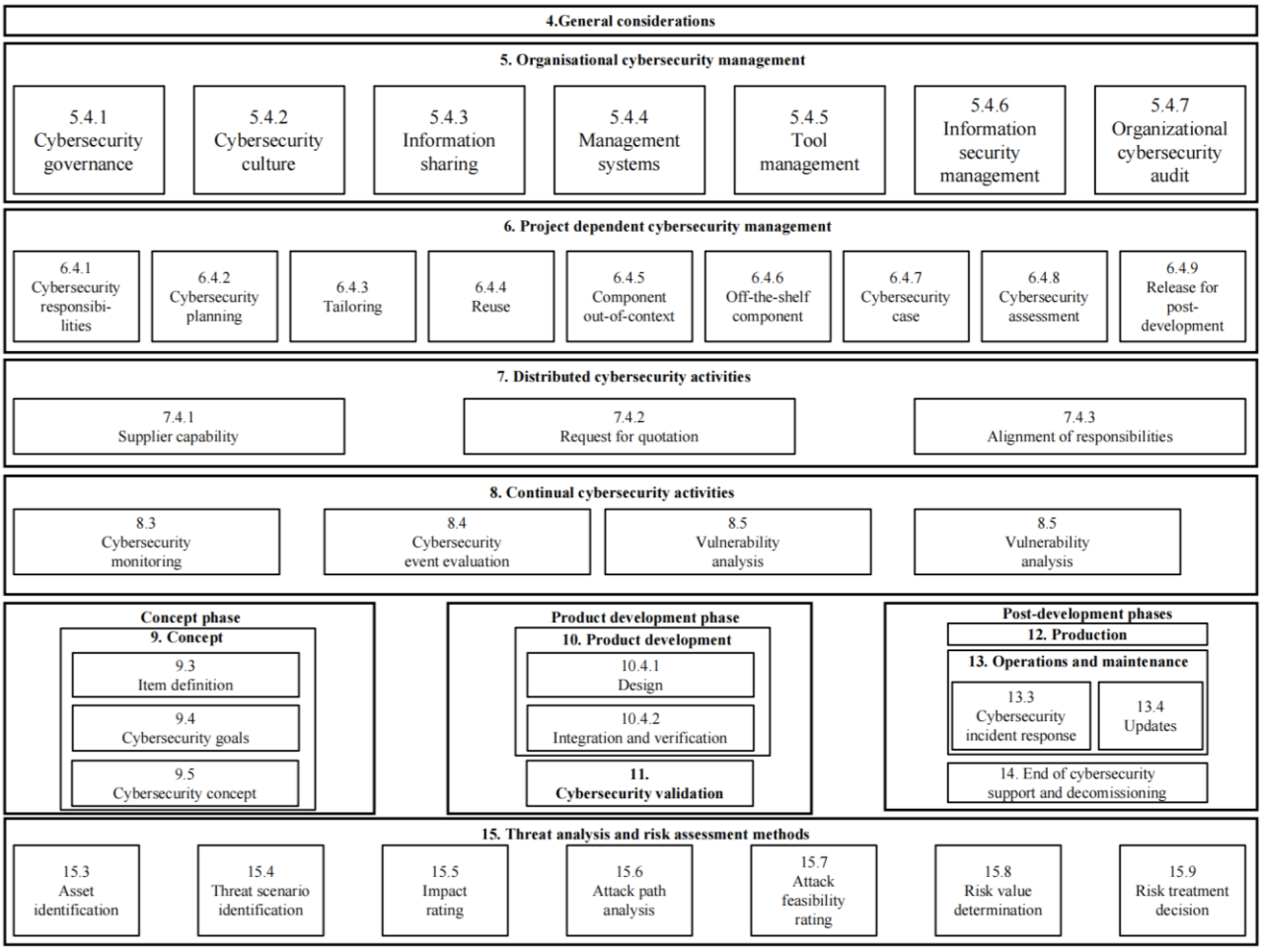

Figure 1 – Cybersecurity management systems [3]

In the ISO/SAE 21434 standard, TARA (threat analysis and risk assessment) is a core component (as shown in Section 15 of *Figure 1*). It is designed to assist in identifying the cybersecurity risks that vehicles may face during the conceptual design stage. From the granularity of the entire vehicle level, the impact and occurrence probability of potential threats are assessed to formulate corresponding security countermeasures [6].

3. PRACTICAL RESEARCH ON THREAT ANALYSIS AND RISK ASSESSMENT OF THE ENTIRE VEHICLE

Based on the theoretical methods provided in *Chapter 15* of the ISO/SAE 21434 standard, a comprehensive risk assessment framework has been constructed at the conceptual stage, with consideration for a systematic approach and practicality.

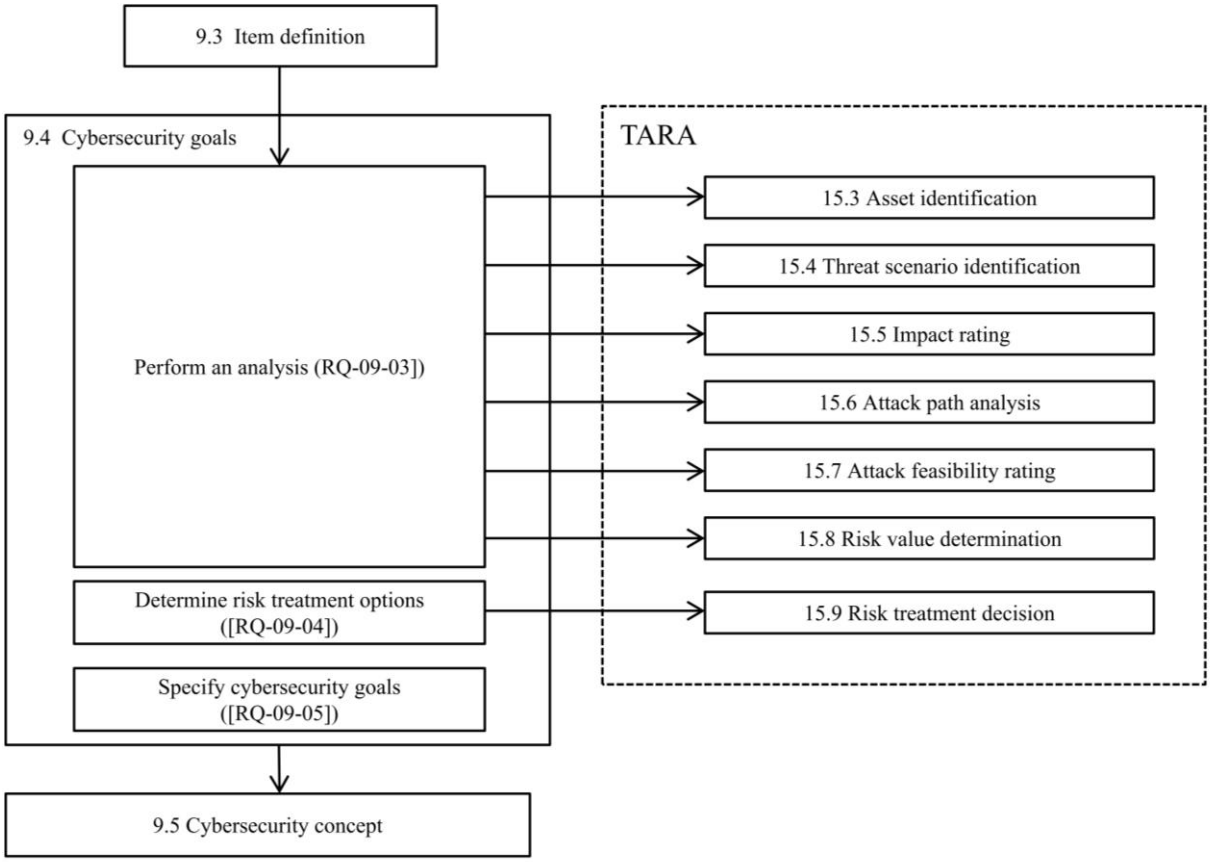

Figure 2 – TARA analysis steps [3]

The framework of TARA analysis (refer to *Figure 2*) mainly includes the following steps:

- *15.3 Asset identification*: Identify the critical assets in the system, such as the firmware and applications of relevant controllers, communication information, data, etc. Understanding the functions and importance of these assets is the basis of the analysis.
- *15.4 Threat scenario identification, 15.6 Attack path analysis, 15.7 Attack feasibility rating*: Identify threat scenarios. Based on the identified assets, conduct threat modelling to identify the threats that may affect these assets and identify potential attack vectors.
- *15.5 Impact rating*: Identify damage scenarios. Based on the identified assets, conduct a cybersecurity attribute analysis to identify the possible impact results after the cybersecurity attributes are damaged.
- *15.8 Risk value determination*: Assess the risks. Conduct a risk assessment for each identified threat, considering the probability of the threat's occurrence and its impact on the assets. Usually, a risk matrix or quantitative analysis method is used to assess the severity of each risk and determine the priority.
- *15.9 Risk treatment decision*: Formulate risk response strategies. According to the results of the risk assessment, formulate corresponding risk response measures. This may include risk avoidance, risk transfer (such as insurance), risk mitigation (strengthening security measures) or risk acceptance (within a controllable range) [3].

3.1 Asset identification

Judgement of relevance

The purpose of conducting a cybersecurity relevance judgement is to determine whether the analysis object is related to cybersecurity. Functions that are not related to cybersecurity do not need to undergo risk analysis. The judgement method is shown in *Figure 3*.

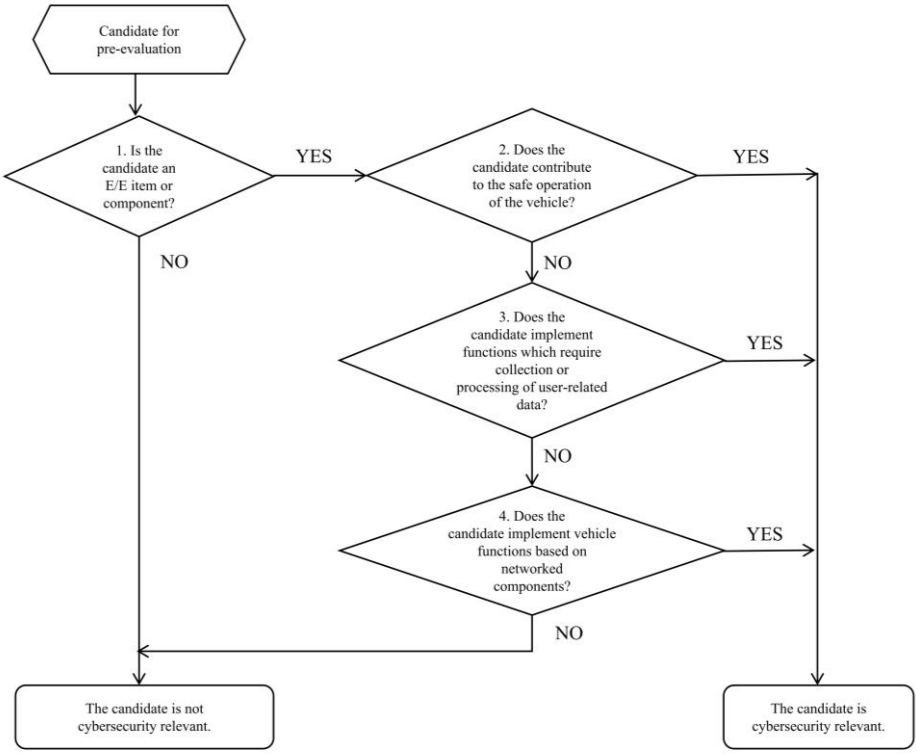

Figure 3 – Judgement logic [3]

The determination process commences with an assessment of whether the system under scrutiny is predicated upon the EE architecture. In accordance with established standards, should the functionality in question not be founded on the EE architecture, it can be categorically determined that said function bears no relevance to the network. Illustrative examples of such non-relevant functions encompass physical interfaces.

If the system is adjudged to be EE-architecture-based, a further assessment of three concurrent conditions is requisite. According to the prescribed methodology, if one or more of these conditions are fulfilled, the function can be deemed pertinent to cybersecurity [3]. These conditions are as follows:

— The nexus between the function and security operations, specifically ascertaining whether the function has implications for vehicle driving safety.
— The capacity of the function to amass user data, such as the collection of personal data, such as facial or fingerprint information.
— The reliance of the function on network connectivity. Network connectivity herein pertains to the necessity of communication modalities such as Bluetooth, WiFi, LTE and in-vehicle CAN/ETH networks for the realisation of the function.

Definition of relevant items

In the standard, the “item” is defined as the relevant electronic devices and software that implement specific functions of the entire vehicle. It includes one or more components as well as their interactions and operating environments. In an actual analysis scenario, a function is generally regarded as an item, such as “unlocking with a Bluetooth key”. This definition emphasises that an item is not just an individual component, but rather the overall consideration of cybersecurity from a system level. There are two key concepts in the definition of an item: *item boundary* (function boundary) and *operation environment* [3].

Item boundary (function boundary): It refers to the connections among the components relevant to the implementation of this function. A data flow diagram should be drawn based on the functional logic. Taking the aforementioned “unlocking with a Bluetooth key” function as an example, refer to the design documents to identify the main in-vehicle components covered by the function, such as the BLE receiver, the left body controller and the right body controller. Identify the flow path of data within the system, including the forwarding direction of instructions and determine the instruction processing in the system. All these components work together as a whole to achieve the function [3].

Operation environment: It refers to the external interfaces of the components that implement this function. Taking the above function boundary as an example, interfaces like the OBD interface, Bluetooth/WiFi module, USB and cellular network interface are included. Although these interfaces do not participate in the implementation of the function, attackers can attack the relevant components through these entry points and thus have an impact on this function. All of these should be encompassed within the operational environment [3].

Through the above steps, a data flow diagram is abstractly drawn as shown in *Figure 4*, which fully depicts the definition of the relevant item. It can be seen that the relevant item is not a single component but a collection of functional systems. This implies that when considering cybersecurity, it is necessary to analyse and assess from the system level rather than looking at each component in isolation. This holistic perspective helps to identify how the interactions among different components affect the overall security [7].

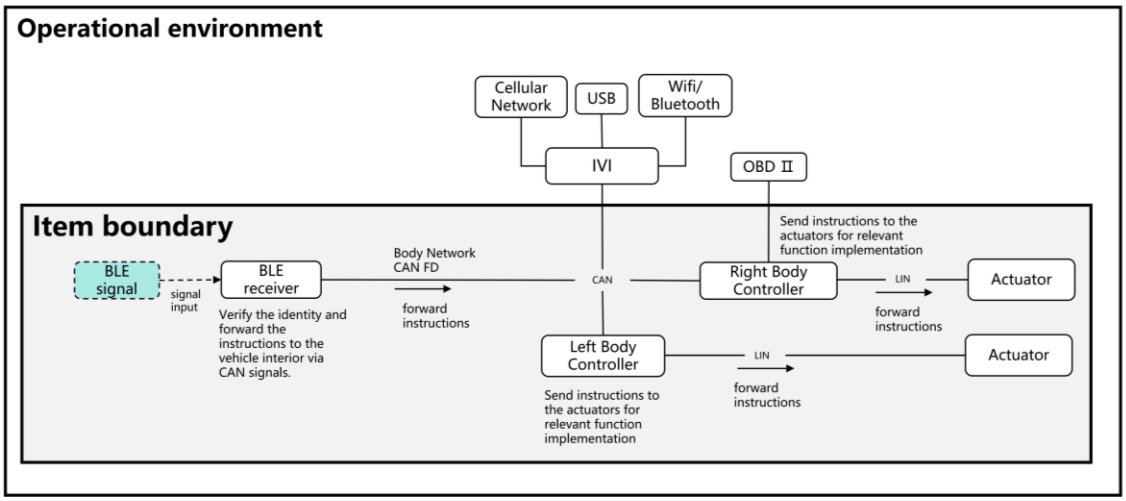

Figure 4 – Data flow diagram (DFD)

Asset inventory

After defining the relevant items, the process of implementing asset identification can be analysed in detail based on the functional logic. For example, when the controller sends a Bluetooth low energy (BLE) signal to the receiver, the following assets can be identified during this process: communication information (i.e. BLE communication information). After the BLE receiver receives the signal, it verifies the identity and records relevant log information. In this step, the following assets can be identified: firmware and applications (controller firmware applications), as well as data (verification record logs). The BLE receiver converts the control instructions into CAN signals through the controller and forwards them to the inside of the vehicle. In this link, the following asset can be further identified: communication information (i.e. CAN communication information). Through the above analysis, the asset identification in each link has clarified the functions of each component within the system and their interrelationships.

In summary, the assets that can be identified for this function include (as shown in *Table 1*):

Table 1 – Asset list

Serial	Asset category	Specific asset name
1	Firmware and applications	Controller firmware application
2	Communication information	BLE communication information, CAN communication information
3	Data	Verification record log

3.2 Threat analysis

Modelling method

Threat modelling is a systematic process used to identify, assess and prioritise potential security threats, thereby providing guidance for the secure design and implementation of systems. Its aim is to sort out possible attack methods so that appropriate defensive measures can be taken at an early stage.

STRIDE is a commonly used threat modelling method which aims to identify six main types of threats. STRIDE is an acronym that stands for the following six threat categories:

— Spoofing: Attackers impersonate legitimate users or systems to gain unauthorised access. For example, logging into a system using stolen credentials.
— Tampering: Attackers make unauthorised modifications to data or systems. For example, tampering with records in a database or modifying software code.
— Repudiation: Users deny the operations they have carried out, resulting in the inability to track or verify the actions. For example, a user deletes a record and then claims that they did not perform this operation.
— Information disclosure: Sensitive information is accessed or disclosed without authorisation. For example, hackers obtain users' personal information or corporate secrets.
— Denial of service: Attackers prevent legitimate users from accessing the system by exhausting or crashing system resources. For example, a distributed denial of service (DDoS) attack.
— Elevation of privilege: Attackers obtain permissions beyond their authorised scope by exploiting system vulnerabilities or misconfigurations. For example, an ordinary user obtains administrator permissions and accesses restricted resources.

Threat scenario analysis

During the threat analysis process, for the identified assets, an analysis is carried out according to the six dimensions of the STRIDE model for threat analysis, which include spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege, in order to determine the corresponding threat scenarios. Take the firmware and application assets as an example:

— *Threat scenario*: Attackers launch an attack on the ECU firmware, causing the ECU firmware to be unable to operate.
— *Threat type*: Tampering.
— *Threat scenario*: Attackers tamper with the ECU firmware, resulting in abnormal operation of the ECU firmware.
— *Threat type*: Information disclosure.
— *Threat scenario*: Attackers extract the ECU firmware, leading to the leakage of information about the ECU firmware.

For assets such as firmware and applications, threats like spoofing, repudiation, information disclosure and elevation of privilege are not applicable [8, 9].

Attack path analysis

Based on the threat scenarios, all possible attack paths need to be constructed. An attack path can be understood as a potential method that leads to the occurrence of a specific threat scenario.

During threat analysis, the external interfaces in the data diagram need to be taken into consideration. Although they may not be directly related to the functions, they may serve as potential attack entry points and pose threats to the target assets. In order to identify the attack paths that may lead to the occurrence of threat scenarios, the following steps should be followed for the analysis:

1) According to the relevant definitions and asset identification results, clearly identify the target assets that are under attack in the threat scenarios.
2) Sort out the external communication interfaces and human-machine interaction assets connected to the target assets as the potential attack entry points that can be exploited.
3) Starting from the available attack entry points, gradually infer the attacks on the target assets until the potential attack paths that can achieve the attacks on the target assets are found. This is regarded as a potentially threatening attack path.

4) Repeat step 3 to continue identifying other potential attack paths until all the potential attack paths initiated from the exploitable assets are completely enumerated.
5) Repeat steps 2 and 3 to successively identify the potential attack paths for other exploitable assets in the operating environment.

Through the above steps, the attack paths that may lead to the occurrence of specific threat scenarios can be identified relatively comprehensively.

For example, in the threat scenario of tampering, the object being attacked is the firmware application of the vehicle controller. According to the data flow diagram of the function shown in *Figure 2*, the gateway participates in the function as an instruction forwarder and is connected to the OBD interface at the same time. If the OBD interface lacks security protection, attackers can launch attacks on the in-vehicle controllers through the OBD interface. This can form a complete attack path to achieve the corresponding threat scenario.

— Attackers utilise the OBD port to launch attacks on the in-vehicle components;
— Tamper with the firmware of the in-vehicle controllers, resulting in abnormal operation of the ECU firmware.

Similarly, for other external interfaces such as the USB interface, when launching attacks on the in-vehicle controllers, the multimedia host needs to be used as a springboard. The attack path is as follows:

— Attackers utilise the USB interface on the IVI to launch attacks on the IVI;
— Obtain the permissions of the IVI and use the IVI to tamper with the firmware of the in-vehicle controllers;
— Result in abnormal operation of the ECU firmware.

By successively repeating the analysis for all the external interfaces in the data diagram, the attack paths for each threat scenario can be identified relatively comprehensively.

Quantitative scoring of attack feasibility

The feasibility of attack paths is scored by using the five dimensions of the HEAVENS model (vulnerability discovery time, professional level, knowledge of the target, window of opportunity and equipment) [10].

— *Elapsed time*: Assess whether attackers can launch attacks by exploiting known or unknown vulnerabilities. If the vulnerabilities have been publicly disclosed and are widely exploited, the feasibility is relatively high. Conversely, if the vulnerabilities have not been discovered or made public yet, the feasibility is relatively low.
— *Specialist expertise*: Assess the technical capabilities and professional knowledge level of attackers. High-level attackers are more likely to successfully execute attacks, so the feasibility is relatively high. On the contrary, low-level attackers may not be able to overcome technical difficulties, and thus, the feasibility is relatively low.
— *Knowledge of the item or component*: Assess the degree of attackers' understanding of the target system. If attackers have detailed target information, such as system architecture, vulnerability intelligence, etc., the feasibility is relatively high. Conversely, if attackers have limited knowledge of the target, the feasibility is relatively low.
— *Window of opportunity*: Assess the timing when attackers launch attacks. If attackers have sufficient time and resources to plan and execute attacks, the feasibility is relatively high. Conversely, if attackers face time constraints or monitoring and other factors, the feasibility is relatively low.
— *Equipment*: Assess the hardware, software, network and other equipment available to attackers. If attackers possess high-performance equipment and tools, the feasibility is relatively high. Conversely, if attackers are limited by equipment resources, the feasibility is relatively low.

By comprehensively considering the above five dimensions and scoring each dimension (as shown in *Table 2*), the feasibility of attack paths can be quantified. Based on the scoring results, the feasibility of attack paths can be judged.

Table 2 – Aggregation of attack potential

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	**Value**	**Enumerate**	**Value**	**Enumerate**	**Value**	**Enumerate**	**Value**	**Enumerate**	**Value**
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialised	4
≤3 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
＞6 months	19	/	/	/	/	/	/	/	/

S (the value of attack feasibility) = indicator value (*elapsed time*) + indicator value (*specialist expertise*) + indicator value (*knowledge of the item or component*) + indicator value (*window of opportunity*) + indicator value (*equipment*) [10].

Table 3 – Attack feasibility rating

Attack feasibility rating	Value
High	0＜S≤13
Medium	13＜S≤19
Low	19＜S≤24
Very low	S≥25

After scoring the attack paths in threat analysis, an aggregation operation needs to be carried out to determine the attack feasibility for specific threat scenarios. The purpose of this aggregation operation is to select the path with the highest feasibility from multiple attack paths. According to the principle of the weakest link, that is, the path with the highest attack feasibility is the most likely to lead to the occurrence of the threat, and it will be used as the attack feasibility scoring level for the threat [11][12]. For details of the scoring classification, please refer to *Table 3*.

3.3 Damage analysis

Asset attribute correlation analysis

The corresponding relationships between the STRIDE method and cybersecurity attributes are as follows:
— Spoofing: Authenticity.
— Tampering: Integrity.
— Repudiation: Non-repudiation.
— Information disclosure: Confidentiality.
— Denial of service: Availability.
— Elevation of privilege: Authorisation. [8, 9]

Damage scenario analysis

Damage scenario analysis (*impact rating*) is a method used to assess the potential impacts that may occur after security attributes are compromised. The damage scenario analysis generally includes the following steps [3]:

Determine functional scenarios: Firstly, it is necessary to fully understand the functions of the vehicle information technology system and determine various functions and behaviours involved in the system under different scenarios. This can be obtained by analysing the system requirements documents, system architecture and relevant design documents [13].

Analyse the impacts after the compromise of security attributes: Combine potential damage events and their impacts to analyse the potential impacts that may occur after the security attributes in the system are compromised. This helps to understand the changes in system behaviour, function degradation, weakened security and other aspects after the compromise [13].

Quantitative scoring of damage scenarios

After determining the damage scenarios, the impact degree on the system or organisation can be measured by quantifying and scoring the severity of the impact. This can be assessed through the impacts in four aspects of SFOP (*Safety/Finance/Operation/Privacy*) [3], as shown in *Table 4*.

Table 4 – Quantitative scoring of damage scenarios

Impact rating	**Criteria for safety impact rating**	**Value**	**Criteria for financial impact rating**	**Value**	**Criteria for operational impact rating**	**Value**	**Criteria for privacy impact rating**	**Value**
Negligible	S0: No injuries	0	The financial damage leads to no effect, negligible consequences, or is irrelevant to the road user.	0	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.	0	The privacy damage leads to no effect, negligible consequences or is irrelevant to the road user. The information regarding the road user is not sensitive and difficult to link to a PII principal.	0
Moderate	S1: Light and moderate injuries	10	The financial damage leads to inconvenient consequences that the affected road user will be able to overcome with limited resources.	10	The operational damage leads to partial degradation of a vehicle's function.	1	The privacy damage leads to inconvenient consequences for the road user. The information regarding the road user is: a) sensitive but difficult to link to a PII principal; or b) not sensitive but easy to link to a PII principal.	1
Major	S2: Severe and life-threatening injuries (survival probable)	100	The financial damage leads to substantial consequences which the affected road user will be able to overcome.	100	The operational damage leads to the loss or impairment of an important vehicle function.	10	The privacy damage leads to a serious impact on the road user. The information regarding the road user is: a) highly sensitive and difficult to link to a PII principal; or b) sensitive and easy to link to a PII principal.	10
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries	1000	The financial damage leads to catastrophic consequences that the affected road user might not overcome.	1000	The operational damage leads to the loss or impairment of a core vehicle function.	100	The privacy damage leads to a significant or even irreversible impact on the road user. The information regarding the road user is highly sensitive and easy to link to a PII principal.	100

S (*impact score*) = indicator value (*safety*) + indicator value (*economy*) + indicator value (*operation and compliance*) + indicator value (*privacy laws and regulations*) [9].

Through damage scenario analysis, the relationship between functional scenarios and security attributes can be better understood, which helps to assess the vulnerability of the system when facing potential threats. Refer to the above score reference table (*Table 5*) and obtain the impact level based on the scores.

Table 5 – Impact analysis rating

Impact analysis rating	Value
Negligible	0<S<20
Moderate	20<=S<100
Major	100<=S<1000
Severe	1000<=S

3.4 Risk value determination

The risk level can be determined through the risk assessment matrix. As shown in *Table 6*, the matrix combines the feasibility of attacks and the degree of impact to determine the priority of risks and adopt corresponding risk disposal measures. It helps organisations determine the risk level more accurately and take appropriate control and mitigation measures in the process of risk management [12].

Table 6 – Risk matrix

Risk rating	Impact rating				
Attack feasibility rating	/	Negligible	Moderate	Major	Severe
	Very low	Very low	Very low	Very low	Low
	Low	Very low	Very low	Low	Medium
	Medium	Very low	Low	Medium	High
	High	Very low	Medium	High	Critical

3.5 Risk treatment

Risk treatment strategies

The main risk treatment strategies are as follows:

— *Risk reduction:* Manage the risk level by introducing, deleting or changing security controls so that the residual risk can be re-assessed to an acceptable level.
— *Risk acceptance*: Retain the risk without taking further measures based on the results of the risk assessment.
— *Risk avoidance*: Avoid activities or behaviours that may cause specific risks.
— *Risk transfer*: Based on the results of the risk assessment, share and transfer the risk to another party that can manage the risk most effectively.

When choosing risk treatment strategies, the following bases need to be considered:

— Risk level: Based on the results of the risk assessment, give priority to dealing with high-risk events or threats. High-risk events may have a serious impact on the organisation.
— Cost-benefit consideration: Consider the cost-benefit of taking control measures, including the investment in terms of time, manpower, finance and resources. Weigh the costs and benefits and choose appropriate treatment strategies.
— Feasibility and sustainability: Consider the feasibility and sustainability of the treatment strategies. Determine whether the strategies can be effectively implemented in actual operations and can continuously protect the organisation from risks.
— Laws, regulations and compliance requirements: Consider the applicable laws, regulations and compliance requirements to ensure that the chosen risk treatment strategies comply with legal and regulatory requirements.

Goals of cybersecurity

In actual assessment practices, the risk reduction strategy will be adopted for risks with an assessment level of “medium” or above according to the risk matrix. When implementing the risk reduction strategy, it is necessary to first formulate the cybersecurity objectives.

Formulating the cybersecurity objectives is needed to clarify the goals and expected results to be achieved during the risk reduction process, to guide the subsequent control measures and action plans. The cybersecurity objectives should be specific, measurable and traceable to ensure the effectiveness of the implementation process and the evaluability of the results [12].

For example, in the above case, the following cybersecurity objective can be formulated: The integrity of the firmware and applications of the vehicle-mounted controller should be protected.

Cybersecurity requirements

The cybersecurity objective represents the highest level of security requirements. Specific control measures are refined based on the cybersecurity objective. When formulating control measures, the following aspects need to be considered:

— Direct coverage of the cybersecurity objective: Control measures should be directly related to the cybersecurity objective to ensure that the implementation of these control measures can achieve the desired effect. For example, it is required that relevant controllers need to achieve a secure boot to ensure the integrity of the controller firmware [7, 15].
— Consider the complete coverage of threat scenarios and attack paths: When formulating control measures, it is necessary to consider the threat scenarios of the output objective and ensure that the control measures can cover the possible attack paths in these threat scenarios. This helps prevent the omission of risks and the existence of vulnerabilities and ensures the comprehensive achievement of the cybersecurity objective [14, 15].
— Consider implementable technologies: When formulating control measures, it is necessary to consider feasible technical solutions. The feasibility of the technology is an important consideration factor in formulating control measures, and appropriate control measures need to be selected and applied based on the currently available technologies and practices in the industry [16].

4. CONCLUSION

This paper puts forward a framework method for threat analysis and risk assessment of intelligent connected vehicles based on ISO/SAE 21434. Through the structured analysis process, cybersecurity risks can be identified and assessed more comprehensively, and major threats can be reduced. The results of risk assessment can help automobile manufacturers identify the most critical security issues and provide targeted security guidance for manufacturers and developers.

REFERENCES

[1] Li J, Liu H, Wang H. Editorial for the special issue on safety for intelligent and connected vehicles. *Engineering*. 2024;33(2):1-2. DOI: 10.1016/j.eng.2024.01.005

[2] Yang DG, et al. Intelligent and connected vehicles: Current status and future perspectives. *Science China (Technological Sciences)*. 2018;61(10):1446-1471. DOI: 10.1007/s11431-017-9338-1

[3] International Organization for Standardization. ISO 21434: *Road vehicles—Cybersecurity engineering,* 2021.

[4] Bergler M, Tavakoli-Kolagari R. Automotive software security engineering based on the ISO 21434. In: Proceedings of the 2023 5th World Symposium on Software Engineering (WSSE '23). *Association for Computing Machinery*. 2023:17-26. DOI: 10.1145/3631991.3631994

[5] Vielberth M, et al. Elevating TARA: A maturity model for automotive threat analysis and risk assessment. In: *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). Association for Computing Machinery*. 2024:1-9. DOI: 10.1145/3664476.3670888

[6] Macher G, et al. A review of threat analysis and risk assessment methods in the automotive context. *Lect Notes Comput Sci*. 2016;9556:130-141. DOI: 10.1007/978-3-319-45477-1_11

[7] Schmittner C, et al. Using SAE J3061 for automotive security requirement engineering. *Lect Notes Comput Sci*. 2016;9556:157-170. DOI: 10.1007/978-3-319-45480-1_13

[8] Zhang Y, et al. Information securityrisk assessment of DCS based on STRIDE threat model. *Journal of Shanghai Jiaotong University*. 2018;52(S1):142-146.

[9] Li F. Android application security testing method based on STRIDE. Shanghai: Donghua University, 2017.

[10] Lautenbach A, Almgren M, Olovsson T. Proposing HEAVENS 2.0—an automotive risk assessment model. In: Proceedings of the 2021 ACM SIGCOMM Conference on Data Communication. *Association for Computing Machinery*; 2021:1-10. DOI: 10.1145/3488904.3493378

[11] Costantino G, De Vincenzi M, Matteucci I. A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Genoa, Italy, 2022, pp. 340-347. DOI: 10.1109/EuroSPW55150.2022.00041

[12] Ward D, Wooderson P. Automotive cybersecurity: An introduction to ISO/SAE 21434. Warrendale, PA, USA: SAE International; 2021.

[13] C. Ebert. Security requirements engineering: From TARA to PenTest, *2019 IEEE 27th International Requirements Engineering Conference (RE)*. Jeju, Korea (South), 2019, pp. 500-501. DOI: 10.1109/RE.2019.00074

[14] Japs S, et al. Model-based systems engineering using security design patterns in the context of ISO/SAE 21434. *Proceedings of the Design Society*. 2023;3:2675-2684. DOI: 10.1017/pds.2023.268

[15] Baotian L, et al. Research on multi-layer cybersecurity protection system of intelligent and connected vehicles. *China Automotive Technology and Research Center.* 2023. DOI: 10.1117/12.2684504