Hindawi
Security and Communication Networks
Volume 2020, Article ID 7169720, 14 pages
https://doi.org/10.1155/2020/7169720

WILEY | Hindawi

Research Article

A Systematic Approach for Cybersecurity Design of In-Vehicle Network Systems with Trade-Off Considerations

Jinghua Yu and Feng Luo

School of Automotive Studies, Tongji University, Shanghai, China

Correspondence should be addressed to Feng Luo; luo_feng@tongji.edu.cn

Received 28 May 2019; Revised 14 February 2020; Accepted 9 July 2020; Published 5 August 2020

Academic Editor: Sherif Abdelwahed

With the increasing connectivity of modern vehicles, protecting systems from attacks on cyber is becoming crucial and urgent. Meanwhile, a vehicle should guarantee a safe and comfortable trip for users. Therefore, how to design a cybersecurity-critical system in vehicles with safety and user experience (UX) considerations is increasingly essential. However, most co-design methods focus on safety engineering with attack concerns and do not discuss conflicts and integration, and few contain the UX aspect. Besides, most existing approaches are abstract at a high level without practical guidelines. This paper presents a literature review of existing safety and security design approaches and proposes a systematic approach for cybersecurity design of in-vehicle network systems based on the guideline in SAE J3061. The trade-off analysis is performed by using association keys and the proposed affecting map. The design process of an example Diagnostic on Internet Protocol (DoIP) system is reported to show how the approach works. Compared with the existing approaches, the proposed one considers safety, cybersecurity, and UX simultaneously, solves conflicts qualitatively or quantitatively, and obtains trade-off design requirements. This approach is applicable to the cybersecurity-driven design of in-vehicle network systems in the early stage with safety and UX considerations.

1. Introduction

Cybersecurity is an essential attribute of in-vehicle network systems. Functions like x-by-wire and autonomous driving applications in modern vehicles largely depend on the signal transmitting in communications systems. Due to the increasing number of vehicle-to-everything (V2X) innovations, more interfaces to the external world raise attack probabilities of in-vehicle systems. Besides, the rising system complexity makes it more difficult to design a secure system with few vulnerabilities. Hackers may easily get unauthorized access into a system to eavesdrop and tamper with data, which may cause privacy issues, safety accidents, or even disasters. Therefore, cybersecurity design should be conducted for in-vehicle security-critical systems.

Since the original purpose of a vehicle is to provide a safe and comfortable trip for users, safety and UX should also be concerned. However, safety, cybersecurity, and UX design are normally designed by different teams separately, which results in possible conflicts in different dimensions. For example, a complex encryption mechanism not only enhances the confidentiality of the data but also increases the delay and may result in a belated emergency reaction of the vehicle. The slow processing speed of some interactive functions may also lead to users' complains, which affect the reputation and incomes of manufactures. Therefore, a trade-off design is necessary to solve possible interferences and figure out an optimized solution.

To achieve the trade-off goal, the designer should consider all relevant issues at the beginning of the system design instead of attempting to add individual mechanisms into existing systems or solve conflicts separately and partially. In this research, a systematic approach is proposed to guideline the design of a cybersecurity-critical system with trade-offs.

The paper is organized as follows. Section 2 summarizes the existing approaches, clarifies confusing concepts, and discusses research gaps as well as our contributions. Section 3 introduces the methodology with the process framework,

Threat Analysis and Risk Assessment (TARA) methods, and association keys of the co-design. Section 4 demonstrates the design process of an example DoIP system to show how to use the proposed approach for the design and then discusses the highlights and deficiencies of the current study. Section 5 concludes the article containing the benefits of the co-design and our future work.

2. Related Work and Our Contribution

This section introduces the current research status related to safety and cybersecurity design as well as co-design approaches in the automobile or relevant industries. Some confusing concepts are identified and integrated into a concept map. Research gaps and our contributions are presented in the end.

2.1. Safety Design. Standards have been published to guide the safety design in the automotive industry. The *Road Vehicles–Functional Safety standards* (ISO 26262) provide requirements and processes to migrate risks from system failures and hardware random failures and ensure the functional safety of vehicle systems. ISO 26262 standards cover the whole lifecycle including management, development, production, and operation phases [1]. The *Road Vehicles–Safety of the Intended Functionality (SOTIF) standard* (ISO/PAS 21448) extends the range of hazard causes addressed in ISO 26262 and focuses on hazardous events resulting from functional insufficiencies and reasonably foreseeable misuse by people [2].

Concerning safety analysis approaches, usually referred as Hazard Analysis and Risk Assessment (HARA), Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), and Failure Mode Effects and Diagnostic Analysis (FMEDA) are widely used approaches in industries. FTA is a top-down method to find out unknown causes based on the known impacts, while FMEA and FMEDA are bottom-up methods to envision unknown impacts through known causes. Besides, another structured method called HAZard and OPerability (HAZOP) analysis uses guide words to identify risks associated with operation and maintenance as well as operability problems of a system [3]. Additionally, Bouissou and Bon introduced a modelling formalism called Boolean logic Driven Markov Process (BDMP) that combined fault trees and Markov models to modelling behaviors and properties of complex dynamic systems [4]. Leveson and Thomas proposed an approach named Systems-Theoretic Process Analysis (STPA), which is based on Systems-Theoretic Accident Model and Process (STAMP) model and envisions safety losses resulting from humans, physical components, and environments [5].

The human factor, as an indispensable aspect in safety issues, has also been discussed in the safety design field. Obviously, a good design of Human-Machine Interface (HMI) can reduce the probability of human misuses and other unexpected behaviors. Wang et al. presented a framework for function allocations for an HMI and explored some new ergonomic principles for comfort and safety driver interfaces [6]. Besides, human factors have already been merged in the process of some safety design approaches. The control structure in the STPA approach can include human actions and factors in human societies, like policies and government behaviors, to analyze the safety issues at high levels [7]. In ISO 26262, human operation ability determines the assessment of the hazard controllability in the HARA process, which may affect the Automotive Safety Integrity Level (ASIL) and safety strategies of target systems [1]. Furthermore, since driver's intervention is still necessary for current automated vehicles, challenges of human factors are identified, which contains driver inattention and distraction, situational awareness, overreliance and trust, skill degradation, and motion sickness [8]. Biever et al. investigated Automated Driving System (ADS) collisions and extracted common factors. Human operator concerns, including training, vigilance, and supervisory, are primary causes in some crashes, which teach lessons for future safety designs [9].

2.2. Cybersecurity Design. The *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* (J3061), published by Society of Automotive Engineers (SAE) in 2016, provides a recommended process for the design of cybersecurity systems in vehicles to help designers to analyze threats, assess risks, and think over security issues throughout the whole lifecycle [10]. Schmittner et al. shared their experience of using J3061 in the concept phase and reported security activities of an in-vehicle communication gateway as the example [11]. The Japanese Automotive Standard Organization (JASO) published the TP15002 guideline to standardize the procedures of the security design in the early stage of the development [12]. Kawanishi et al. proposed better solutions for security evaluation based on TP15002 [13, 14]. The E-safety Vehicle Intrusion Protected Application (EVITA) project, funded by European Union, designed, verified, and prototyped a security architecture for in-vehicle networks where security-relevant components and data are pretested against unauthorized access. The EVITA project proposed an approach to derive security requirements in the early design stage and demonstrated the analyses of defined use cases with details [15].

Some general frameworks for security design in other industries also provide solid references. The *Information Technology–Security Techniques–Evaluation Criteria for IT Security* (ISO/IEC 15408) standards proposed the evaluation process and assurance measures to meet the security requirements of IT products and is useful for development, evaluation, and procurement of product's security functionalities [16]. The *Framework for Improving Critical Infrastructure Cybersecurity*, issued by National Institute of Standards and Technology (NIST), is a risk-based approach to managing cybersecurity risks and provides common taxonomies and mechanisms to ensure the cybersecurity of critical infrastructures [17].

The TARA is the key step to identify threats and assess risks in the design process. Table 1 lists prevalent TARA methods with brief introductions.

Table 1: TARA method list.

Name	Brief introduction
EVITA method	A TARA method in the EVITA project which concerns issues in four aspects (operational, safety, privacy, and financial) [15]
TVRA	Threat, vulnerabilities, and implementation risk analysis method, which is a process-driven threat and risk assessment method developed by the European Telecommunications Standards Institute (ETSI) [10]
OCTAVE	Operationally critical threat, asset, and vulnerability evaluation method, which is suitable for enterprise information security risk assessment [10]
HEAVENS security model	A TARA method in the HEAling vulnerabilities to enhance software (HEAVENS) project, which is based on Mircosoft's STRIDE threat model and focuses on the method, process, and tool support for TARA [10]
Attack trees	A method for vulnerability analysis, which identifies attack goals, objectives, methods, and attack scenarios of the target system [10]
SW vulnerability analysis	A method to find vulnerabilities in codes [10]
SHIELD	A method to analysis security, privacy, and dependability (SPD) for the embedded system by using control science theory [18]
NHTSA method	A threat modelling approach by using threat matrix in the technical report of U.S. National Highway Traffic Safety Administration (NHTSA) [19]
BRA	The binary risk analysis method which is a lightweight risk analysis tool for a quick assessment and used as a part of other TARA processes like OCTAVE [20]
NIST SP 800-30	A risk assessment guide proposed in NIST SP 800-30 and applicable to identify, estimate, and prioritize risks for a large range of security-critical targets [21]

Each method has its merits and demerits as well as applicable scopes. Macher et al. analyzed most of the mentioned TARA in automotive context and provided comparative evaluation results for design references [22].

2.3. Co-Design. ISO 26262 requires that 'the organization shall institute and maintain effective channel functional safety, cybersecurity, and other disciplines (e.g., quality and non-electrical/electronic related safety) that are related to the achievement of functional safety and guides the potential interaction of functional safety with cybersecurity [23]. However, ISO 26262 only focuses on achieving functional safety and discusses the interactions generally without working flows.

SAE J3061 describes two options of the co-design between safety and cybersecurity. The first one is to apply a cybersecurity process separately with integrated communication points to the safety process. Two teams in different fields are required to perform safety or security design individually and combine outcomes of analogous steps through potential communication paths between parallel activities. The other option is to apply the cybersecurity process in conjunction with the safety process. The integration may be done by performing both activities in conjunction with each other in the same team or using an integrated technique that covers both safety and cybersecurity at the same time for parallel activities [10]. Macher et al. discussed merits and demerits of both options and took an electrical steering column lock system in vehicles as an example to show how to perform co-analysis by using SAHARA, which is an integrated technique covering hazard and threat analysis [24].

However, SAE J3061 only provides general ideas of the co-design. Approaches with more details and examples are proposed in other papers. T. Amorim et al. provided a systematic pattern-based approach to interlink safety and security patterns. The co-engineering loop was introduced into the waterfall engineering lifecycle to analyze and solve conflicts between both sides [25]. Pereira et al. presented an integrated approach, in which two teams work separately in parallel steps and then work cooperatively for integrated analysis. Feedback loops are required to adjust the hazard or threat identification and solutions [26]. A European working party called SoQrates introduced an assessment model with the integration of the automotive SPICE (Software Process Improvement and Capability Determination), the functional safety, and the cybersecurity to ensure both safety and security aspects based on existing process landscape [27].

Many co-analysis methods are proposed to cover both safety and security concerns, which are listed in Table 2.

Schmittner et al. reported a case study by using FMVEA and CHASSIS for automotive cyber-physical systems and discussed the applicability of both methods [33]. Wei presented the analyses of passenger autonomous vehicles by using STPA-Sec and CHASSIS and compared the achieved outcomes of the same target system [34].

2.4. Confusing Concept. The interpretation of safety and security varies in different contexts, which usually leads to confusions. A concept map of safety and security in the automotive domain is proposed by synthesizing and integrating definitions in various publications. The map in Figure 1 illustrates the key elements and relationships of definitions and clarifies confusing concepts effectively and unambiguously.

The horizontal axis represents the causes that may result in harmful consequences. "System" means factors that are only related to the system itself, such as system failures caused by design faults and random hardware failures. Besides, functional insufficiencies of the intended

Table 2: Co-analysis method list.

Name	Brief introduction	Gaps in co-analysis
FMVEA [28]	Failure mode, vulnerabilities, and effect analysis, a method of safety and security cause-effect analysis by using templates from the FMEA method	No interaction concerns
CHASSIS [29]	Combined harm assessment of safety and security, a systematic method for information system to analyze safety and security interactively by using HAZOP guidewords	No conflicts analysis between safety and security
SAHARA [30]	Security-aware hazard analysis and risk assessment, a method to perform security-aware identification of safety hazards and analyze impacts of security issues on safety aspects based on the STRIDE threat model	No conflicts analysis between safety and security
STPA-sec [7]	An extension of STPA for security, a method to identify losses, security vulnerabilities, and insecure control actions, in which steps are identical to the ones in STPA and can be executed in parallel	No discussion about the dependencies between both safety and security
STPA-SafeSec [31]	An optimized method of STPA-Sec, which integrates STPA and STPA-Sec into one concise framework and detects interdependencies between safety and security constraints	Only considers safety and security aspects, no UX concerns
BDMP-based method [32]	A BDMP-based method, which allows graphical modelling and advanced characterization of safety and security interdependencies	Only considers safety and security aspects, no UX concerns

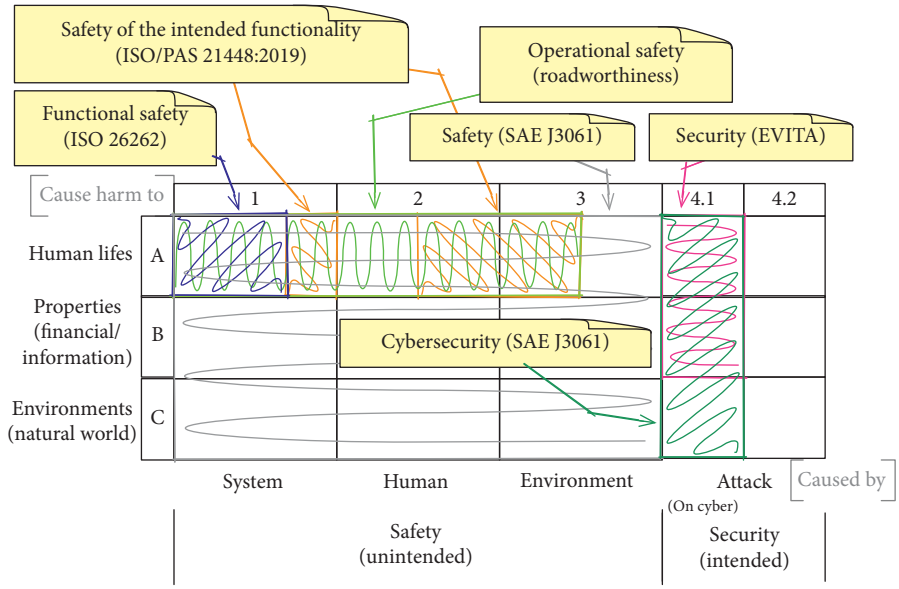


Figure 1: Concept map of safety and security.

functionality caused by the insufficient design of the system also belong to this category. The factor "Human" is divided into "Human Errors" and "Misuse by Human.". The former means that something has been done not intended by the actor and may lead system outside its acceptable limits [35], while the latter refers to the usage of the system by a person in a way not intended by the manufacturer [2]. The third factor 'Environment' contains external physical conditions, like temperature and humidity, and system prerequisites, like correct data inputs from sensors. The final 'Attack' represents any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to or make unauthorized use of an asset [36].

The vertical axis represents the categories of the potential harmed objects. Physical injuries or damages to the health of persons like bone fracture, traumatism, or even death belong to the first group "Human Lives." The second one "Properties" includes both financial and information losses. Financial losses are the extra expenditure cost by the occupant, and information losses refer to information relevant issues like data leakage and privacy exposure. The group "Environment" represents the natural world in which people, animals, and other lives live, and the harm to the environment could be the emission of toxic gases, the waste of resources, and so on.

Table 3 lists the definitions of the confusing concepts and their mappings in the proposed map.

The grids related to 4.2 are uncovered in the current industry documents. Situations in these grids, like the violent physical attack on vehicles, are still probable and critical. However, this part is out of the research scope.

2.5. Gap and Our Contribution. Two main gaps are identified based on the current states in this research field. Firstly, most co-design approaches only concern interactions between safety

Table 3: List of definitions and mappings of confusing concepts.

Term	Definition	Source	Mapping
Safety	The state of a system that does not cause harm to life, property, or the environment	SAE J3061 [10]	Ax, Bx, Cx ($x = 1, 2, 3$)
Functional safety	The absence of unreasonable risk due to hazards caused by malfunctioning behaviors of E/E system	ISO 26262 [37]	Part of A1
SOTIF	The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or reasonably foreseeable misuse by the person	ISO/PAS 21448 : 2019 [2]	Part of (A1, A2, A3)
Operational safety	The combination of functional safety, safety of the intended functionality, and safety in use	A research article [38]	A1, A2, part of A3
Security	Security requirements are identified based on four types of possible security breaches, which are safety, financial, privacy, and operational	EVITA project [11]	Ax, Bx ($x = 4.1$)
Cybersecurity	The state of a system that does not allow exploitation of vulnerabilities to lead to losses, such as financial, operational, privacy, or safety losses	SAE J3061 [10]	Ax, Bx, Cx ($x = 4.1$)

and security, and other aspects (e.g., UX and development cost) cannot be integrated into existing approaches. Secondly, current co-design approaches are presented at high levels and lack of concrete guidelines with operation details, which makes them difficult to be used in practical cases directly.

To fill the gaps, we first summarize the state of the art in relevant fields and clarify confusing concepts. Then, a systematic trade-off design approach based on the SAE J3061 process is proposed, in which safety, security, and UX are considered integrally via association keys. Finally, an example design process of a DoIP system is presented with details to demonstrate how to use the proposed approach in practices.

3. Methodology

In this section, a systematic approach is proposed with the process framework and association keys. The TARA method from EVITA project is also introduced to show how the TARA process works.

3.1. Design Process Framework. The proposed design process, based on the process in SAE J3061, is shown in Figure 2 with marks of the modified, added steps compared with the J3061 framework.

The process starts from the system definition, which specifies not only the analysis scope but also system features containing the reference architecture, use cases, and key parameters.

Then, the TARA phase identifies potential threats by using systematic methods like attack tree analysis (ATA) and achieves risk levels of those threats, based on which security goal are derived. System parameters can also be refined to supplement the previously defined parameters.

The goal of the security concept phase is to determine security strategies and requirements. To get a trade-off solution, impacts of enumerated strategies on parameters are analyzed via an affecting map. If the merits and demerits of a strategy are obvious, designers can make a quick decision by comparing and assessing countermeasures qualitatively. Otherwise, parameters should be quantified by calculation or stimulation for each possible countermeasure.

The preliminary assessment with the chosen strategy is then performed and represents the primary expected attributes of the system.

Finally, the designer reviews the overall analysis process and outputs the results, which are inputs of the next development stage.

Compared with the security design framework in J3061, the proposed one considers the influences of strategies on multiattributes. The affecting map is created to analysis impacts, and qualitative or quantitative evaluations are introduced to help to determine a trade-off strategy. Besides, steps are refined with details to make the framework more practical and operable. Since the proposed framework is based on an existing industry guideline, designers can use the new framework by adding particular steps into their existing working system without too many efforts.

3.2. TARA Method. TARA is one of the key steps in the framework and affects the design strategy. The EVITA method is presented here, which is used in the example of this paper.

Firstly, the attack tree (Figure 3) of an attack goal is established to attain potential threats of the target system, in which attack objectives, methods, and scenarios are identified according to experts experience or brainstorms. Child nodes are the refined means or scenarios of the parent node and are linked to the parent node with logic gates. The "or" gate means that the achievement of any subnode can result in achieving its parent node, while the "and" gate means that all subnodes are necessary to achieve their parent node.

Secondly, the severity (S) of each objective is categorized into 0 (no hazard) to 4 (severest) classes according to the "Severity Classification Scheme" table in [15] to represent the severity of the attack objects in four aspects, which are safety, privacy, financial, and operational. The severity values are notated as S_S, S_P, S_F, and S_O.

Thirdly, the probability of each attack scenario is evaluated by scoring various factors according to the "rating of aspects of attack potential" table in [15]. The attack probability (AP) value, representing the relative likelihood of attacks, can then be marked from 5 (highest probability) to 1 (lowest probability) and notated as P_{Attack_n}. The probability

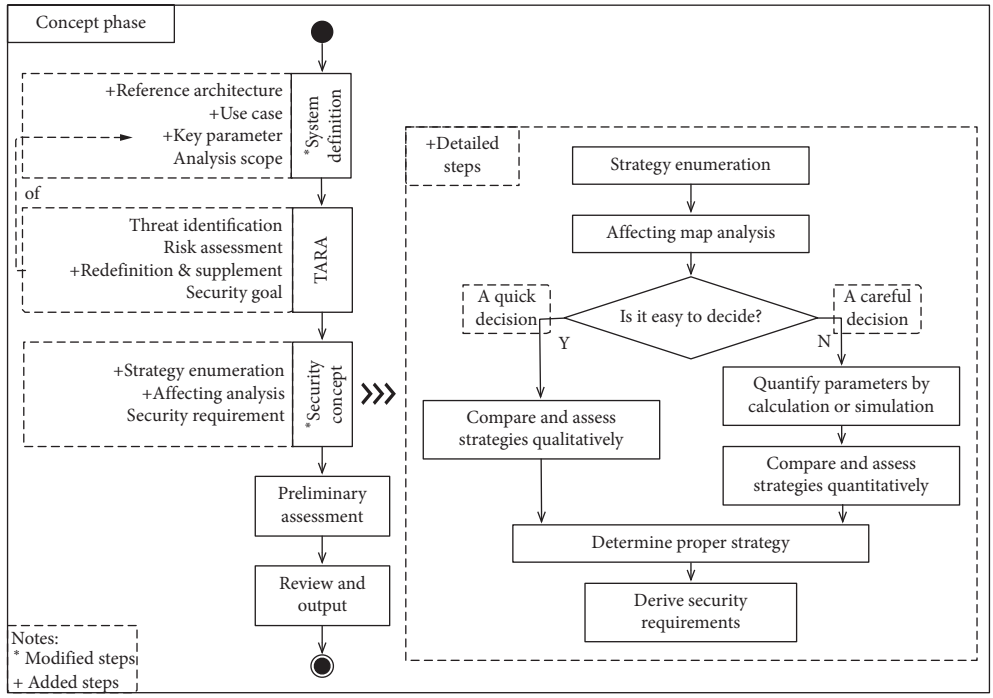


Figure 2: Design process framework.

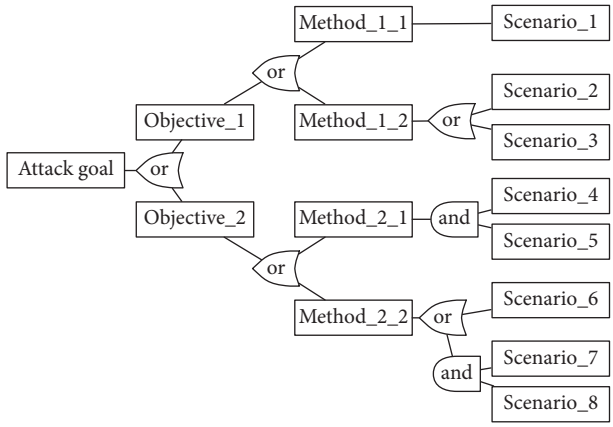


Figure 3: A general attack tree.

of each method, called combined attack potential (CAP) and notated as A_{Method}, is calculated based on P_{Attack_n} and the relationship of attacks. For attacks with the "or" relationship, the CAP is the highest value of the probability of relevant attacks, while the CAP is the lowest value of those with the "and" relationship (formulas 1 and 2):

$$A_{Method\_n\_or} = \max\left\{P_{Attack\_n}\right\}, \quad (1)$$

$$A_{Method\_n\_and} = \min\left\{P_{Attack\_n}\right\}. \quad (2)$$

Finally, the risk level (RL) of each attack method can be achieved by mapping the S and CAP in risk graphs. The RL can be notated as $R_{Method\_n}(S_{i\_Objective\_n}$ and $A_{Method\_n})$, and a risk map of nonsafety threats is shown in Table 4, in which a bigger risk number represents a higher risk of a threat.

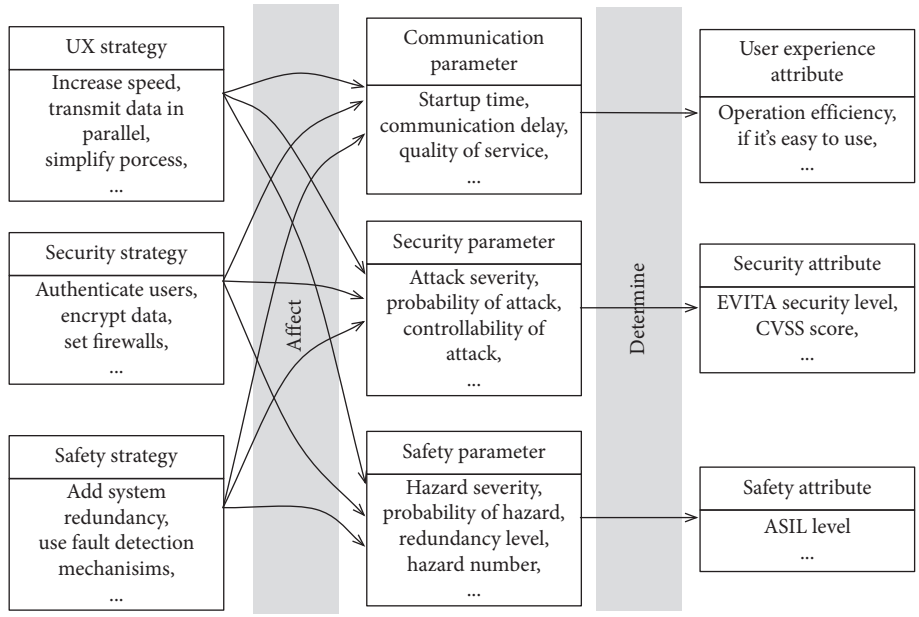
Table 4: Risk map of nonsafety threat in [15].

Security risk level (R)		Combined attack probability(A)				
		$A=1$	$A=2$	$A=3$	$A=4$	$A=5$
Security risk level (S_i)	$S_i=1$	R0	R0	R1	R2	R3
	$S_i=2$	R0	R1	R2	R3	R4
	$S_i=3$	R1	R2	R3	R4	R5
	$S_i=4$	R2	R3	R4	R5	R6

3.3. Association Key. One essential element in this approach is the system parameter, which is the association key among different aspects. System parameters are a set of factors, whose values determine corresponding behaviors of a system. Parameters are categorized into three groups in this research, which are communication, security, and safety groups. Parameters can be measured directly or quantified by proper methods.

The system attributes, which represents system features concerned by designers, are affected by relevant parameters. For example, the security attribute is related to parameters like the attack severity and threat probability, and the data transmitting time determines UX when a user performs vehicle diagnostics. The system attribute can be assessed to indicate system abilities. The system safety, for instance, can be tagged by ASIL defined in ISO 26262 [39], and the security can be judged by the EVITA risk levels [15].

Figure 4 shows the relationship among design strategies, system parameters, and attributes. Since it may be complex and difficult to figure out the impacts of strategies on various attributes directly, the system parameter is injected between them as the bridge to help to identify conflicts or reinforcements and work out a trade-off solution.



Abbreviations:
1. EVITA: E-safety vehicle intrusion protected applications project
2. CVSS: common vulnerability scoring system
3. ASIL: automotive safety integrity Level

Figure 4: Relationship among strategies, parameters, and attributes.

4. Implementation

Since the automotive ethernet (AE) has been a hot candidate for in-vehicle communication solutions, the design of a DoIP system based on AE technologies is presented as an example to demonstrate how to use the proposed approach as well as provide the design guideline with details for similar use cases.

4.1. System definition

4.1.1. Reference Architecture. The architecture of the example system is shown in Figure 5. It is an in-vehicle domain-based architecture with a central gateway (CGW) and five domain controller units (DCUs). Only the ETE, central gateway, and vehicle dynamics DCU blocks in Figure 5 are relevant in this example. The external test equipment (ETE) connects CGW directly through an on-board diagnostics (OBD) interface. CGW, as the DoIP edge node and gateway, establishes a connection with ETE according to DoIP protocols and routes data to the target DCU in the vehicle dynamics domain.

4.1.2. Use Case. Generally, the applications of a diagnostic system can be divided into two groups, which are data uploading and downloading. The former retrieves information like diagnostic trouble codes (DTCs) from supported electronic control units (ECUs) in vehicles, while the latter sends updated configurations or software into ECUs. The DCU firmware update based on DoIP protocols is taken as the example use case in this paper. The sequence diagram shown in Figure 6 describes working sequences of the use case on network layer complying with the ISO 13400 standards.

4.1.3. Key Parameter. The parameters concerned in this example are listed in Table 5 with notations and descriptions.

4.1.4. Analysis Scope. Safety and security issues, which cover the grids Ax and Bx ($x = 1$ and 4.1) in Figure 1, as well as UX, are concerned in this example. UX refers to a person's emotion and attitudes about using a particular system. Timing parameters and service quality are normally key factors influencing UX. The analysis is performed on the communication level, which means that nodes, links, and messages transmitted on networks are basic elements for the analysis. Software or hardware problems in a single ECU are out of scope.

4.2. TARA. System assets like ECU firmware, vehicle information, and authentication key (if any) are normally attack targets. An attack tree of an example attack target is presented in Figure 7.

The goal in this example is to attack DCU firmware, which contains three options (called attack objectives in the attack tree) for hackers. They can download malicious firmware to DCU, abort the update process, or steal firmware and perform reverse engineering. Several ways exist to achieve these objectives. For example, the hacker can get access into the communication channel and install malicious software on the DCU if no authentication mechanism exists in the system or the hacker provides a fake key to cheat the authentication mechanism. For each attack method, attack scenarios can be derived to describe possible attack behaviors by using this method. For example, the adversary needs to steal data on links and retrieve useful information

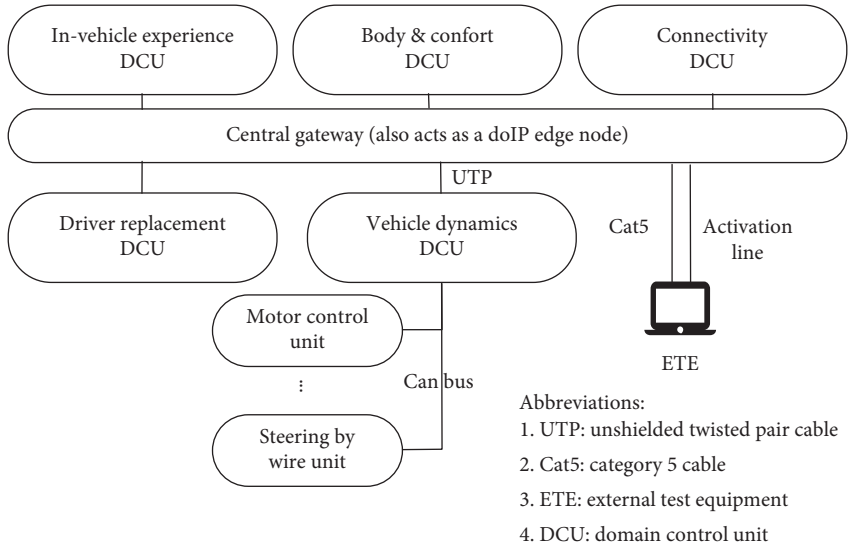


Figure 5: System architecture.

from the stolen data to achieve the "reverse engineering" objective by using "eavesdrop on links" method.

Based on the attack tree, the probabilities of attack scenarios can be evaluated according to principles in the EVITA approach. The scoring for each scenario in various aspects and the final probability values, which are categorized based on the scores, is shown in Figure 8 with class explanations. Note that all evaluated scores in this paper are based on common knowledge and the authors' experience.

After rating the severity of each attack objective, the risk assessment results shown in Table 6 are achieved.

During the risk assessment process, more parameters are identified as important ones and listed in Table 7. The new security parameters indicate attributes in three concrete aspects of information security. P_{Hazard} is introduced due to the possible occurrence of hazard events in attack objective 1, in which the vehicle dynamic functions may be modified and cause disasters when driving.

Finally, security goals (SGs) are listed in Table 8 based on attack objectives.

4.3. Security Concept

4.3.1. Possible Strategy Enumeration. For each attack, one or more proper mechanisms can be applied to prevent attacks. Table 9 shows the possible countermeasures against each attack to mitigate attack risks.

4.3.2. Affecting Analysis. The affecting map is shown in Figure 9 to indicate impacts of possible countermeasures on the system, in which green arrows represent a positive change while the white ones represent a negative change.

According to the arrows, there are conflicts in C1, C2, C3, and C7, in which the increase of security attributes results in the decrease of the communication performance. Whether to use a countermeasure depends on the system purposes that the designer prefers. If the designer aims to design an efficient system for updating ECU firmware, C3 and C7 may have low priority due to too much extra delay in transmission. Other protection efforts may be considered in technical or management aspects instead of those in communication process. If nodes in a system have enough computing ability and the target requires high safety level, like the DCU in the vehicle dynamics domain, C3 is supposed to be used to achieve the highest safety and security insurance with an acceptable downloading time interval. If the firmware software is a commercial secret with high confidentiality requirements, encryption countermeasures like C7 would be mandatory despite the delay in communications.

The analysis above is qualitative and suitable for quick decision with clear preference. Parameters can also be quantified by simulation or evaluation for various algorithms. Finally, the designer compares the assessment outcomes and determines a suitable strategy quantitatively.

4.3.3. Security Requirement. We assume that the DCU computing ability is on the average level, and the system owner cares the intellectual property and wants to achieve the security goal with minimum additional investment. Therefore, RLs in the privacy aspect should be reduced with the priority and RLs in other aspects should also be cut down as much as possible with lightweight countermeasures. C1 and C7 can be applied in this system to improve information authentication and confidentiality, while C3 is not considered in the first place because of too many delays. C4 may not be taken since it may require much investment in labor and money, and it can only be used to against attack 2.2.1, while C1 and C7 have positive impacts on multithreats. Requirements listed in Table 10 can be derived from the chosen countermeasures.

4.4. Preliminary Assessment. The system is assessed again to show the effects of the security strategy theoretically. The

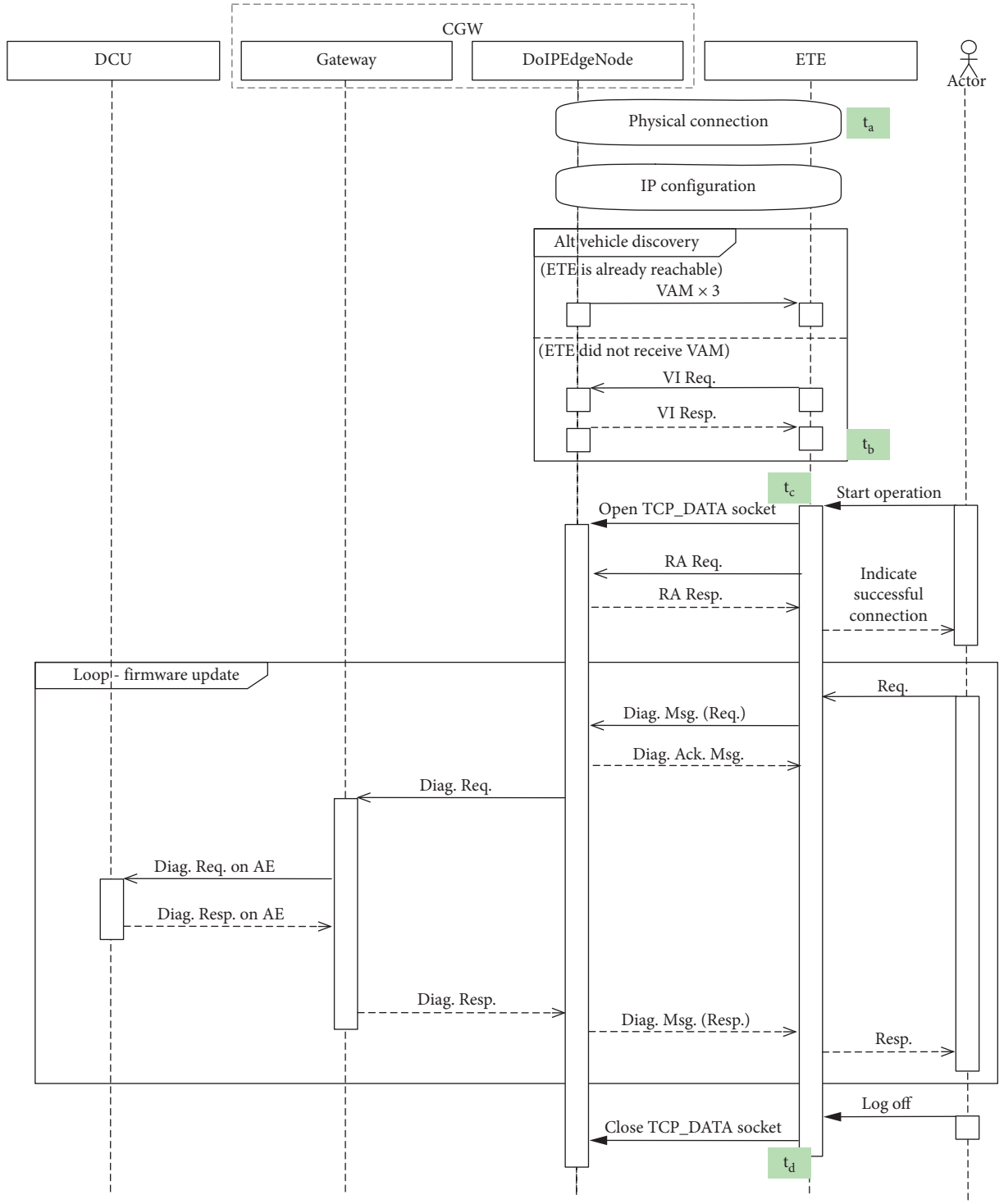


Figure 6: Sequence diagram of the use case on network layer.

reassessment scoring and the comparison results with or without countermeasures are shown in Figure 10. RS, RP, RF, and RO in the figure represent risk levels in safety, privacy, financial, and operational aspects.

According to the reassessment of the improved system, RLs have been reduced after applying C1 and C7. The UX and safety attributes are always in the mind during the design process. Countermeasures reduce the attack probability but add transmission delays due to the additional computing requirements. To achieve an acceptable system performance, delays should be limited in a suitable range by choosing proper authentication and encryption algorithms.

The reassessment result in this phase is an interim one and represents the current level of system security with trade-off considerations. During further development, more threats or security issues, along with the UX and safety

Table 5: Identified system parameters.

Group	Notation	Description
Communication	$T_{ConnEst}$	Equals $t_b - t_a$, time for the connection establishment
	T_{Update}	Equals $t_d - t_c$, time for the update, which is from the first request message to the last response message according to the firmware update protocol
Security	$N_{AttackPoint}$	Number of attack points
	S_{Attack}	Severity of attacks
	P_{Attack}	Probability of attacks
Safety	—	Since this is a nonsafety-critical system, no safety-related parameter is identified

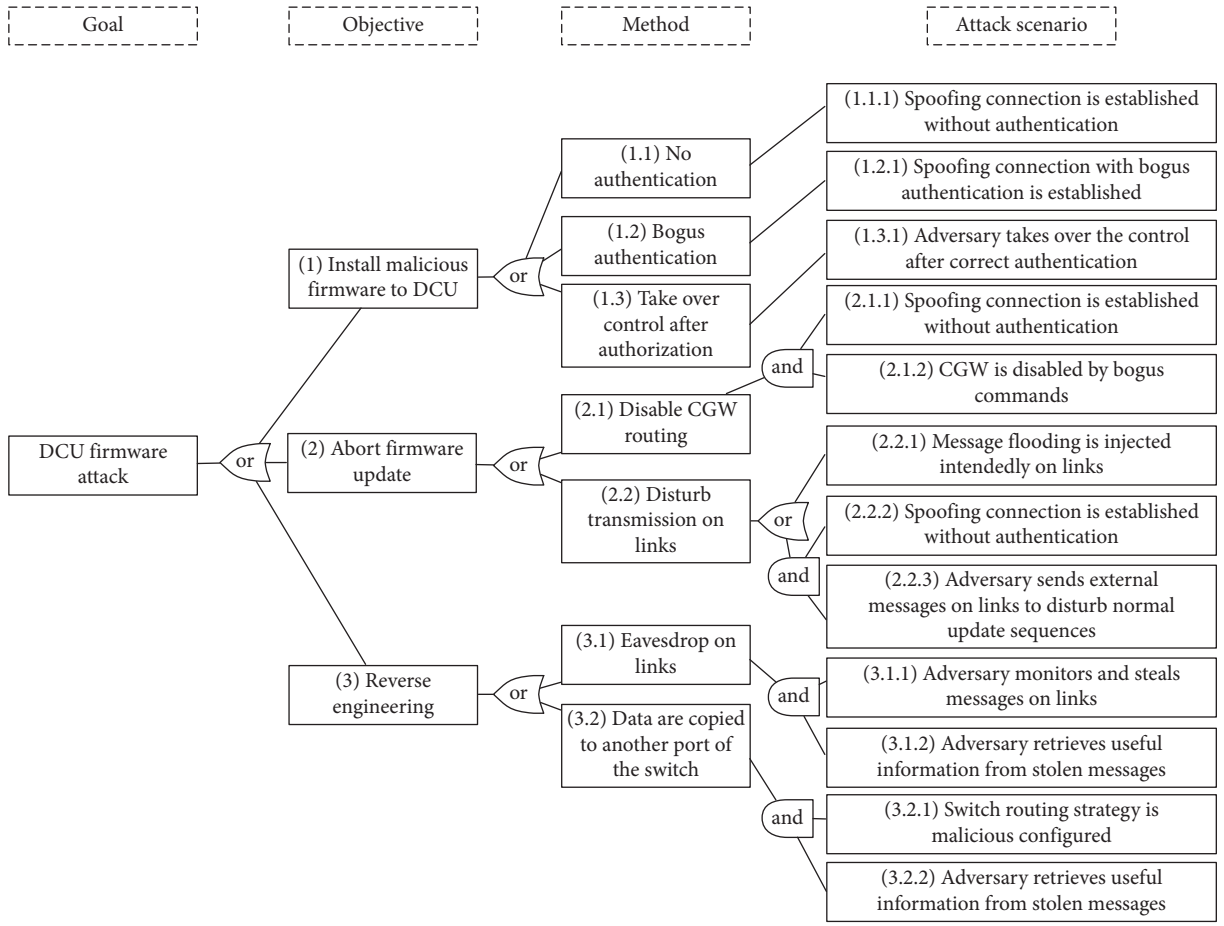


Figure 7: Attack tree of the example use case.

issues, maybe explored and affect the final system design. The trade-off idea should go through the whole lifecycle of the system.

5. Discussion

By using the proposed approach, trade-off requirements are achieved finally with systematic steps. Conflicts or reinforcements of different system attributes are revealed by association keys. The whole traceable analysis and the reducing risk levels in the reassessment show that the proposed approach is effective to improve preferred system attributes by considering the impacts on other aspects at the same time. There are three main merits of this approach. Firstly, system parameters are introduced as the association keys to reveal relationships between concerned attributes and countermeasures, which helps the designer understand interactions and control impacts on various aspects. Other design attributes, like financial cost and labor cost, can also be considered integrally by adding relevant parameters under this framework. Secondly, the steps in this approach are operable and unambiguous. With the demonstration of an example case, users can master the approach easily. Thirdly, the proposed framework is based on the J3061 process, which makes the designer easy to integrate the new approach into existing working systems.

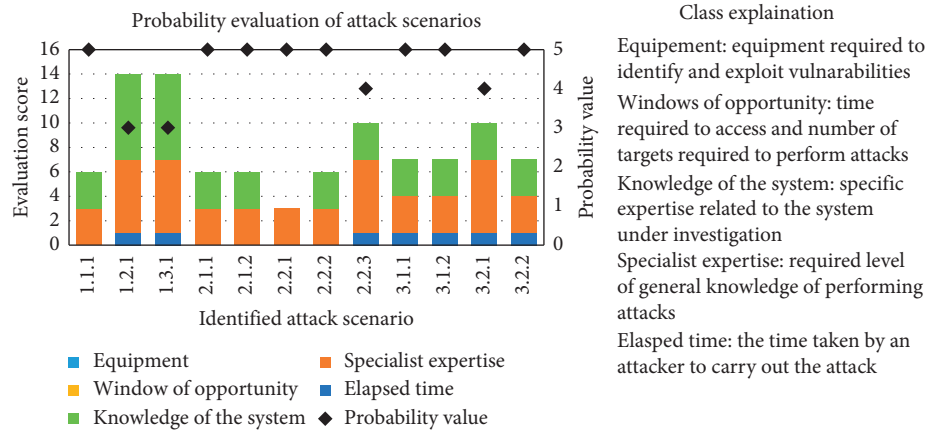


Figure 8: Probability evaluation of attack scenarios.

Table 6: Risk assessment results.

Attack objective	Severity	Attack method	RL	CAP	Attack scenario no.	AP
[1] Install malicious firmware to DCU	$S_S = 3$ $S_P = 0$ $S_F = 3$ $S_O = 0$	[1.1] No authentication	$R_S = R5$ $R_F = R5$	$P_{[1.1]} = P_{[1.1.1]} = 5$	[1.1.1]	5
		[1.2] Bogus authentication	$R_S = R3$ $R_F = R3$	$P_{[1.2]} = P_{[1.2.1]} = 3$	[1.2.1]	3
		[1.3] Take over control after authorization	$R_S = R3$ $R_F = R3$	$P_{[1.3]} = P_{[1.2.1]} = 3$	[1.3.1]	3
[2] Abort firmware update	$S_S = 0$ $S_P = 0$ $S_F = 2$ $S_O = 3$	[2.1] Disable CGW routing	$R_F = R4$ $R_O = R5$	$P_{[2.1]} = \min\{P_{[2.1.1]}, P_{[2.1.1]}\} = 5$	[2.1.1] and [2.1.2]	5 5
		[2.2] Disturb transmission on links	$R_F = R4$ $R_O = R5$	$P_{[2.2]} = \max\{ P_{[2.2.1]}, \min\{P_{[2.2.2]}, P_{[2.2.3]}\}\} = 5$	[2.2.1] [2.2.2] and [2.2.3]	5 5 4
[3] Reverse engineering	$S_S = 0$ $S_P = 3$ $S_F = 3$ $S_O = 0$	[3.1] Eavesdrop on link	$R_P = R5$ $R_F = R5$	$P_{[3.1]} = \min\{P_{[3.1.1]}, P_{[3.1.1]}\} = 5$	[3.1.1] and [3.1.2]	5 5
		[3.2] Copy data to another port of the switch	$R_P = R4$ $R_F = R4$	$P_{[3.2]} = \min\{P_{[3.2.1]}, P_{[3.2.2]}\} = 4$	[3.2.1] and [3.2.2]	4 5

Table 7: Newly added parameters.

Group	Notation	Description
Security	I_{Confi}	Information confidentiality
	I_{Authe}	Information authentication
	I_{Avail}	Information availability
Safety	P_{Hazard}	Probability of the occurrence of hazardous events

Table 8: Security goals.

Index	Security goal
SG_1	Avoid installing malicious firmware
SG_2	Avoid aborting firmware update
SG_3	Prevent the firmware from reverse engineering

On the other hand, some deficiencies exist yet in this research. Cases with quantitative assessments need to be performed to show the details of the careful decision path. Besides, more design cases using the proposed approach need to be analyzed and evaluated. Interviews can be conducted to get feedback from system designers who use this approach. Through various and practical cases and feedbacks, existing unknown weaknesses can be exploited and fixed to achieve a practical and widely applicable methodology.

This approach and the demonstrated example are a valuable start to solve the trade-off design issue. Works are going to be done to make up the mentioned deficiencies and achieve an optimized solution for balancing in different fields.

Table 9: Possible countermeasures of each asset attack.

Asset attack index	Possible countermeasures
[1.1.1]	[C1] Add authentication mechanisms when establishing connection
[1.2.1]	[C2] Enhance authentication mechanisms when establishing connection
[1.3.1]	[C3] Add authentication mechanisms in every diagnostic request and response
[2.1.1]	[C1] Add authentication mechanisms when establishing connection
[2.1.2]	[C8] Add authentication mechanisms when configuring switches
[2.2.1]	[C4] Add detecting and handling mechanisms of flooding attacks
[2.2.2]	[C1] Add authentication mechanisms when establishing connection
[2.2.3]	[C5] Add detecting and handling mechanisms of unexpected messages
[3.1.1]	[C6] Add detecting and handling mechanisms of illegal monitors
[3.1.2]	[C7] Encrypt messages
[3.2.1]	[C8] Add authentication mechanisms when configuring switches
[3.2.2]	[C7] Encrypt messages

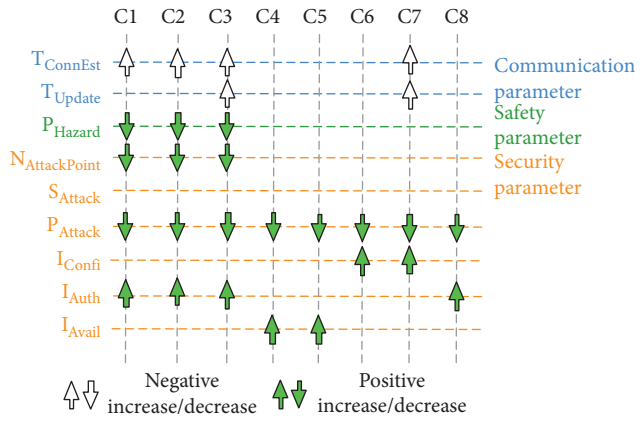


Figure 9: Affecting map.

Table 10: Example security requirements.

Requirement no.	Description
R1	Authentication mechanisms should be used during the connection establishment
R2	Encryption mechanisms which require average computing resources should be used when transmitting firmware data

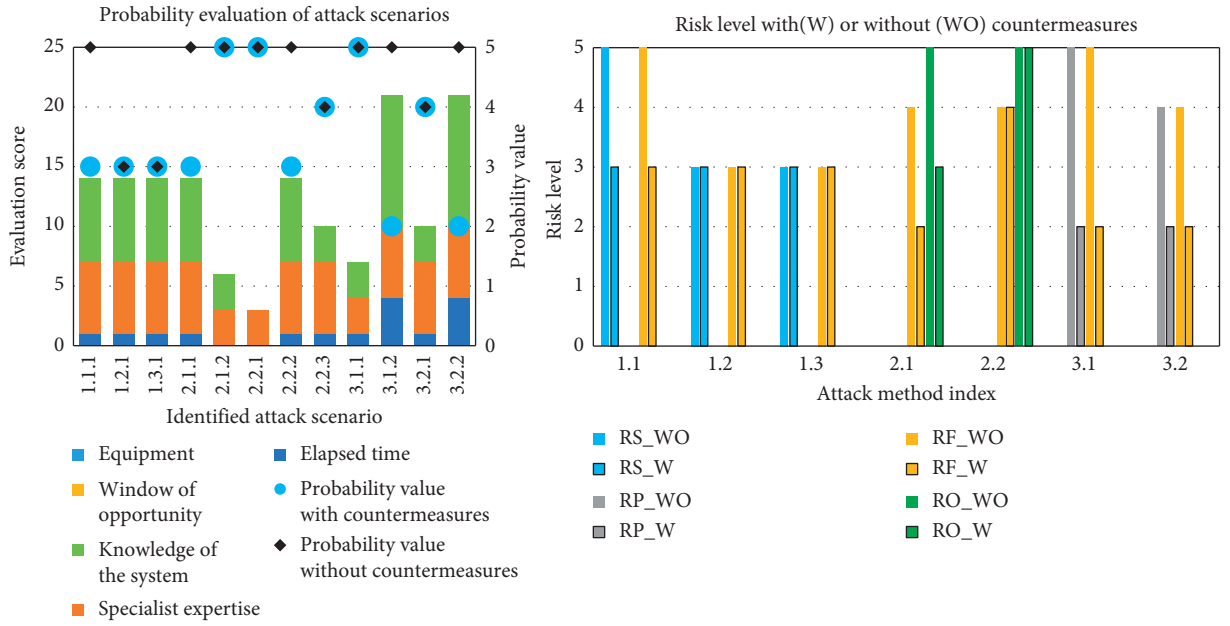


Figure 10: Reassessment scoring and comparison results with or without countermeasures.

6. Conclusion and Future Work

This paper proposed a systematic approach for cybersecurity design of in-vehicle systems. The aim of this is to balance system attributes in safety, cybersecurity, and UX in the concept design phase and find an optimized solution for possible conflicts systematically. The methodology is explained in Section 3 containing the working process, the TARA method, and association keys. An implementation of a DoIP system is reported in Section 4 with details. The example process shows that the proposed approach is operable and useful for identifying conflicts in different aspects and leading to a trade-off solution at the concept phase. This research increases our understanding of confusing concepts as well as their relationships and broadens the concerning scope of the co-design with safety, security, and UX. Other concerning attributes can also be integrated under this framework.

The increasing system complexity and interactions between the system and normal users make it important to ensure and balance expected system performance in various disciplines, in which conflicts may exist. One key benefit of the co-design is to discuss conflicts or reinforcements in different fields at the whole system level and propose balanced solutions systematically. Another benefit of the systematic co-design is to use a unified system model and terminology to conduct a holistic design. Elements in the design process (e.g., parameters and strategies) are synthesized and integrated no matter which fields they belong to, which makes the design process and outcomes traceable to original design inputs (e.g., goals and design requirements) even in different disciplines.

Nevertheless, further studies should be conducted to establish a comprehensive guideline for the trade-off design activity. More empirical cases should be performed with qualitative or quantitative evaluations by using this approach. Possible weaknesses would be exploited and fixed to improve the approach. Besides, how to solve conflicts is one of the core questions in a balanced design. More researches under varied situations should be carried out to find suitable strategies with technical details to solve conflicts and achieve the trade-off effectively and efficiently.

Data Availability

No additional data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Shanghai Science and Technology Commission Project (No. 18DZ1101300).

References

[1] International Standard Organization, *ISO 26262-3 Road Vehicles - Functional Safety - Part 3: Concept Phase*, International Standard Organization, Geneva, Switzerland, 2018.

[2] International Standard Organization, *ISO/PAS 21448: Road Vehicles - Safety of the Intended Functionality*, International Standard Organization, Geneva, Switzerland, 2019.

[3] International Electrotechnical Commission, *IEC 61882: Hazard and Operability Studies (HAZOP Studies) - Application Guide*, International Electrotechnical Commission, Geneva, Switzerland, 2016.

[4] M. Bouissou and J.-L. Bon, "A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes," *Reliability Engineering & System Safety*, vol. 82, no. 2, pp. 149–163, 2003.

[5] N. G. Leveson and J. P. Thomas, "STPA handbook," 2018.

[6] W. Wang, F. Huo, H. Tan, and H. Bubb, "A framework for function allocation in intelligent driver interface design for comfort and safety," *International Journal of Computational Intelligence Systems*, vol. 3, no. 5, pp. 531–541, 2010.

[7] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, vol. 57, no. 2, pp. 31–35, 2014.

[8] S. S. Borojeni, S. C. J. Boll, W. Heuten, H. H. Bülthoff, and L. Chuang, "Autonomous vehicles: human factors issues and future research," *Conference on Human Factors in Computing Systems*, vol. 2018, 13 pages, 2018.

[9] W. Biever, L. Angell, and S. Seaman, "Automated driving system collisions: early lessons," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 62, no. 2, pp. 249–259, 2020.

[10] Society of Automotive Engineers, *J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, Society of Automotive Engineers, PA, USA, 2016.

[11] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, "Using SAE J3061 for automotive security requirement engineering," in *Computer Safety, Reliability, and Security*, pp. 1–14, Springer, Berlin, Germany, 2016.

[12] Japanese Automotive Standard Organization, *Guideline for Automotive Information Security Analysis*, Society of Automotive Engineers of Japan (JSAE), Tokyo, Japan, 2016.

[13] Y. Kawanishi, H. Nishihara, D. Souma, and H. Yoshida, "Detailed analysis of security evaluation of automotive systems based on JASO TP15002," in *Computer Safety, Reliability, and Security*, pp. 211–224, Springer, Berlin, Germany, 2017.

[14] Y. Kawanishi, H. Nishihara, D. Souma, H. Yoshida, and Y. Hata, "A comparative study of JASO TP15002-based security risk assessment methods for connected vehicle system design," *Security and Communication Networks*, vol. 2019, Article ID 4614721, 35 pages, 2019.

[15] EVITA, *D2.3 Security Requirements for Automotive On-Board Networks Based on Dark-Side Scenarios*, EVITA, Campitello di Fassa, Italy, 2009.

[16] International Standard Organization and International Electrotechnical Commission, *ISO/IEC 15408 - 1: Information Technology - Security Techniques - Evaluation Criteria for IT Security*, International Standard Organization and International Electrotechnical Commission, Geneva, Switzerland, 2014.

[17] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.

[18] A. Fiaschetti, V. Suraci, and F. D. Priscoli, "The SHIELD framework: how to control security, privacy and dependability in complex systems," in *Proceedings of the 2012 Complexity in Engineering (COMPENG)*, Aachen, Germany, June 2012.

[19] U.S. National Highway Traffic Safety Administration, Characterization of Potential Security Threats in Modern Automobiles -A Composite Modeling Approach, U.S. National Highway Traffic Safety Administration, Washington, DC, USA, 2014.
[20] B. Sapiro, "Binary risk analysis," May 2011.
[21] National Institute of Standards and Technology, *SP 800-30: Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2012.
[22] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "A review of threat analysis and risk assessment methods in the automotive context," in *Computer Safety, Reliability, and Security*, pp. 1–12, Springer, Berlin, Germany, 2016.
[23] International Standard Organization and ISO, International Standard Organization and ISO, *ISO 26262-2 Road Vehicles - Functional Safety - Part 2: Management of Functional Safety*, Geneva, Switzerland, 2018.
[24] G. Macher, R. Messnarz, E. Armengaud, A. Riel, E. Brenner, and C. Kreiner, *Integrated Safety and Security Development in the Automotive Domain*, pp. 2011–2017, SAE World Congress Experience, Detroit, MI, USA, 2017.
[25] T. Amorim, H. Martin, Z. Ma et al., "Systematic pattern approach for safety and security Co-engineering in the automotive domain," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 329–342, 2017.
[26] D. Pereira, C. Hirata, R. Pagliares, and S. Nadjm-Tehrani, "Towards combined safety and security constraints analysis," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 70–80, 2017.
[27] Automotive SIG, "Automotive SPICE process reference model/process assessment model," 2017.
[28] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure Mode and effect analysis (FMEA)," in *Proceedings of the International Conference on Computer Safety, Reliability, and Security*, pp. 1–16, Delft, The Netherlands, September 2014.
[29] C. Raspotnig, P. Karpati, and V. Katta, "A combined process for elicitation and analysis of safety and security requirements," *Business-Process and Information Systems Modeling*, pp. 1–15, Springer, Berlin, Germany, 2012.
[30] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: a security-aware hazard and risk analysis method," in *Proceedings of the Design, Automation Test in Europe Conference Exhibition*, pp. 1–4, Grenoble, France, March 2015.
[31] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: safety and security analysis for cyber-physical systems," *Journal of Information Security and Applications*, vol. 34, pp. 183–196, 2017.
[32] L. Pietre-Cambacedes and M. Bouissou, "Modeling safety and security interdependencies with BDMP (boolean logic driven Markov processes)," in *Proceedings of the 2010 IEEE International Conference on Systems, Man and Cybernetics*, pp. 2852–2861, Istanbul, Turkey, October 2010.
[33] C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber, "A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive cyber-physical systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, pp. 69–80, Xi'an, China, 2015.
[34] L. C. Wei, "A system theoretic approach to cybersecurity risks analysis of passenger autonomous vehicles," 2018.
[35] J. W. Sender and N. P. Moray, *Human Error: Cause, Prediction, and Reduction*, Lawrence Erlbaum Associates, NJ, USA, 1991.
[36] International Standard Organization, *ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*, International Standard Organization, Geneva, Switzerland, 2009.
[37] International Standard Organization, *ISO 26262-1 Road Vehicles - Functional Safety - Part 1*, International Standard Organization, Geneva, Switzerland, 2018.
[38] A. Abdulkhaleq, D. Lammering, S. Wagner et al., "A systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles," *Procedia Engineering*, vol. 179, pp. 41–51, 2017.
[39] International Standard Organization, *ISO 26262-9 Road Vehicles - Functional Safety - Part 9: Automotive Safety Integrity Level(ASIL)-oriented and Safety-Oriented Analyses*, International Standard Organization, Geneva, Switzerland, 2018.