IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 January 2023, accepted 10 February 2023, date of publication 21 February 2023, date of current version 24 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3246497

APPLIED RESEARCH

A Study on Threat Analysis and Risk Assessment Based on the "Asset Container" Method and CWSS

YASUYUKI KAWANISHI [1,2,3], **HIDEAKI NISHIHARA** [2], **HIROTAKA YOSHIDA** [2], **HIDEKI YAMAMOTO** [1,2], **AND HIROYUKI INOUE** [2,3]

[1]Cyber-Security Research and Development Office, Research and Development Unit, Sumitomo Electric Industries Ltd., Osaka 554-0024, Japan
[2]SEI-AIST Cyber Security Cooperative Research Laboratory, Cyber Physical Security Research Center, National Institute of Advanced Industrial Science and Technology (AIST), Osaka 563-8577, Japan
[3]Division of Frontier Informatics, Kyoto Sangyo University, Kyoto 603-8555, Japan

Corresponding author: Yasuyuki Kawanishi (kawanishi-yasuyuki@sei.co.jp)

ABSTRACT In recent years, legislation and standardization of cyber security management for cyber-physical systems such as automotive systems have been progressing steadily. ISO/SAE 21434, published in 2021, addresses the management and analysis of electrical systems within road vehicles from a cybersecurity perspective. It also recommends some methods for the threat analysis and risk assessment (TARA) process. However, there are two problems in the evaluation methods derived from conventional security analysis approaches. One problem is related to the insufficient evaluation of attack feasibilities for cyber-physical systems by the CVSS-based approach. Another problem is the unclear relationship between damage factors in analyzing the impact of damage to each asset. In this paper, we focus on the TARA process, and apply an "asset container" method for threat classification, proposed by the authors at DECSoS 2017, and a CWSS-based risk quantification method. Moreover, we can also add some perspective to improve risk evaluation suitable for automotive systems. Following our past studies on methodologies to evaluate the risk of such special cyber-physical systems, we can quantify risks limited to some cyber-physical systems, such as direct access attacks to in-vehicle networks.

INDEX TERMS In-vehicle security, security design, risk analysis, TARA, ISO/SAE 21434, CWSS.

I. INTRODUCTION

A connected vehicle is one of safety-critical systems whose failure or malfunction may harm road users or damage their environment. As a result of the recent implementation of information and communication technology (ICT), a connected vehicle is also a cyber-physical system that integrates ICT systems and field devices which control actuators and sensors in the physical world. Therefore, it has become necessary to consider risks where cyberattacks on them may bring physical harm to the real world.

To deal with such new risks concerning not only safety but also security, legislation and standardization are urgent. Formulation of such legislation is underway at the United Nations world forum for harmonization of vehicle regulations Working Party 29 (WP.29), for example UN-R155 [1]. The 11 major manufacturing companies involved in the automobile field also released a framework for the development, testing and validation of safe automated vehicles in 2019 [2]. In 2020, ENISA released a report which defined good practice for security of smart cars in the same year [3], and the US Department of Transportation published "Automated Vehicles 4.0" [4] as a new guideline for automated cars.

The movement to incorporate security requirements from the design stage is called "security by design" and has already begun. The Common Criteria (CC) -based [5] cyber security certification scheme (EUCC) [6] has been promoted mainly in the EU, and a draft was released in 2021. In 2019, Maliatsos et al. also proposed selecting security requirements for connected vehicles in CC [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Engang Tian.

ISO/SAE 21434 [8] was published in 2021 under such circumstances. It is an international standard which provides vocabulary, objectives, requirements and guidelines related to cybersecurity management for automobiles. The threat analysis and risk assessment (TARA) process in ISO/SAE 21434 is a series of processes for model-based threat and risk analysis of automotive systems. In this standard, some approaches are recommended to evaluate attack feasibility and impact of each cyber security threat. In particular, a CVSS-based [9] approach and an attack vector-based approach are recommended for an attack feasibility rating (while an attack potential-based [10] approach is also mentioned, it is out of the scope of this paper).

However, we found two problems when focusing on these recommended approaches in the TARA process. One problem is related to the two approaches recommended for the attack feasibility rating mentioned above. They are too simple to interpret complicated logical and physical structures of cyber-physical systems and their environments. The other problem is related to the evaluation approach recommended for impact rating. It evaluates the risks of assets by four factors (safety, financial, operational, and privacy), but the relationships among the four factors are unclear. Classifying the magnitude of impact by only one factor is too inexact, and an appropriate compound formula to calculate the impact by multiple factors is undefined.

Regarding risk quantification analysis, methods using CVSS in calculation formulas have been proposed before, such as JASO TP15002 [11] and Ando's previous research [12]. Based on guideline TP15002, the authors have also reported their research on the application of various calculation formulas to quantify risks in cyber-physical systems such as automobile systems [13], [14], [15], which finally led them to come up with CWSS (Common Weakness Scoring System) [16], [17] as a suitable method for risk quantification of cyber-physical systems [18].

In this paper, we apply two ideas to implement the TARA process more practically and efficiently. One idea is an ''asset container'' method [13] which is an easy-to-describe method for identifying attack vectors in an attack feasibility rating. This method is also suitable for risk quantification methods such as CVSS and CWSS, because we can analyze attack paths using only the information that the victim has.

The other perspective is a risk scoring system (RSS) focused on CWSS, RSS-CWSS_CPS [15], [18]. CWSS has many similar metrics in common with CVSS suitable for an ''asset container'' method, some of which may affect evaluation more finely than CVSS. For example, appendix A in [17] shows that the metric related to attack complexity is only AC in CVSS, but IC, EC, etc. can be added to the evaluation in addition to AC in CWSS. This feature of CWSS appears to provide an accurate perception of the attack feasibility rating in TARA. Moreover, CWSS also has a metric BI for financial risk in its impact rating. In the impact rating in TARA, a financial criterion is added in addition to the conventional criteria of safety, operational and privacy, and CWSS also seems to be suitable for an impact rating approach.

Our methodology can actually contribute to the efficiency of the TARA process and solve the two problems mentioned above. For verification, we conducted a case study of the risk analysis on a connected vehicle to verify our contributions. In order to compare our new method with the conventional CVSS-based approach, we cited a recent attack referred to as ''CAN invader'' [19], and confirmed that our method could detect this attack, which could not be detected by the conventional method.

The remainder of this paper is structured as follows. In Section II, we introduce preliminary work related to this paper. In Section III, we identify the problems in previous works and then we propose our method for the TARA process. In Section IV, we conduct a case study on automotive systems and address our new method. In Section V, we explain the merits and findings seen in the case study results. In Section VI, we raise issues for future study. Finally, in Section VII, we present our conclusion.

II. PRELIMINARY

A. TARA PROCESS IN ISO/SAE 21434

FIGURE 1 shows a block diagram of the TARA defined in Clause 15 of ISO/SAE 21434. In this Clause, the following two processes are defined:

- **Process to identify a damage scenario:** A damage scenario is defined as ''an adverse consequence involving a vehicle or vehicle function and affecting a road user.'' It determines the impact (severity of damage) of threat-damaged assets on humans.
- **Process to identify a threat scenario:** A threat scenario is defined as ''a potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario.'' It determines the attack feasibility of exploiting assets concerning security.

By combining these two scenarios, the risks of threats to the system are calculated. Based on this idea, security analysis methods for IT systems are successfully applied to cyber-physical systems and their SFOP attributes.

B. ATTACK FEASIBILITY RATINGS IN TARA PROCESS

The following three approaches are recommended to evaluate attack feasibility of each threat scenario:

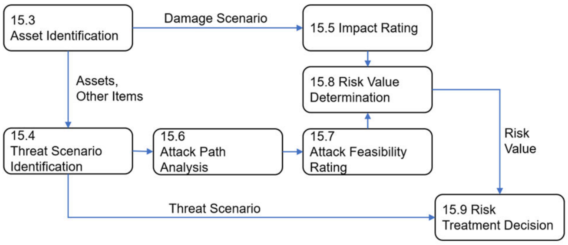

FIGURE 1. Block diagram of TARA [8].

(i) **Attack potential-based approach:** It is a method based on ISO/IEC 18045 (CEM) [10] which analyzes attack feasibility from the attacker's point of view such as their knowledge and equipment.
NOTE: This approach is out of the scope of this paper because we focus on the network structure of the target of evaluation (TOE) to analyze attack feasibility. This is another useful approach based around the TOE.

(ii) **CVSS-based approach:** It is a method based on the Common Vulnerability Scoring System (CVSS) [9]. Compared with method (i), it performs risk evaluation from the information that the attack victim may have. Ando et al. also proposed CVSS version 3.0 (older version of [9]) for their threat analysis of automotive systems.

(iii) **Attack vector-based approach:** It is a simpler approach than method (ii) that classifies attack feasibility only by the type of entry point.

C. IMPACT RATINGS IN TARA PROCESS

The four attributes of impact are considered as safety, financial, operational and privacy (SFOP attributes), but each of them is inexactly classified in only four ranks, "Severe," "Major," "Moderate" and " Negligible," and the relationship between these attributes is unclear.

D. PROBLEMS WITH TARA RATINGS

The TARA ratings have the following problems:

A) Methods (ii) and (iii) for attack feasibility rating tends to favor attacks over a network. However, in reality, attacks that are not over a network, such as direct access attacks to vehicles, are sometimes carried out.

B) Details of the method for impact rating are unclear and too inexact to classify the magnitude of damage. In the case of vehicles, we think that the financial issue is closely related to other factors.

Problem B includes the issue that it was unclear which attributes among the SFOP attributes are weighted. Regarding the relationship between SFOP attributes, safety and financial attributes are weighted significantly for the impact assessments in the HEAVENS security model [20]. Püllen et al. also evaluated the impact value with three attributes, Passenger Safety (PS), Operational Limitation (OL) and Financial Loss (FL), which are weighted so that PS takes a relatively larger value based on the so-called Value of a Statistical Life (VSL) [21], [22]. However, we will take an approach based on another perspective. Problem B includes another issue where there is a tendency to overestimate in the evaluation because of a fear of risk. This leads to biasing the distribution of impact values. This is due to a type of cognitive bias called "prospect theory," which is mentioned in [23]. These issues regarding Problem B will be confirmed in Subsection V-B with the data of a case study from Section IV.

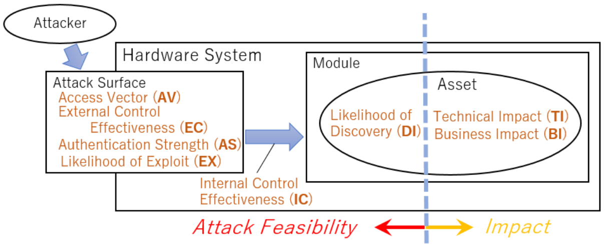
Attacker
Hardware System
Attack Surface
Access Vector (AV)
External Control Effectiveness (EC)
Authentication Strength (AS)
Likelihood of Exploit (EX)
Module
Asset
Likelihood of Discovery (DI)
Technical Impact (TI)
Business Impact (BI)
Internal Control Effectiveness (IC)
Attack Feasibility
Impact

FIGURE 2. RSS-CWSS_CPS metrics and "asset container" method [15] [18].

III. OUR APPROACH: TARA PROCESS BASED ON THE "ASSET CONTAINER" METHOD AND CWSS QUANTIFICATION

To solve these problems, we promote the following approaches, the "asset container" method and RSS-CWSS_CPS. The former is an approach to evaluate risk from the attack victim's point of view only, the latter is an approach to quantify risk more flexibly using multiple factors.

A. "ASSET CONTAINER" METHOD

The idea of the "asset container" method is to extract threats comprehensively as proposed in [13] and [14]. This idea is a technique for organizing threat scenarios in terms of assets and means of attack. We use this idea to identify and prioritize significant risks rapidly. The threat scenario is analyzed from the following three perspectives, "Where," "At" and "Asset," where "At" and "Asset" are decomposed perspectives of "What."

These three perspectives are only based on information from the attack victim's point of view, and it is possible to cover all threat scenarios without overlooking unexpected threats and prioritizing scrutiny of significant threats. This idea is based on the interpretation that a threat is perceived as an action where "an attacker tries to harm an asset by reaching into the container of the asset" shown in FIGURE 2.

B. RSS-CWSS_CPS AS RISK QUANTIFICATION METHOD

The vulnerability scoring system is originally used for evaluation of vulnerabilities of products released to the market. CVSS and CWSS are examples of this, and we use them as risk quantification methods in the security design phase. It is a method which uses a formula consisting of several metrics. Each metric has several ranks corresponding to the severity of risk, and each rank is assigned a numerical value so that the higher the risk, the higher the value. All the numerical values of the metrics are substituted into the formula, and finally the magnitude of the risk is obtained numerically.

ISO/SAE 21434 provides some guidelines on how the following approaches can be applied to attack feasibility analysis in Annex G. For example, the CVSS-based approach shows that the overall exploitability value of attack feasibility E is calculated by the following formula:

$$E = 8.22 \times V \times C \times P \times U \tag{1}$$

where V is metric AV (Attack Vector)
C is metric AC (Attack Complexity)
P is metric PR (Privileges Required)
U is metric UI (User Interaction) in CVSS [9]

Each metric has several ranks, and each rank is a category which expresses a characteristic of the metric. For example, V is a metric concerning attack vector, and four categories, "Network," "Adjacent," "Local" and "Physical," which express communication characteristics categorized by communication distances.

Each rank is also assigned a numerical value that quantifies a severity of the risk concerning the metric. For example, the rank "Network" is assigned 0.85 which is the highest value among the four ranks. When these numerical values are substituted in formula (1), the value of attack feasibility E is obtained.

We proposed a risk quantification method, RSS-CWSS_CPS [15], [18], which is based on CWSS [16], [17]. This method quantifies a risk value Rw that includes both attack feasibility ratings and impact ratings with the following formula:

$$\mathrm{Rw} = \mathrm{SBase} \times \mathrm{SSurface} \times \mathrm{SEnv}/10.0 \qquad (2)$$

where $f(x) = 0$ (if $x = 0$), 1 (otherwise)

$\mathrm{SBase} = 4\,\{f(\mathrm{TI}) \times (10\mathrm{TI} + 15) \times \mathrm{IC}\}$

$\mathrm{SSurface} = \{20\,(\mathrm{AV} + 2) + 5\mathrm{AS} + 35\}\,/\,100.0$

$\mathrm{SEnv} = \{f(\mathrm{BI}) \times (10\mathrm{BI} + 3\mathrm{DI} + 4\mathrm{EX} + 3) \times \mathrm{EC}\}\,/\,20.0$

In this formula, TI, IC, AV, AS, BI, DI, EX and EC are the metrics defined in CWSS (see concepts in TABLE 1), each of them having various ranks and each rank being assigned a value so that the larger the value, the more risk there is from each perspective. All the numerical values of the metrics are substituted into the formula, and finally Rw representing the magnitude of the risk is obtained numerically.

TABLE 1. CWSS metrics (excepted) [16] [17].

Metric	Concept
Technical impact (TI)	Potential result that can be produced by the weakness.
Internal control effectiveness (IC)	The ability of the control to render the weakness unable to be exploited by an attacker.
Access vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.
Authentication strength (AS)	The strength of the authentication routine.
Business impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.
Likelihood of discovery (DI)	The likelihood that an attacker can discover the weakness.
Likelihood of exploit (EX)	The likelihood that an attacker would be able to successfully exploit it.
External control effectiveness (EC)	The capability of mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.

TABLE 2. CWSS metrics for TARA.

CWSS Metric	Belongs to	Used for What in TARA
TI	"Asset"	Impact Rating (damage scenario)
BI		
DI		
AV	"Where"	Attack Feasibility Rating (attack path)
AS		
EX		
EC		
IC	"Where" & "At"	

CWSS is a vulnerability criteria for software systems, so the following two metrics are redefined to apply to the hardware structure of the cyber-physical system:

- **Internal control effectiveness (IC):** It is originally defined as "the ability of the control to render the weakness unable to be exploited by an attacker," we implemented it as "a physical or logical structure that induces difficulty in attacking," for example, an attack path which needs to exploit multiple modules on its way to reach the target module.
- **External control effectiveness (EC):** It is originally defined as "the capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger." We implemented it as "the physical characteristics of the entry point that make it difficult to access," for example, the entry point where some authentication or some complex work is required for access.

We applied a combination of the "asset container" method and RSS-CWSS_CPS to the TARA process. TABLE 2 shows the relationship between CWSS metrics, the "asset container" perspective, and the TARA ratings.

C. HOW TO USE OUR METHODS FOR TARA PROCESS

Our methods help to efficiently organize threats into a risk quantification formula, and can be applied to the TARA process without any modification as well as other existing informative approaches. Below, we describe how to implement our methods for each process, following the block diagram in FIGURE 1.

- **15.3 Asset identification:** We consider damage scenarios in which road users are harmed. This is the same procedure as other approaches in ISO/SAE 21434.
- **15.4 Threat scenario identification:** We identify threat scenarios as the combinations of "Where," "At" and "Asset" that classify attack targets and attack routes based on the "asset container" method described in Subsection III-A.
- **15.5 Impact Rating:** The ranks and values of metrics TI and BI (see TABLE 1) are determined for each asset based on the damage scenarios. They can also be assigned based on SFOP attributes in Annex F of ISO/SAE 21434.

- **15.6 Attack Path Analysis:** All attack paths are determined by exhaustive analysis of “Where,” “At” and “Asset” perspectives.
- **15.7 Attack Feasibility Rating:** The ranks and values of metrics IC, AV, AS, EX, EC and DI are assigned from “Where,” “At” and “Asset” perspectives (see also FIGURE 2). This is a process similar to method (ii), the CVSS-based approach.
- **15.8 Risk Value Determination:** The risk value Rw of each threat scenario is calculated by the formula in (2).

D. MERITS FOR USE OF THIS METHODOLOGY

The merits of using these methods are as follows:

- It is possible to interpret the network structure of TOE in a more complex manner than a CVSS-based approach, and attacks over the network no longer always have an advantage (details will be mentioned in Subsection V-A).
- A more detailed impact rating can be achieved by guaranteeing the valuation of assets in multiple metrics TI and BI using CWSS as a proven method. Business impacts (BI) as financial attributes are often closely linked to technical impacts, so it is possible to quantify the asset more realistically than selecting only one perspective between safety, financial, operational or privacy (details will be explained in Subsection V-B).

IV. CASE STUDY

In this section, we consider an architecture example of a connected vehicle as a TOE. FIGURE 3 is a typical network structure of the TOE as shown in [24]. In the figure, functional modules for infotainment, telematics, and an ITS control console are connected via Ethernet network, and functional modules belonging to the control system of the power train (PT), body, chassis, advanced driver assistance system (ADAS), and immobilizer are connected via CAN bus network. A CGW (Central Gateway) also supports both networks. We apply the proposed TARA process to it.

***NOTE:** In this case study, values are used instead of ranks for each metric to make the risk comparison easier to understand.*

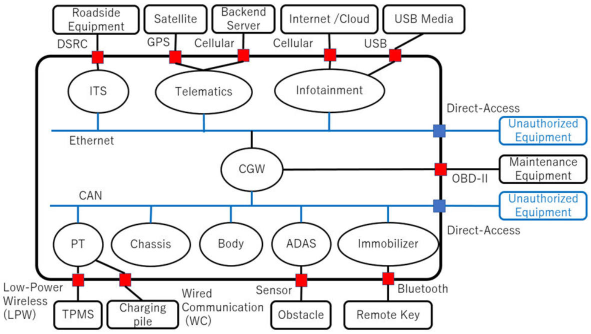

FIGURE 3. An example architecture of a connected vehicle.

A. DEFINITION OF NETWORK STRUCTURE

The following modules are connected internally by Ethernet network or CAN bus:

- **PT:** Modules for power train and control.
- **Chassis:** Modules for brake and steering.
- **Body:** Modules for door, air-conditioner, etc.
- **ADAS:** Modules for driving support.
- **Immobilizer:** Modules for engine ignition.
- **CGW:** Protocol converter.
- **ITS:** Modules for V2X communication.
- **Telematics:** Modules for remote communications.
- **Infotainment:** Modules for information and entertainment.

The entry points (communication interfaces) of the TOE are as follows:

- **Cellular:** Long-distance communication interface used for application updates, internet connection, etc.
- **GPS:** Long-distance communication interface with GPS satellites.
- **DSRC:** Adjacent communication interface for road-to-vehicle and vehicle-to-vehicle communication.
- **Bluetooth:** Adjacent communication interface.
- **LPW(Low Power Wireless):** Adjacent communication interface between TPMS and vehicle.
- **USB:** Physical interface such as USB, SD card, etc.
- **WC (Wired Communication):** Wired communication interface for charging pile
- **Sensor:** Sensor used for distance measurement.
- **OBD-II:** Wired interface used for vehicle diagnosis
- **DA(Direct-Access):** Abused interface used for attacks, such as connecting an unauthorized device to vehicle’s internal communication line.

B. ASSET IDENTIFICATION AND IMPACT RATING

First, we define assets in the automotive system, consider damage scenarios respectively, and decide the rank value of each metric (TI and BI), and the SFOP attributes. TABLE 3 shows some examples of the definitions. It also shows that the attributes of each damage scenario seem to be a set of a financial attribute and one other attribute.

For example, the “control function of PT module” asset is evaluated as “both TI and BI are set to 1.0 as a critical threat because the malfunction of the asset compromises the safety of road users.”

TABLE 3. Mapping of TI, BI and SFOP attributes (excepted).

“At”	“Asset”	TI	BI	SFOP Attributes of Damage Scenario
PT	Control Function	1.0	1.0	Safety, Financial
Telematics	Ex-Comm. Function	0.9	0.9	Operational, Financial
Immobilizer	Auth. Information	0.9	0.9	Privacy, Financial
Infotainment	In-Comm. Function	0.6	0.3	Operational, Financial
ITS	Auth. Function	0.6	0.9	Operational, Financial

We consider that an automotive system is a cyber-physical system that has an impact on not only the environment, but also the owner or user of the product, and as such, the financial aspect among SFOP attributes should be evaluated separately. CWSS is suitable for the evaluation of automobile assets. In CWSS, the metric TI evaluates the aspects of safety, operational, and privacy, and the metric BI classifies the financial aspect.

C. THREAT SCENARIO IDENTIFICATION

Next, we define the threat scenarios which determine how an attacker reaches the assets. We apply the "asset container" method, and describe their attack routes by a combination of the perspectives, "Where," "At" and "Asset." TABLE 4 shows some examples of the combinations. At this stage we describe all combinations of these perspectives. For example, threat #1 means "a threat scenario of intrusion from the DSRC interface and attack on the control function of the PT module."

D. ATTACK PATH ANALYSIS AND ATTACK FEASIBILITY RATING

Next, the ranks of the CWSS metrics are added to each threat scenario. Each of the six metrics are defined in TABLE 1 and Subsection III-B, TABLE 5 shows some examples. Whereas CVSS uses 4 metrics for calculating attack feasibility.

RSS-CWSS_CPS uses 6 metrics and can also set rank values more exactly. It is possible to think more concretely about the interpretation of attack paths and clearly distinguish the attack feasibility for each route.

For example, threat #1 "a threat scenario of intrusion from the DSRC interface of the ITS module and attack on the control function of the PT module via the ITS module and CGW" is evaluated as:

- It is difficult to attack the PT module via multiple modules (IC=0.5)
- DSRC is adjacent communication and thus shorter than network communication (AV=0.7)
- Authentication is necessary to access the ITS module (AS=0.8)
- It is necessary to disguise the source when making DSRC communication such as camouflaging the roadside unit (EX=0.6)
- Certain countermeasures are considered for the DSRC communication interface (EC=0.9)
- It is hard to find features that differ from the interface the attacker is accessing (DI=0.6)

In this way, the rank of each metric is determined so that the #1 threat can be judged to be of relatively low risk. However, the impact rating and the attack feasibility rating cannot be quantified individually, so the risk values are determined in the next subsection.

E. RISK VALUE DETERMINATION AND CONSIDERATION

Finally, the eight CWSS metrics are decided, and the risk value Rw is calculated by formula (2) based on RSS-CWSS_CPS. TABLE 6 shows the excerpt list of threat scenarios and their risk values. In addition to attacks via networks such as the cellular network, an attack via direct-access (DA) also ranks highly in threatening attacks.

Attacks via DA are considered to be an old method, and they have not received much attention as a method of cybersecurity attack. However, as in the example of the "CAN invader," which is a recent case where some car theft groups in Japan [19] accessed a communication line connecting an important ECU, they are likely to be more effective attack paths for automotive systems. We can rent a vehicle through regular services such as car sharing and rental car agencies, and it is easy to access the in-vehicle network by pretending to do maintenance.

TABLE 4. List of threat scenarios (excepted).

#	Simplified Threat Scenario		
	"Where"	"At"	"Asset"
1	DSRC	PT	Control Function
101	GPS	Telematics	Ex-Comm. Function
201	Bluetooth	Immobilizer	Auth. Information
301	DA	Infotainment	In-Comm. Function
401	WC	ITS	Auth. Function

TABLE 5. List of attack feasibility (excepted).

#	CWSS Metrics for Attack Feasibility					
	IC	AV	AS	EX	EC	DI
1	0.5	0.7	0.8	0.6	0.9	0.6
101	1.0	1.0	1.0	1.0	0.9	1.0
201	0.9	0.7	0.8	0.2	0.9	1.0
301	0.9	0.5	1.0	1.0	1.0	0.6
401	0.5	0.2	1.0	0.2	0.9	1.0

TABLE 6. List of threats and risk values(excepted).

#	Rank	"Where"	CWSS Metrics for RSS-CWSS_CPS								Rw
			Attack Feasibility						Impact		
			IC	AV	AS	EX	EC	DI	TI	BI	
269	1	DA	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.00
101	7	GPS	1.0	1.0	1.0	1.0	0.9	1.0	0.9	0.9	8.46
63	16	Cellular	1.0	1.0	0.8	1.0	0.9	1.0	0.9	0.9	8.13
322	26	OBD-II	1.0	0.5	1.0	1.0	0.9	1.0	0.9	0.9	7.39
345	51	LPW	1.0	0.7	1.0	0.2	0.9	1.0	1.0	1.0	7.11
20	53	DSRC	1.0	0.7	0.8	0.6	0.9	1.0	0.9	0.9	6.99
421	62	Sensor	0.9	0.5	1.0	0.6	0.9	1.0	1.0	1.0	6.71
383	90	WC	1.0	0.2	1.0	0.2	0.9	1.0	1.0	1.0	6.35
193	91	Bluetooth	0.9	0.7	0.8	0.2	0.9	1.0	1.0	1.0	6.33
170	142	USB	0.9	0.2	1.0	0.6	0.9	1.0	0.9	0.9	5.68
…	…	…	…	…	…	…	…	…	…	…	…
1	297	DSRC	0.5	0.7	0.8	0.6	0.9	0.6	1.0	1.0	3.60

RSS-CWSS_CPS make it possible to interpret their characteristics that cannot be expressed by conventional methods using metrics such as IC and EC. We believe that the proposed method matches the actual demand.

As a side note, threat #1 has a risk value of 3.60, which is ranked as a low risk at 297th. This is likely due to the low values of metrics that determine attack feasibility, despite the high value of the assets, TI and BI. Threat #20 is also a threat from DSRC communication the same as threat #1, but it is a riskier threat (DI=1.0, IC=1.0) because it doesn't require a springboard attack. As a result, the overall risk value of threat #20 (Rw=6.99, 53th) is higher than that of threat #1.

V. MERITS OF PROPOSED METHODOLOGY FROM CASE STUDY RESULTS

In this section, we discuss the merits of our methodology seen from the case study results. Although intended as a demonstration, it seems that our ideas solve two problems mentioned in Subsection II-D and there are some findings revealed by proceeding with a concrete analysis.

A. CHANGE OF TENDENCY BY ENTRY POINT IN ATTACK FEASIBILITY

As mentioned in Subsection II-B, method (ii) based on CVSS is recommended for evaluation of attack feasibility. For Problem A mentioned in Subsection II-D, we propose another approach, RSS-CWSS_CPS. In this subsection, we confirm that our approach solves this problem.

In TABLE 7, we categorize the entry points into four categories and compare the ranking of the top threats in each category between method (ii) and RSS-CWSS_CPS respectively (method (iii) is omitted because it is a simplified version of method (ii)). In method (ii), the threats are ranked higher in the order of network, adjacent network, direct-access, and other physical communication for each entry point, and attack methods seem advantageous in that order. On the other hand, in our proposed method, the order of the highest ranked threats is the same for network and direct-access. As a result, it is not always advantageous for attackers if the attack distance is long.

In [18], the authors compared risk scores between RSS-CWSS_CPS with CRSS (CVSS version 2 based risk scoring system), and mentioned that RSS-CWSS_CPS did not consider the difference of entry point as a decisive factor. They pointed out the weighting of the metrics in RSS-CWSS_CPS is different from that in CVSS (version 2) as a basis for the differences. Based on these claims, we also compare the weighting of the metrics of method (ii) (based on CVSS version 3) with RSS-CWSS_CPS. TABLE 8 shows the amount of change in risk score when one metric is changed by 0.1 and all the remaining metrics are set to 1.

TABLE 7. Ranking trends by entry point.

Entry Point	First Appeared in 456 threats	
	Method (ii) CVSS-based	Our proposal RSS-CWSS_CPS
Network (Cellular, GPS)	1	1
Adjacent (DSRC, LPW, Bluetooth)	8	117
Direct-Access, OBD-II	27	1
Other physical (USB, WC, Sensor)	213	142

TABLE 8. Ammount of change in risk score when metric related to attack feasibility fluctuates by 0.1.

Change of Rw calculated by RSS-CWSS_CPS				
AV	AS	IC	EC	EX
0.2	0.05	1.0	1.0	0.2
Change of Rr calculated by CRSS [18]				
AV	Au	AC		
0.941	0.941	0.941		
Change of E calculated by Method(ii):CWSS-based				
V	C	P	U	
0.822	0.822	0.822	0.822	

The fluctuations by both metrics V and P in method (ii) related to the entry point are 0.822, while those by the metrics AV and AS in RSS-CWSS_CPS are 0.2 and 0.05, whose fluctuations are as small as 1/4 or less. On the other hand, the fluctuation amount by metric C regarding the complexity of the attack of method (ii) is 0.822, while the fluctuations amount by the metrics IC and EC of RSS-CWSS_CPS are both 1.0, which are higher than the fluctuation amount by method (ii).

Thus, it is shown that Problem A is solved. This result shows that CWSS is flexible in terms of attack feasibility and can accommodate characteristics of a particular system.

B. BIAS OF ASSET IMPACT RATING

As we mentioned in Subsection II-D, there exists an impact rating problem in Problem B. Although the four attributes of impact are specified to be safety, financial, operational and privacy, each of them is inexactly classified in only four ranks and the relationship between these attributes is unclear. In this subsection, a solution to this problem is given.

First, we confirm the relationship between attributes (safety, financial, operational, and privacy) in TARA, metrics (C, I, and A) in CVSS, and metrics (TI and BI) in RSS-CWSS_CPS. TABLE 9 shows which metric of each method the SFOP attributes corresponds to. In CVSS, metrics of C (confidentiality), I (integrity) and A (availability) have attributes close to safety, operational and privacy, but there is no corresponding financial attribute. On the other hand, if we use RSS-CWSS_CPS, the three attributes of safety, operational and privacy need to be evaluated only by one metric TI. However, financial attribute can be evaluated by metric BI.

TABLE 9. Interpretation of asset impact.

SFOP attributes	Impact metrics in CVSS	RSS-CWSS_CPS
Safety	Integrity (I) and Availability (A)	The combination of Safety, Operational and Privacy impacts can be evaluated to Technical Impact (TI)
Operational	Availability (A)	
Privacy	Confidentiality (C)	
Financial	No applicable metric	Business Impact (BI)

Although it is necessary to evaluate safety, operational and privacy attributes as the single metric TI, we consider that RSS-CWSS_CPS is advantageous for two reasons:

1) The relationship between the metrics TI and BI is thoroughly considered and standardized, so it is reliable.
2) The metric TI alone can sufficiently evaluate these safety, operational and privacy attributes of the damage scenario.

The rationale for reason 2) is that operational and privacy issues are relatively minor compared to safety as mentioned above for the HEAVENS security model in Subsection II-D. The metric TI can select up to 9 ranks, allowing for more exact quantification of the impact. Therefore, the metric TI can be used to make a comprehensive assessment that combines the impacts of safety attribute and the less weighted operational and privacy attributes.

The left histogram in FIGURE 4 shows the result of the CVSS impact rating of the case study. The histogram of the impact values, which consists of the three attribute values of metrics C, I and A in CVSS, behaves as if it were evaluated by only one attribute value. On the other hand, the middle histogram in FIGURE 4 shows the distribution of TI values in the RSS-CWSS_CPS impact rating results of the case study. The bias in the distribution of the histogram is reduced, and even if the attributes of safety, operational, and privacy are aggregated into the only one metric TI, it seems that impact rating can be performed to classify the impact of individual assets with these three attributes.

The right histogram in FIGURE 4 shows the distribution of the combination values of metrics TI and BI in the RSS-CWSS_CPS impact rating. The histogram distribution is even less skewed, and the risk quantification using BI in addition to TI allows more detailed differentiation of risk values and enables prioritization when taking countermeasures. Thus, it is shown that Problem B is solved.

We also believe that the use of RSS-CWSS_CPS can also mitigate the effects of the cognitive biases also mentioned in Subsection II-D. If the metric rankings become more granular, and the impact of shifting a rating one rank up (or down) for a metric is a small change in rating, analysts are more likely to emotionally choose a higher (or lower) rank.

For example, if there are only two ranks of severity, "High" and "Low," an analyst may hesitate to choose "Low" instead of "High" because of concerns about underestimating risk. However, if the rank of "Middle" is in the middle between "High" and "Low," it may be easier to select "Middle" rather than "High." RSS-CWSS_CPS has finer-grained ranks for each metric and as a result can mitigate cognitive biases.

VI. DISCUSSION

As shown in Section V, we confirm that our methodology makes the TARA process more exact to interpret characteristics of cyber-physical systems, and helps to prioritize significant threats objectively according to the current state of the system. Moreover, we confirm that our methodology can sufficiently quantify the impact of damage to assets while reducing bias in values due to cognitive bias.

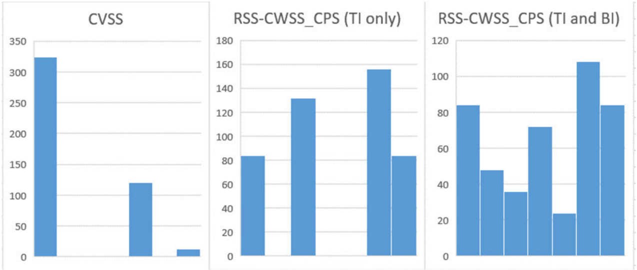

FIGURE 4. Bias of impact rating.

We are also considering an idea to mitigate the effects of cognitive bias. In our case study, the metrics TI and BI, and the SFOP attributes of each asset are linked such as shown in TABLE 3, but it may be better to set certain rules for the distribution of their ranks.

For example, the number of assets whose rank of severity are "High" may be limited within 20% of the total, where there are three ranks such as "High," "Middle" and "Low" to evaluate the severity of an asset's impact. It might be beneficial to create a rule so that the rank allocation is reviewed frequently in the impact rating.

Making rules like them so that the ranks of the metrics are not decided by inertia may be more effective for removing cognitive bias. It seems to be necessary to set each rank of the asset more strictly in the phase of considering the damage scenario.

We mentioned the idea for rank allocations of metrics related to asset impact rating as an example, but similar considerations also seem to be effective in attack feasibility ratings. The issues of rank allocation concerning the attack feasibility is a future study.

VII. CONCLUSION

We focused on the TARA process in the standard ISO/SAE 21434, and introduced "asset container" method and a risk quantification method RSS-CWSS_CPS, for more practical and efficient analysis. We proposed the latter method in particular, as an alternative to describe features such as attack complexity and financial impact on automotive systems more exactly. These features were difficult to describe clearly by existing approaches mentioned on the standard.

We confirmed that our methodology could be applied to the TARA process via a case study of a connected vehicle. The proposed risk quantification method, RSS-CWSS_CPS could detect the recently reported "CAN Invader" direct-access attack, which was not detected by conventional approaches. We also mentioned the relationship between the SFOP attributes of impact rating in the TARA process and metrics TI and BI of RSS-CWSS_CPS. The combination of TI and BI could more exactly express the difference between the four attributes of SFOP.

Although more real case studies are needed, we can interpret real threats correctly, clarify significant threats and analyze risks in more detail. We will proceed with our research, and establish a method that allows researchers to make easy evaluations without relying on advanced security expertise.

REFERENCES

[1] UN Regulation No. 155, *Uniform Provisions Concerning the Approval of Vehicles With Regards to Cyber Security and Cyber Security Management System*, 2021.

[2] M. Wood. (2019). *Safety First for Automated Driving*. [Online]. Available: https://newsroom.intel.com/wp-content/uploads/sites/11/2019/07/Intel-Safety-First-for-Automated-Driving.pdf

[3] *Good Practices for Security of Smart Cars*, ENISA, Athens, Greece, 2019.

[4] *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0*, U.S. Department of Transportation, Washington, DC, USA, 2020.

[5] ISO/IEC, *Information Technology—Security Techniques—Evaluation Criteria for IT Security*, Standard ISO/IEC 15408, 2009.

[6] *Cybersecurity Certification—EUCC, a Candidate Cybersecurity Certification Scheme to Serve as a Successor to the Existing SOG-IS*, Version 1.1.1, ENISA, Athens, Greece, 2021.

[7] K. Maliatsos, C. Lyvas, P. Pantazopoulos, C. Lambrinoudakis, A. Kanatas, M. Gay, and A. Amditis, "Standardizing security evaluation criteria for connected vehicles: A modular protection profile," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2019, pp. 1–7.

[8] ISO/SAE, *Road Vehicles—Cybersecurity Engineering*, Standard ISO/SAE 21434, 2021.

[9] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST). *Common Vulnerability Scoring System (CVSS), Common Vulnerability Scoring System V3.1: Specification Document*. Accessed: Feb. 20, 2023. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[10] Common Criteria, *Common Methodology for Information Technology Security Evaluation*, Evaluation methodology Version 3.1 Revision 5, document CCMB-2017-04-004, 2017.

[11] Society of Automotive Engineers of Japan, *Guideline for Automotive Information Security Analysis*, document JASO TP15002, 2015.

[12] E. Ando, M. Kayashima, and N. Komoda, "A proposal of security requirements definition methodology in connected car systems by CVSS v3," in *Proc. 5th IIAI Int. Congr. Adv. Appl. Informat. (IIAI-AAI)*, Jul. 2016, pp. 894–899.

[13] Y. Kawanishi, H. Nishihara, D. Souma, and H. Yoshida, "Detailed analysis of security evaluation of automotive systems based on JASO TP15002," in *Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS)*. New York, NY, USA: Springer, 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," *Secur. Commun. Netw.*, vol. 2019, pp. 1–35, Feb. 2019, doi: 10.1155/2019/4614721.

[15] Y. Kawanishi, H. Nishihara, H. Yoshida, and Y. Hata, "A study of the risk quantification method focusing on direct-access attacks in cyber-physical systems," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Oct. 2021, pp. 298–305.

[16] ITU-T, *Cybersecurity Information Exchange, Vulnerability/State Exchange, Common Weakness Scoring System*, document ITU-T X.1525, 2015.

[17] Common Weakness Enumeration, *Common Weakness Scoring System (CWSS)*. Accessed: Feb. 20, 2023. [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html

[18] Y. Kawanishi, H. Nishihara, H. Yamamoto, H. Yoshida, and H. Inoue, "A study of the risk quantification method of cyber-physical systems focusing on direct-access attacks to in-vehicle networks," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, 2022, doi: 10.1587/transfun.2022CIP0004.

[19] (2021). *Nearly 20% of Lexus LX SUVs Stolen in Aichi Prefecture*. The Asahi Shinbun. [Online]. Available: https://www.asahi.com/ajw/articles/14378293/

[20] M. Islam, "Deliverable D2-security models. HEAVENS project," Version 2.0, Heavens Consortium, Vinnova/FFI(Fordonsutveckling/Vehicle Development), Sweden, Tech. Rep. D2, 2016.

[21] D. Püllen, N. Anagnostopoulos, T. Arul, and S. Katzenbeisser, "Safety meets security: Using IEC 62443 for a highly automated road vehicle," in *Proc. 39th Int. Conf. Comput. Saf., Rel., Secur. (SafeComp)*, 2020, pp. 325–340.

[22] *U.S. DoT: Revised Departmental Guidance 2016: Treatment of the Value of Preventing Fatalities and Injuries in Preparing Economic Analyses*, U.S. Department of Transpotation, Washington, DC, USA, 2016.

[23] W. T. Siefert and E. D. Smith, "Cognitive biases in engineering decision making," in *Proc. Aerosp. Conf.*, Mar. 2011, pp. 1–10.

[24] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, May 2017.

YASUYUKI KAWANISHI received the B.S. and M.S. degrees in engineering from Tokyo University, in 1991 and 1993, respectively. He is currently pursuing the Ph.D. degree with Kyoto Sangyo University. He is also with Sumitomo Electric Industries Ltd., and the National Institute of Advanced Industrial Science and Technology (AIST). His research interest includes cyber security for cyber-physical systems.

HIDEAKI NISHIHARA received the Ph.D. degree from Osaka University, in 2003. He is currently a Senior Researcher with the Cyber Physical Security Research Center, National Institute of Advanced Industrial Science and Technology (AIST). He has worked on formal approaches for system development for more than 15 years. His current research interests include analyzing safety and security aspects of cyber-physical systems with formal models.

HIROTAKA YOSHIDA received the B.S. degree from Meiji University, Japan, in 1999, the M.S. degree from the Tokyo Institute of Technology, Japan, in 2001, and the Ph.D. degree in electrical engineering from KU Leuven, Belgium, in 2013. From 2001 to 2016, he was with the Research and Development Group, Hitachi Ltd. He is currently a Team Leader with the National Institute of Advanced Industrial Science and Technology (AIST). He is also a member of IACR, IPSJ, and JSAE. In 2013, he won the award for industrial standardization granted by the Japanese Ministry of Economy, Trade and Industry (METI).

HIDEKI YAMAMOTO received the B.E. degree from Kobe University, Japan, in 1985, and the M.E. degree from Kyushu University, Japan, in 1987. Since 1987, he has been with Sumitomo Electric Industries Ltd. (SEI). His current research interest includes cyber security.

HIROYUKI INOUE received the B.S. and M.S. degrees in electronic engineering from Osaka University, in 1987 and 1989, respectively, and the Ph.D. degree in engineering from the Nara Institute of Science and Technology, in 2000. He has been a Professor with the Faculty of information Science and Engineering, Kyoto Sangyo University, since 2021. He is also a Visiting Researcher with the National Institute of Advanced Industrial Science and Technology (AIST). His research interests include technologies for embedded security, especially automotive network security and network protocol of the internet.