IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Advancing Threat and Risk Analysis with a Combined Approach: Asset Container Method and CWSS Integration

Mr. Mounesh A, Ms. Shikha Shetty, Ms. Shilpa, Ms. Shilpa A, Mr. Showrya Shetty
Department of CSE (IoT, Cyber Security including BlockChain)
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India
mouneshstjit25@gmail.com , shikashetty2013@gmail.com , shilpashettigar102@gmail.com ,
mail2shilpa.ajeru@gmail.com, showryashetty20112004@gmail.com

Abstract: *In recent years, the development of cybersecurity standards for cyber-physical systems, such as automotive systems, has seen significant progress. One key development is ISO/SAE 21434, released in 2021, which provides a framework for managing and analyzing cybersecurity in the electrical systems of road vehicles. This standard also introduces methods for the Threat Analysis and Risk Assessment (TARA) process. However, current security analysis techniques face two notable challenges: first, the conventional CVSS-based approach is inadequate for assessing attack feasibility in cyber-physical systems. Second, the relationship between damage factors and their impact on assets remains unclear. This paper addresses these issues by enhancing the TARA process through the use of the "asset container" method for threat classification, as proposed at DECSoS 2017, alongside a CWSS-based risk quantification approach. Furthermore, the paper suggests improvements to risk evaluation methods specifically tailored for automotive systems, focusing on direct access attacks on in-vehicle networks.*

Keywords: Risk quantification and cognitive bias reduction in automotive cybersecurity

I. INTRODUCTION

Connected vehicles are considered safety-critical systems, where a failure or malfunction can pose risks to road users and potentially damage the surrounding environment. With the integration of information and communication technology (ICT), these vehicles have evolved into cyber-physical systems (CPS), merging traditional ICT components with devices that control physical actuators and sensors. This integration has introduced the need to address risks where cyberattacks on these systems can result in physical harm.

In response to the increasing complexity of these systems, there is an urgent need for comprehensive legislation and standardization to address both safety and cybersecurity concerns. Regulatory efforts have been initiated by various bodies, such as the United Nations World Forum for Harmonization of Vehicle Regulations (WP.29) with frameworks like UN-R155. Additionally, major automotive manufacturers have collaborated to develop a framework for testing and validating automated vehicles, and the European Union Agency for Cybersecurity (ENISA) has issued best practices for the security of smart vehicles. In parallel, the U.S. Department of Transportation introduced "Automated Vehicles 4.0" guidelines for automated systems.

The movement toward incorporating security considerations at the design stage, referred to as "security by design," has already begun. This includes initiatives like the Common Criteria (CC)-based cybersecurity certification scheme, which has gained traction, particularly within the EU. Furthermore, various researchers have proposed methods for selecting security requirements for connected vehicles based on CC principles.

The ISO/SAE 21434 standard, published in 2021, builds upon these efforts by providing a comprehensive framework for cybersecurity management in automotive systems. It includes the Threat Analysis and Risk Assessment (TARA) process, which offers guidance for model-based threat and risk analysis. Despite the progress made, challenges remain in applying the TARA process, particularly concerning the evaluation of attack feasibility and the impact of cybersecurity threats. Traditional approaches, such as the Common Vulnerability Scoring System (CVSS) and attack vector analysis,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

are often too simplistic for assessing the complex structures of cyber-physical systems. Additionally, current impact evaluation methods are limited by their inability to clearly define the relationships between different risk factors, such as safety, financial, operational, and privacy concerns.

To address these issues, the authors propose the use of a more refined methodology that leverages the "asset container" approach and the Common Weakness Scoring System (CWSS). These methods are designed to provide a more accurate and practical evaluation of risks in cyber-physical systems. In particular, CWSS introduces additional metrics for evaluating attack complexity and financial risk, which are not as well-defined in CVSS. This paper aims to demonstrate how these approaches can improve the TARA process by conducting a case study on a connected vehicle, comparing the results to traditional CVSS-based methods. The findings show that the proposed approach can identify vulnerabilities, such as the "CAN invader" attack, which were not detected by conventional methods.

The remainder of this paper is organized as follows: Section II reviews related preliminary work, Section III outlinesthe identified problems and introduces the proposed improvements to the TARA process, and Section IV presents a case study on automotive systems using the new methodology. Section V discusses the merits of the approach, Section VI outlines areas for future research, and Section VII concludes the paper.

II. PRELIMINARY

TARA Process in ISO/SAE 21434

The Threat Analysis and Risk Assessment (TARA) process, outlined in Clause 15 of ISO/SAE 21434, is shown in FIGURE 1. This process involves two key steps:

- Defining a damage scenario: This involves outlining a negative outcome related to a vehicle or its functions that impacts a road user. It assesses the extent of damage inflicted on assets due to cybersecurity threats.
- Identifying a threat scenario: This is defined as "a potential cause that compromises the cybersecurity properties of one or more assets, leading to a damage scenario." It assesses how easily attackers can exploit vulnerabilities related to system security.

By combining these two scenarios, the overall risks to the system can be calculated. This concept allows IT security analysis methods to be adapted for use in cyber-physical systems, while addressing safety, financial, operational, and privacy (SFOP) attributes.

Attack Feasibility Ratings in the TARA Process

There are three main methods suggested for assessing the feasibility of attacks on each threat scenario:

- Attack potential-based approach: This method, based on ISO/IEC 18045 (CEM), evaluates attack feasibility from the attacker's viewpoint, considering factors such as their level of expertise and the tools available. However, since thispaper focuses on the network structure of the target of evaluation (TOE), this approach will not be discussed further.
- CVSS-based approach: This method relies on the Common Vulnerability Scoring System (CVSS) to evaluate risks from the perspective of the potential victim. It has been proposed by Ando et al. for threat analysis in automotive systems,including CVSS version 3.0.
- Attack vector-based approach: This simpler method classifies attack feasibility based solely on the type of entry point used by attackers

Impact Ratings in the TARA Process

The impact attributes in the TARA process include safety, financial, operational, and privacy (SFOP), but they are categorized into only four levels: "Severe," "Major," "Moderate," and "Negligible." Additionally, the relationships between these attributes are not clearly defined.

Problems with TARA Ratings

The TARA rating system faces two key issues:

- Problem A: Methods relying on CVSS and attack vector analysis often prioritize network-related threats.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

- Problem B: The impact rating system lacks the necessary precision to evaluate the extent of damage accurately. In automotive systems, financial aspects are often closely linked with other factors, making the current evaluation too simplistic.

Regarding the relationship between SFOP attributes, models like the HEAVENS security framework heavily weight safety and financial factors. For instance, Püllen et al. evaluated impacts based on Passenger Safety (PS), Operational Limitation (OL), and Financial Loss (FL), giving more importance to Passenger Safety, influenced by the Value of a Statistical Life (VSL). This paper takes a different approach to addressing these relationships.

Another issue related to Problem B is the tendency to overestimate risks due to cognitive biases such as "prospect theory," which leads to skewed impact evaluations. These issues will be explored further in Subsection V-B using data from the case study presented in Section IV.

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

To address the issues in the TARA process, we propose the following two methods: the "asset container" method andthe RSS-CWSS_CPS quantification approach. The "asset container" focuses solely on the attack victim’s perspective, while the latter quantifies risks using multiple factors, offering a more flexible evaluation.

"Asset Container" Method

The "asset container" method systematically identifies and organizes threat scenarios based on assets and potential attack vectors, as proposed in [13] and [14]. This method allows for rapid identification and prioritization of risks by analyzing threat scenarios from three perspectives: "Where," "At," and "Asset," which are broken down components of "What."

By focusing only on the victim’s viewpoint, this method ensures that all significant threats are identified without overlooking potential risks, providing a comprehensive analysis of threat actions. The concept, "an attacker tries to harm an asset by reaching into the container of the asset," is visually represented in FIGURE 2.

(Insert FIGURE 2 here)

RSS-CWSS_CPS as Risk Quantification Method

Originally used to evaluate product vulnerabilities, systems such as CVSS and CWSS are employed here as risk quantification methods for the security design phase. They use metrics ranked by severity, which are assigned numerical values. These values are then used in formulas to determine the magnitude of risks.

In ISO/SAE 21434, Annex G provides guidelines for applying these methods in attack feasibility analysis. For example, the CVSS-based approach uses the following formula to calculate the overall exploitability value (E):

E=8.22×V×C×P×UE = 8.22 \times V \times C \times P \times UE=8.22×V×C×P×Uwhere:

- V: Attack Vector (AV),
- C: Attack Complexity (AC),
- P: Privileges Required (PR),
- U: User Interaction (UI)

Each metric is assigned a numerical value based on its rank, indicating the severity of risk. For instance, the "Network" rank for AV has the highest value at 0.85. Once the values are substituted into the formula, the attack feasibility E is calculated.

We propose the RSS-CWSS_CPS method, a risk quantification approach based on CWSS. It computes a risk value Rw, combining attack feasibility and impact ratings through the following formula:

Rw=SBase×SSurface×SEnv10.0Rw = \frac{SBase \times SSurface \timesSEnv}{10.0}Rw=10.0SBase×SSurface×SEnv where:

SBase, SSurface, and SEnv are calculated using CWSS metrics such as TI (Technical Impact), IC (InternalControl), AV, and more.

By assigning appropriate ranks and values, Rw numerically represents the overall risk. The details of these metrics are listed in TABLE 1 and TABLE 2, which show how CWSS metrics align with TARA ratings.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

IV. CASE STUDY

In this section, we consider the architecture of a connected vehicle as a Target of Evaluation (TOE). FIGURE 3 depictsa typical network structure of a connected vehicle, as shown in [24]. In this architecture, functional modules for infotainment, telematics, and an ITS control console are interconnected via an Ethernet network, while the functional modules for power train (PT), body, chassis, advanced driver assistance systems (ADAS), and immobilizer are connected via a CAN bus network. The Central Gateway (CGW) supports communication across both networks. We will apply the proposed TARA process to this architecture.

Definition of Network Structure

The TOE modules are connected via internal networks, such as Ethernet or CAN bus, as follows:

- PT: Powertrain control modules.
- Chassis: Brake and steering control modules.
- Body: Modules for door control, air-conditioning, etc.
- ADAS: Driving assistance modules.
- Immobilizer: Engine ignition control modules.
- CGW: Protocol conversion modules.
- ITS: Modules for V2X (vehicle-to-everything) communication.
- Telematics: Remote communication modules.
- Infotainment: Information and entertainment modules.
- The following are the communication interfaces (entry points) of the TOE:
- Cellular: Long-distance communication interface used for software updates, internet connection, etc.
- GPS: Long-distance communication interface with GPS satellites.
- DSRC: Adjacent communication interface for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication.
- Bluetooth: Adjacent communication interface.
- LPW (Low Power Wireless): Adjacent communication interface between the TPMS and the vehicle.
- USB: Physical interface, such as USB, SD card, etc.
- WC (Wired Communication): Interface used for charging.
- Sensor: Distance measurement sensors.
- OBD-II: Wired interface used for vehicle diagnostics.
- DA (Direct-Access): Unauthorized interface for potential attacks (e.g., connecting an unauthorized device to the internal communication network).

Asset Identification and Impact Rating

We define the assets in the automotive system and identify potential damage scenarios, assigning rank values for each metric, including TI (Technical Impact) and BI (Business Impact), as well as the SFOP attributes. TABLE 3 provides examples of these definitions.

For instance, the "control function of the PT module" is evaluated with a TI and BI of 1.0, indicating a critical threat due to the potential safety risk to road users in case of malfunction.

Threat Scenario Identification

Next, we define threat scenarios that describe how an attacker might access and compromise the assets. Using the "asset container" method, we organize these scenarios using the perspectives of "Where," "At," and "Asset." TABLE 4 lists some example scenarios.

For example, Threat #1 represents an intrusion scenario where an attacker uses the DSRC interface to target the control function of the PT module.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Attack Path Analysis and Attack Feasibility Rating

For each threat scenario, we apply CWSS metrics (detailed in TABLE 1) to rank the attack feasibility. TABLE 5 provides examples of these ratings. Compared to the CVSS approach, which uses only four metrics, the RSS-CWSS_CPS method uses six metrics, allowing for a more granular evaluation of attack feasibility.

For example, Threat #1 (an intrusion via the DSRC interface into the PT module through the ITS module and CGW)is rated as follows:

- IC (Internal Control): 0.5 (due to the complexity of attacking multiple modules),
- AV (Attack Vector): 0.7 (since DSRC is an adjacent communication interface),
- AS (Authentication Strength): 0.8 (authentication required for access to the ITS module),
- EX (Exploitability): 0.6 (disguising the DSRC source is necessary),
- EC (External Control): 0.9 (DSRC interface has countermeasures),
- DI (Distinguishability): 0.6 (limited features distinguishable by the attacker).

This detailed ranking suggests that Threat #1 is relatively low-risk. However, this threat's impact and attack feasibility ratings need to be further quantified to determine the final risk value.

Risk Value Determination and Consideration

Finally, using the eight CWSS metrics, we calculate the risk value Rw for each threat scenario using Formula (2) fromthe RSS-CWSS_CPS method. TABLE 6 provides a list of threat scenarios and their corresponding risk values. Attacks via traditional network interfaces, such as Cellular, as well as direct-access attacks (DA), are included in this list.

For instance, Threat #1 (intrusion via the DSRC interface) has a risk value of 3.60, placing it at 297th in risk severity. However, Threat #20, another DSRC-based attack that doesn't require a springboard, has a higher risk value of 6.99, ranking 53rd due to its greater feasibility.

V. MERITS OF PROPOSED METHODOLOGY FROM CASE STUDY RESULTS

In this section, we discuss the merits of our methodology based on the case study results. Although the study was a demonstration, it appears that our approach addresses two key problems mentioned in Subsection II-D, while revealing additional findings through detailed analysis.

Change of Tendency by Entry Point in Attack Feasibility

As detailed in Subsection II-B, the approach outlined in method (ii), which utilizes CVSS, is suggested for assessing the feasibility of attacks For Problem A (Subsection II-D), we propose an alternative approach using RSS-CWSS_CPS. In this subsection, we confirm that our method solves this issue

In TABLE 7, we categorize the entry points into four groups and compare the top threats in each group, ranked by both method (ii) and RSS-CWSS_CPS (method (iii) is omitted since it is a simplified version of method (ii)). In method(ii), threats are categorized according to their attack proximity, including network, adjacent network, direct access, and other physical communication interfaces. In contrast, our proposed method ranks the top threats similarly for both network and direct access, showing that longer attack distance does not always favour attackers.

In reference [18], the authors contrasted the risk scores obtained using RSS-CWSS_CPS with those from the CRSS, which is based on CVSS version 2. They highlighted that RSS-CWSS_CPS did not prioritize the entry point difference as a decisive factor, unlike CVSS version 2, which weights metrics differently. We also compared the metric weightings in method (ii) (CVSS version 3) with RSS-CWSS_CPS. TABLE 8 shows the risk score changes when a single metric is varied by 0.1 while all other metrics are held at 1.

In method (ii), the fluctuations of metrics V and P, related to the entry point, are both 0.822, while in RSS-CWSS_CPS,the fluctuations of AV and AS are much smaller (0.2 and 0.05, respectively). On the other hand, the complexity metric C in method (ii) fluctuates by 0.822, whereas the IC and EC metrics in RSS-CWSS_CPS both have fluctuations of 1.0, making them more significant than in method (ii).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

This comparison shows that Problem A is resolved, as the CWSS methodology is flexible regarding attack feasibility and better accounts for system characteristics.

Bias of Asset Impact Rating

As discussed in Subsection II-D, Problem B relates to the impact rating, where the attributes—safety, financial, operational, and privacy—are imprecisely classified into just four ranks, and the relationship between these attributes is unclear. This subsection presents our solution.

We first examine the relationship between the SFOP attributes in TARA, the C, I, and A metrics in CVSS, and the TI and BI metrics in RSS-CWSS_CPS. TABLE 9 shows how these metrics correspond. In CVSS, the C, I, and A metrics align with safety, operational, and privacy, but there is no corresponding financial attribute. In RSS-CWSS_CPS, the TI metric evaluates safety, operational, and privacy together, while the financial attribute is handled by the BI metric.

Although TI alone evaluates safety, operational, and privacy, RSS-CWSS_CPS has two distinct advantages:

- The relationship between TI and BI is well-defined and standardized, making it more reliable.
- TI can effectively assess these attributes, particularly safety, which outweighs operational and privacy concerns. The reasoning for this second point stems from the HEAVENS security model (Subsection II-D), where safety dominates the impact assessment. The TI metric, which has up to 9 ranks, provides more precise quantification of impact,

allowing it to combine safety with operational and privacy concerns effectively.

The left histogram in FIGURE 4 shows the results of the CVSS impact rating for the case study. The impact distribution, represented by the C, I, and A values, behaves as if it were evaluated by a single attribute. In contrast, the middle histogram shows the distribution of TI values from the RSS-CWSS_CPS impact rating, with reduced bias. Even with safety, operational, and privacy attributes aggregated into one metric (TI), the impact rating distinguishes between individual assets.

Finally, the right histogram in FIGURE 4 shows the distribution of the combined TI and BI values in RSS-CWSS_CPS, with even less skewness. This combination allows for more detailed risk differentiation and prioritization when countermeasures are taken, thus solving Problem B.

We also believe that RSS-CWSS_CPS helps reduce cognitive biases, as mentioned in Subsection II-D. Finer-grained metrics make it less likely for analysts to emotionally select higher or lower ranks based on perceived risk severity. For example, if there are only two ranks ("High" and "Low"), an analyst may hesitate to select "Low" for fear of underestimating risk. However, if a middle rank is available, such as "Medium," the selection becomes easier and less prone to bias. With RSS-CWSS_CPS, the granular ranking system helps mitigate these biases

VI. DISCUSSION

In Section V, we established that our methodology enhances the TARA process by providing a more precise interpretation of cyber-physical systems' characteristics and facilitating the objective prioritization of significant threats based on the system's current state. Additionally, our approach successfully quantifies the impact of asset damage while mitigating biases introduced by cognitive factors.

Mitigating Cognitive Bias

To further address cognitive bias, we propose refining the ranking process for asset impact ratings. Currently, the metrics TI and BI and the SFOP attributes are linked, but introducing rules for rank distribution could improve accuracy. For instance, limiting the proportion of assets rated as "High" severity to 20% might prevent overestimation of risks and ensure a more balanced assessment.

Regular review and adjustment of rank allocations could help avoid inertia in the rating process, thus reducing cognitive bias. This adjustment should be part of the damage scenario evaluation phase, ensuring that each asset's rank is assigned with greater precision.

Rank Allocation in Attack Feasibility

Our discussion also touches on the importance of rank allocation in evaluating attack feasibility. Similar to impact rating, setting clear and structured rules for ranking attack feasibility could enhance the assessment's accuracy. This

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

aspect will be explored in future research to determine how best to apply such rules to mitigate biases and ensure a thorough evaluation of potential attack paths.

Overall, our methodology provides a more nuanced approach to threat assessment and risk analysis, addressing previous limitations and offering a framework that can be adapted to various contexts within cybersecurity for cyber-physical systems.

VII. CONCLUSION

In this study, we focused on the Threat Analysis and Risk Assessment (TARA) process outlined in the ISO/SAE 21434 standard, introducing the "asset container" method and the RSS-CWSS_CPS risk quantification method for a more practical and efficient analysis. The RSS-CWSS_CPS method, in particular, serves as an alternative to describe attack complexity and financial impact on automotive systems with greater accuracy—features that existing approaches within the standard have struggled to address clearly.

Our case study on a connected vehicle demonstrated that our proposed methodology can be effectively applied to the TARA process. The RSS-CWSS_CPS method successfully identified the "CAN Invader" direct-access attack, which conventional approaches failed to detect. By integrating the metrics TI and BI, our approach provides a more precise representation of the SFOP attributes—safety, financial, operational, and privacy—allowing for a more nuanced impact assessment.

While further real-world case studies are needed to validate and refine our methodology, our research indicates that it is possible to interpret threats accurately, highlight significant risks, and perform detailed risk analysis. We aim to continue developing our method to enable easier evaluations and enhance security assessments, even for those without advanced security expertise.

REFERENCES

[1] Kawanishi, Y., Nishihara, H., Yamamoto, H., Yoshida, H., & Inoue, H. (2022). ‘‘A study of the risk quantification method of cyber-physical systems focusing on direct-access attacks to in-vehicle networks,’’ IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2022. doi:10.1587/transfun.2022CIP0004.

[2] Common Weakness Enumeration. (2023). Common Weakness Scoring System (CWSS). [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html

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

[4] ISO/SAE. (2021). Road Vehicles—Cybersecurity Engineering, Standard ISO/SAE 21434. International Organization for Standardization.

[5] Kawanishi, Y., Nishihara, H., Souma, D., & Yoshida, H. (2019). ‘‘A comparative study of JASO TP15002-based security risk assessment methods for connected vehicle system design,’’ Security and Privacy, vol. 2019, pp. 1–35, Feb. 2019. doi: 10.1155/2019/4614721.

[6] Kawanishi, Y., Nishihara, H., Yoshida, H., & Hata, Y. (2021). ‘‘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.

[7] ISO/IEC. (2009). Information Technology—Security Techniques—Evaluation Criteria for IT Security, Standard ISO/IEC 15408. International Organization for Standardization.

[8] Common Criteria. (2017). Common Methodology for Information Technology Security Evaluation, Evaluation Methodology Version 3.1 Revision 5. Document CCMB-2017-04-004.

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

[10] Ando, E., Kayashima, M., & Komoda, N. (2016). ‘‘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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

[11] ITU-T. (2015). Cybersecurity Information Exchange, Vulnerability/State Exchange, Common Weakness Scoring System, document ITU-T X.1525.
[12] Siefert, W. T., & Smith, E. D. (2011). ‘‘Cognitive biases in engineering decision making,’’ in Proc. Aerosp. Conf., Mar. 2011, pp. 1–10.
[13] Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). ‘‘In-vehicle network attacks and countermeasures: Challenges and future directions,’’ IEEE Network, vol. 31, no. 5, pp. 50–58, May 2017.
[14] Püllen, D., Anagnostopoulos, N., Arul, T., & Katzenbeisser, S. (2020). ‘‘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.
[15] Islam, M. (2016). Deliverable D2-security models. HEAVENS project, Version 2.0, Heavens Consortium, Vinnova/FFI (Fordonsutveckling/Vehicle Development), Sweden, Tech. Rep. D2.
[16] U.S. Department of Transportation. (2016). Revised Departmental Guidance 2016: Treatment of the Value of Preventing Fatalities and Injuries in Preparing Economic Analyses, Washington, DC, USA.