Human Interaction and Emerging Technologies (IHIET 2023), Vol. 70, 2023, 232–241
https://doi.org/10.54941/ahfe1002948

Safety and Security Analysis of Connected and Automated Vehicles: A Methodology Based on Interaction with Stakeholders

Shahzad Alam[1], Giedre Sabaliauskaite[2], Hesamaldin Jadidbonab[1], and Jeremy Bryans[1]

[1]Systems Security Group, Centre for Future Transport and Cities, Coventry University, Coventry, CV1 5FB, UK
[2]Systems Security Group, Department of Computer Science, Swansea University, SA1 8EN, UK

ABSTRACT

Connected and Automated Vehicles (CAVs) are becoming global phenomena and making their way into our society. With the increase in vehicle system automation and connectivity levels, reliance on technology increases, which reduces the human influence on vehicle dynamic driving tasks. This development significantly transformed the nature of human-vehicle interaction design from control to supervisory control. The final goal of CAVs is to enable driverless rides (SAE L4 – 5), where various stakeholders (passengers, service providers, and insurers) will interact during the post-development phases of the vehicle life cycle. CAVs are susceptible to safety and cyber security attacks where a successful attack could lead to various safety, operational, financial, and privacy losses. This paper aims to propose a methodology for safety and security analysis of CAV interaction with various stakeholders and is aligned with automotive cyber security standard ISO/SAE 21434. This standard provides the guideline to perform risk management for vehicles, considering the vehicle system level only; whereas the prescribed methodology will complement standard ISO/SAE 21434, performs safety and security analysis based on the CAV - Stakeholders interaction model and investigates the impact of cybersecurity incidents on various stakeholders. The paper presents the methodology which builds upon knowledge combining the known techniques from the safety and security domain. The research results in developing an interaction model, and identifying interaction assets, their vulnerabilities, and threats. Furthermore, it performs an attack consequences analysis to demonstrate the impact of the attack on various stakeholders. The developed methodology can be applied to any post-development phase of the CAV life cycle, such as operation, maintenance, and decommissioning.

Keywords: Connected and automated vehicles (CAVs), Safety and cybersecurity, Stakeholder interaction, Human-computer interaction, ISO/SAE 21434

INTRODUCTION

The rapid development in digital technologies (i.e., the Internet of things, artificial intelligence, and power communication networks) enables modern vehicles to become more connected and intelligent. Now automotive industries are trending towards bringing fully automated vehicles to the market (Jahan et al., 2019). With the increase in automation level, reliance on technology increases and which reduces the human influence on vehicle's dynamic driving tasks. This development significantly transformed human-vehicle interaction from control to supervisory control (Sun et al., 2018). There are different levels of vehicle automation, which are defined by the Society of Automotive Engineers (SAE) standards J3016, from level 0 (no driving automation) to level 5 (full automation) (SAE, 2016). The final goal of Connected and Automated Vehicles (CAVs) is to enable driverless vehicles (SAE L4 – 5) into our society.

With the increase in vehicle automation and connectivity level, CAVs are becoming more vulnerable and brought unprecedented cyber-attacks. It is evident from the literature that CAVs are susceptible to cyber-attacks (Aliwa et al., 2021, Sun et al., 2021, Woo et al., 2014, Bouchelaghem et al., 2020). Before providing any effective solution for the security of CAV, risk assessment is considered as an important foundation for the realization of automotive cyber security (Wang et al., 2021). Recently, in 2021 a new standard "ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering" was introduced, which emphasizes managing the security risk of vehicles throughout the vehicle life cycle (*ISO/SAE 21434:2021* 2021). As a result, we can now expect automotive companies to be required to perform Threat Analysis and Risk Assessment (TARA) in accordance with the ISO/SAE 21434 guidelines.

Several risk assessment frameworks and approaches have been proposed to address risks at the vehicle system level, including EVITA (Ruddle et al., 2009), STPA (Salmon et al., 2022), SAHARA (Macher et al., 2015), and THARA (Agrawal et al., 2021) which identify weaknesses that could be exploited by attackers. However, there are currently no methods available for conducting safety and security analysis that take into account the interactions between CAVs and stakeholders and explore the impact of cybersecurity incidents on these stakeholders. Security failure in the CAV system potentially may threaten human safety, and privacy or/and can cause vehicle damage and financial losses (Wang et al., 2021). Hence, it is crucial to approach the human-technology relationship in a more systematic manner, as relying solely on technological solutions for cybersecurity will not suffice to resolve the issue (Chong et al., 2019).

This study aims to fill the above gap by proposing a methodology that focuses on stakeholder interaction and performs safety and security analysis. The proposed methodology is aligned with the guidelines of the cybersecurity standard ISO/SAE 21434 and considers the post-development phases of the CAV life cycle. As in ISO/SAE 21434, the post-development phase refers to the operations, maintenance, and decommissioning phases of the vehicle (*ISO/SAE 21434:2021* 2021). Figure 1 illustrates various stakeholders'

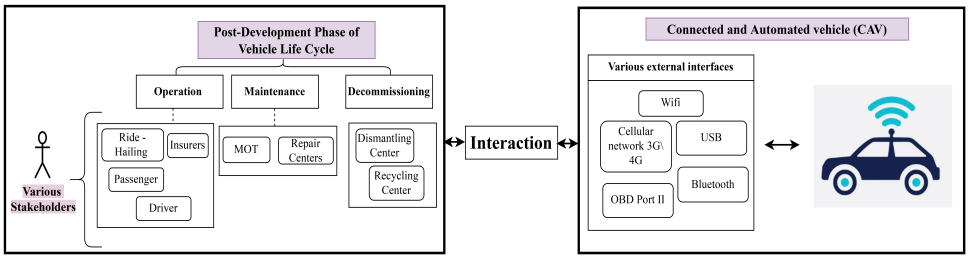

Figure 1: CAV- Stakeholder Interaction – During post-development phases of vehicle.

interaction with CAV during post development phases of the CAV life cyle. The interaction between CAV and stakeholders refers to the exchange of information and data between stakeholders and the CAV system. This enables the stakeholders to stay informed about the vehicle's behavior, use its features and functions, and perform supervisory control over the CAV (Bakhtina and Matulevicius, 2022). The CAV system is responsible for supporting and enabling this interaction. The stakeholders in this process may include passengers, service providers, ride-hailing services, insurers, and maintenance and repair providers, as depicted in Figure 1.

The proposed methodology will potentially enhance the risk assessment approach as it considers human factors within the cybersecurity context, to investigate the impact of cybersecurity incidents on various stakeholders.

METHODOLOGY

This section explains the overall structure of the Safe and Secure Interaction (SSI) methodology (see Figure 2). The proposed SSI methodology considers SAE (L4-5) vehicles, and its scope is not limited to a specific scenario; it includes post-development phases of the vehicle life cycle.

Overview

The proposed methodology SSI consists of a process modeling technique, a threat-driven approach, and tool support from the safety and security domain. The aim is to find the risks associated with CAV – Stakeholder interaction and keeping it aligned with the guidelines of cybersecurity standard ISO/SAE 21434. It systematically develops the CAV – Stakeholder interaction model, identifies assets, threats, and performs attack consequences analysis.

To model the CAV – Stakeholder interaction process, the Business Process Model Notation (BPMN) is used. It is a process modeling tool that visually represents the process as a network of activities and tasks and information data flows between them (Aagesen and Krogstie, 2015). The objective of using BPMN is to provide a process-oriented approach that is easily understandable for both business and technical stakeholders. BPMN allows the process to be represented from a business perspective, helping to bridge the gap between business requirements and technical implementation.

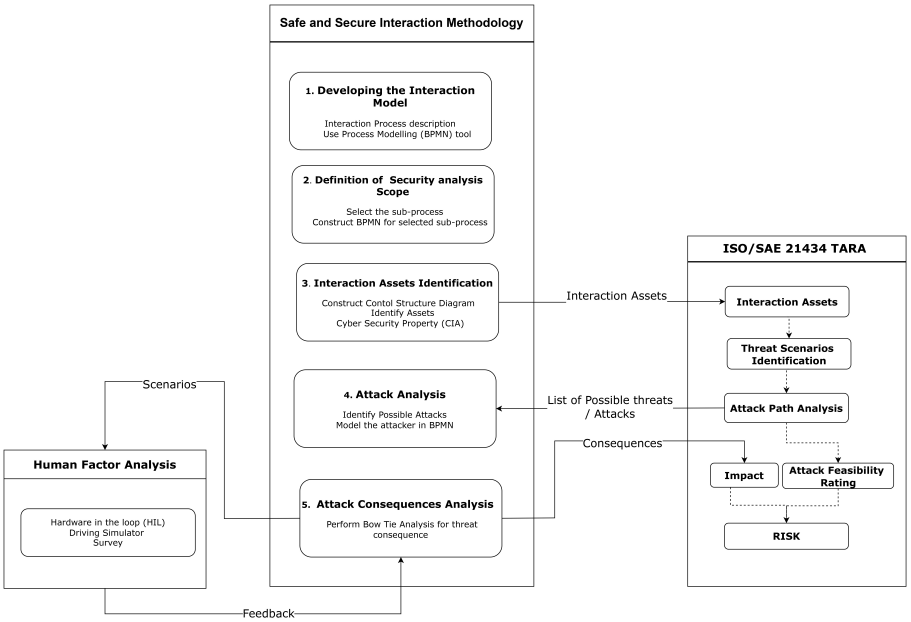

Figure 2: Proposed methodology for safety and security analysis of CAVs based on Interaction with Stakeholders – Aligned with ISO/SAE 21434.

The proposed methodology uses the Control Structure Diagram (CSD) to identify interaction assets in the process. The CSD is a useful tool in System-Theoretic Process Analysis (STPA) that helps to identify potentially unsafe control actions which may lead to system failures (Salmon et al., 2022).

To identify potential threats to interaction assets, threat-driven approach is employed. Various threat modeling techniques exist in the literature to identify potential threats and attacks. ISO/SAE 21434 recommends several approaches to threat modeling, including EVITA (Ruddle et al., 2009), PASTA (UcedaVelez and Morana, 2015), and STRIDE (Scandariato et al., 2015). Any of these methods can be used to identify threats on interaction assets.

Bow Tie Analysis (BTA) is utilized for analyzing the consequences of an attack and demonstrating how it can impact all stakeholders involved in the interaction process. BTA is a risk assessment tool widely used in various industries to identify potential hazards and associated risks (Aust and Pons, 2020). This tool visually represents potential risks, their causes, and consequences in a model that resembles a bow tie. BTA is predominantly used in safety risk management and combines elements of both fault tree analysis and event tree analysis (Shahriar et al., 2012). The BT model features a central node that represents a potential risk or hazard/incident, with the causes of the risk located on the left side of the model, while the right side represents the consequences of the risk. We have developed an extended model of BTA that allows for the modeling of attack consequences on various stakeholders and their impacts in terms of safety, privacy, financial, and operational considerations. This extended model helps to identify the potential impact of an attack on these key areas and can inform risk management and mitigation strategies.

Moreover, the various scenarios that are identified in the BT model will be utilized to conduct Hardware-in-the-loop (HIL) simulations for the purpose of validating and verifying the proposed methodology. By incorporating human factors into simulation-based results, this approach provides a more comprehensive and effective analysis. Furthermore, the output from this analysis can also be used as input for the risk calculation in accordance with ISO/SAE 21434 TARA.

The proposed methodology consists of five key steps.

Step 1: Developing the Interaction Model

To develop the interaction model, the CAV-Stakeholder interaction process should be described in a descriptive form, covering the process from start to end. This will help to establish the scope, context, and understanding of the process.

- Define the internal and external stakeholders in the interaction process.
- What are the major steps in the CAV - Stakeholders interaction process?
- What information data is being exchanged between CAV - Stakeholders?
- Define the major activities, and tasks in the process and specify stakeholders responsible for performing the activities and tasks.

Based on the description, develop the interaction model using BPMN. The objective of developing the interaction model is to visually represent the CAV-stakeholder interaction process with a particular focus on the exchange of information data in the process. The information data is crucial for performing a comprehensive safety and security analysis. The interaction model is used as input for safety and security analysis.

Step 2: Definition of Security Analysis Scope

Here the scope of security analysis is defined based on the interaction model. To narrow down the scope of security analysis, we consider the part from the complete interaction process model and perform a detailed analysis.

Step 3: Interaction Assets Identification

According to the cyber security standard ISO/SAE 21434, assets can be any data, components, and/or device that supports information-related activities and can impact the cyber security property of the process – Confidentiality, Integrity, and Availability (CIA). Based on this definition we consider our Interaction assets as transmitted or received data that could be subject to attack and lead to disruption in the CAV-Stakeholder interaction process. In this step, based on the Control Structure Diagram (CSD), interaction assets are identified.

CSD contains the main control elements and control actions between the controllers and the controlled systems. Based on the CAV-Stakeholder interaction model, CSD is derived. Considering stakeholders as controllers, and information exchange during the process as control actions. The failure of the control action would lead to any disruption in the process is considered an interaction asset.

Next, define the cybersecurity properties of interaction assets. The cybersecurity criteria of assets are defined by cybersecurity goals, which are to ensure the CIA, of an asset from threats. CIA triad is the main cybersecurity criteria that characterize the assets.

Input to ISO/SAE 21434: Once interaction assets are identified, the next is to identify cyber threats and attacks on assets. Adversary usually exploits the vulnerabilities in the system assets (i.e. In-vehicle Infotainment system (IVI), Telematic Control Unit (TCU)) to launch attacks (Matulevičius, 2017). These system assets support the interaction assets and are responsible for storing, producing, and generating interaction assets. In ISO/SAE 21434 TARA, various approach is suggested for the identification of possible threats and attacks on system asset use any of these methods for the identification of threats and attacks. In addition, there are various other approaches as well in the literature that can be used for threat and attack identification such as - CAPEC (Xiong et al., 2022), and Attack Trees (Saini et al., 2008).

Step 4: Attack Analysis

In this step attack analysis is performed based on a list of possible threats and attacks identified in the previous step. First, enlist all the possible threats and attacks derived from threat modeling (i.e., STRIDE) which is identified in the previous step as depicted in Figure 2. Then add the attack to the CAV-Stakeholder interaction model, to visualize the attack on assets and their relationship with remaining activities and information data flows. We use cyber security extension to BPMN, illustrated in (Altuhhov et al., 2013) to add the attacker to the model. Based on the attacker model - compromise activities and information data flow in the CAV-Stakeholder interaction is identified.

Step 5: Attack Consequences Analysis

In this last step of methodology, Bow Tie analysis is used to identify possible consequences of an attack on various stakeholders. we proposed the extended Bowtie model which contains seven elements that help to identify the potential risk associated with the attack. The main element of the BT model include:

Top Event: The first step is to identify the top event. The top event is the central point of the model and represents an undesirable incident/ event. For instance, the top event is when the cybersecurity property of an interaction asset has been compromised. Cybersecurity properties of interaction assets are identified in step 2 of the methodology (Interaction Assets identification) and consider as the top event in this model.

Causes: Once the top event is identified, next is to identify the potential causes (threats and attacks) which could lead to the undesirable event (Top Event). In step 3 of methodology (Attack analysis) list of threats and attacks are identified, which could lead to compromising the CIA property of assets

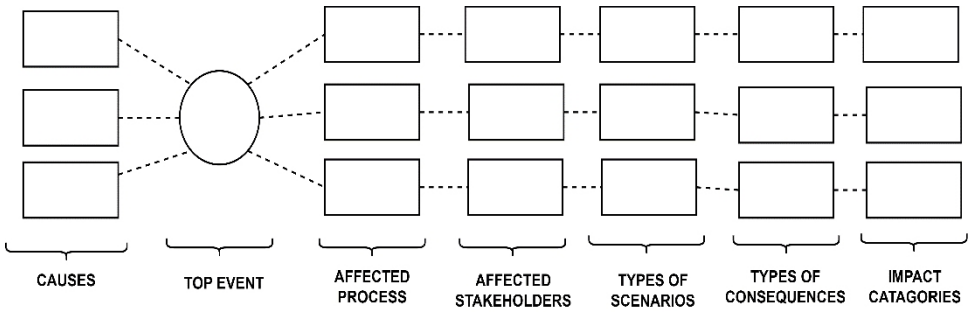

Figure 3: Extended Bow Tie Model – Consequences of an undesirable event on stakeholders.

(Top Event). We consider these identified threats and attacks as causes in this model.

Affected Process: Identify the affected process, which part of the interaction process is affected by the cyber-attack.

Affected Stakeholders: Identify all possible affected stakeholders in the process. For this step, consider the interaction model, which is developed in the first step of methodology, where various stakeholder is identified.

Types of Scenarios: In this step, types of scenarios are identified. What can be the possible scenarios of attack? Is it a silent attack – a person is unaware of the attack (personal data is compromised but the victim is unaware of the attack). Or is it an explicit attack – where a person is been aware of the attack (i.e., ransomware attack, encrypts the victim's personal data, and demands ransom payment) (Payre et al., 2022).

Types Consequences: Based on scenarios, what are the consequences of the top event (undesirable event) on affected stakeholders. This could be injuries, loss of personal data, damage to equipment, loss of service, loss of trust, financial loss, or loss of life.

Impact Category: The last step of the BT model is to categorize the impact of these consequences on stakeholders in terms of Safety, Financial, Operational, and Privacy (S, F, O, P) as suggested in ISO/SAE 21434.

Figure 3 illustrates the BT model, where on the left side of the Top event are the causes, and on the right side of the Top event are the affected process, affected stakeholders, type of scenarios, types of consequences, and impact category.

Different scenarios identified in the BT model will be replicated to conduct Hardware-in-the-loop (HIL) simulation as shown in Figure 2. The objective is to enhance the Attack consequences analysis. The output of this analysis is the potential consequences of undesirable events on various stakeholders during CAV interaction. These results are provided to calculate the impact rating and risk calculation (Figure 2).

DISCUSSION

The proposed SSI methodology demonstrates a comprehensive approach to analyzing the potential consequences of the undesirable event by considering

safety, security, and human factors. Our methodology is well aligned with the guideline of cyber security standard ISO/SAE 21434 and is not limited to one specific scenario; it includes post-development phase of the vehicle life cycle.

There are various approaches for determining attack feasibility level, such as attack potential based and Common Vulnerability Scoring System (CVSS) based methods. However, there are no approaches for identifying attack impact level. Thus, SSI methodology, which provided a comprehensive approach for determining attack impact, could potentially complement risk assessment in ISO/SAE 21434 TARA process.

CONCLUSION

The primary goal of this study is to propose a methodology based on CAV interaction with various stakeholders to perform safety and security analysis. In the literature, it is evident that CAVs are vulnerable to cyber-attacks and a hacker can exploit those vulnerabilities and can gain unauthorized access to the vehicle system. Therefore, before providing an effective cybersecurity solution, it is important to perform a comprehensive risk assessment of automotive cybersecurity across all phases of the vehicle life cycle. Several risk assessments have been proposed, that deal with risk at the vehicle's system. We propose a novel methodology that includes CAV – Stakeholder interaction risk assessment.

In this study, we consider the post-development phases of the CAV (L4-5) life cycle and presented a methodology which builds upon techniques from the safety and security domain and is used in conjunction with ISO/SAE 21434. This methodology includes several steps, such as interaction model construction, asset identification, attack identification, and attack consequences analysis. The output of this analysis provides input in calculating the impact rating and risk calculation.

In future work, we will investigate the impact of a cyberattack on various stakeholders by keeping the hardware in the loop simulation. Different scenarios identified in the attack consequences analysis of the proposed methodology will be used in conducting this simulation. The feedback from this simulation will enhance the methodology and will be useful in calculating the risk level.

REFERENCES

AAGESEN, G. & Krogstie, J. 2015. BPMN 2.0 for modeling business processes. *Handbook on Business Process Management 1: Introduction, Methods, and Information Systems*, 219–250.

Agrawal, V., Achuthan, B., Ansari, A., Tiwari, V. & Pandey, V. 2021. THARA-A Framework to Align the Functional Safety and Security Process in Automotive Domain.

Aliwa, E., Rana, O., Perera, C. & Burnap, P. 2021. Cyberattacks and countermeasures for in-vehicle networks. *ACM Computing Surveys (CSUR),* 54, 1–37.

Altuhhov, O., Matulevičius, R. & Ahmed, N. 2013. An extension of business process model and notation for security risk management. *International Journal of Information System Modeling and Design (IJISMD),* 4, 93–113.

Aust, J. & Pons, D. 2020. A systematic methodology for developing bowtie in risk assessment: application to borescope inspection. *Aerospace,* 7, 86.

Bakhtina, M. & Matulevicius, R. 2022. Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.,* 13, 87–111.

Bouchelaghem, S., Bouabdallah, A. & Omar, M. Autonomous Vehicle Security: Literature Review of Real Attack Experiments. The 15th International Conference on Risks and Security of Internet and Systems, 2020.

Chong, I., Xiong, A. & Proctor, R. W. 2019. Human factors in the privacy and security of the internet of things. *Ergonomics in design,* 27, 5–10.

Jahan, F., Sun, W., Niyaz, Q. & Alam, M. 2019. Security modeling of autonomous systems: A survey. *ACM Computing Surveys (CSUR),* 52, 1–34.

Macher, G., Sporer, H., Berlach, R., Armengaud, E. & Kreiner, C. Sahara: a security-aware hazard and risk analysis method. 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015. IEEE, 621–624.

Matulevičius, R. 2017. *Fundamentals of secure system modelling*, Springer.

Payre, W., Perello March, J., Sabaliauskaite, G., Jadidbonab, H., Shaikh, S., Nguyen, H. N. & Birrell, S. How System Failures and Ransomwares Affect Drivers' Trust and Attitudes in an Automated Car? A Simulator Study. International Conference on Human Interaction & Emerging Technologies: IHIET, 2022. 453–460.

Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., Leimbach, T., Fuchs, A., Gürgens, S. & Henniger, O. 2009. Deliverable D2. 3: Security requirements for automotive on-board networks based on dark-side scenarios. *EVITA project*.

Sae, T. 2016. Definitions for terms related to driving automation systems for on-road motor vehicles. *SAE Standard J,* 3016, 2016.

Saini, V., Duan, Q. & Paruchuri, V. 2008. Threat modeling using attack trees. *Journal of Computing Sciences in Colleges,* 23, 124-131.

Salmon, P. M., Stanton, N. A., Walker, G. H., Hulme, A., Goode, N., Thompson, J. & Read, G. J. 2022. The Systems Theoretic Process Analysis (STPA) Method. *Handbook of Systems Thinking Methods*. CRC Press.

Scandariato, R., Wuyts, K. & Joosen, W. 2015. A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering,* 20, 163–180.

Shahriar, A., Sadiq, R. & Tesfamariam, S. 2012. Risk analysis for oil & gas pipelines: A sustainability assessment approach using fuzzy based bow-tie analysis. *Journal of loss prevention in the process Industries,* 25, 505–523.

Sun, X., Chen, H., Shi, J., Guo, W. & Li, J. From hmi to hri: Human-vehicle interaction design for smart cockpit. Human-Computer Interaction. Interaction in Context: 20th International Conference, HCI International 2018, Las Vegas, NV, USA, July 15–20, 2018, Proceedings, Part II 20, 2018. Springer, 440–454.

Sun, X., Yu, F. R. & Zhang, P. 2021. A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*.

Ucedavelez, T. & Morana, M. M. 2015. *Risk Centric Threat Modeling: process for attack simulation and threat analysis*, John Wiley & Sons.

Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y. & Wang, J. 2021. A systematic risk assessment framework of automotive cybersecurity. *Automotive Innovation,* 4, 253–261.

Woo, S., Jo, H. J. & Lee, D. H. 2014. A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on intelligent transportation systems,* 16, 993-1006.

Xiong, W., Legrand, E., Åberg, O. & Lagerström, R. 2022. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling,* 21, 157–177.

ISO/SAE 21434:2021 (2021) *ISO*. Available at: https://www.iso.org/standard/70918.html (Accessed: February 17, 2023).