Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434

Khan, A., Bryans, J. & Sabaliauskaite, G.

Original citation & hyperlink: Khan, A, Bryans, J & Sabaliauskaite, G 2022, Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434. in J Zhou, S Adepu, C Alcaraz, L Batina, E Casalicchio, S Chattopadhyay, C Jin, J Lin, E Losiouk, S Majumdar, W Meng, S Picek, J Shao, C Su, C Wang, Y Zhauniarovich & S Zonouz (eds), Applied Cryptography and Network Security Workshops - ACNS 2022 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S and P, SCI, SecMT, SiMLA, Proceedings. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 13285 LNCS, Springer, Cham , pp. 235-247, International Conference on Applied Cryptography and Network Security, ACNS 2022, Rome, Italy, 20/06/22. https://doi.org/10.1007/978-3-031-16815-4_14

DOI 10.1007/978-3-031-16815-4_14
ISSN 0302-9743
ESSN 1611-3349

Publisher: Springer

The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-031-16815-4_14

Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434

Ahmed Khan, Jeremy Bryans, and Giedre Sabaliauskaite

Center for Future Transport and Cities, Coventry University, UK
khana270@uni.coventry.ac.uk, ac1126@coventry.ac.uk,
ad5315@coventry.ac.uk

Abstract. Safety-critical Cyber-Physical Systems, such as high-tech cars, require new risk management approaches to investigate and address their cybersecurity risks. The current standard for automotive security ISO/SAE 21434 presents such a framework, which discusses the threats, the associated risk, and the chosen treatment, which can be risk reduction through the implementation of a countermeasure or defense. This paper presents a residual cybersecurity risk management framework aligned with the ISO/SAE 21434 framework. The proposed approach audits the applied defenses over the generated attack paths for the identified threats and associated system components. Flow networks are used to calculate the reduced or mitigated risk and the remaining risk of the threat in the presence of the selected countermeasure. The feasibility of the method is explained using a simple automotive system example.

Keywords: Cybersecurity, ISO/SAE 21434, Risk management framework, Residual risk, Attack tree, Flow graph.

1 Introduction

A few decades ago, vehicles had few basic Electronic Control Units (ECUs) connected to actuators and sensors for small-scale communication. Over time, cars used artificial intelligence-enhanced components, became connected to the Internet and the adjacent vehicles and the roadside infrastructure. These improvements were only possible because of the complex integration of control units, sensors, actuators, and different communication systems [1]. There are up to 150 ECUs in any modern vehicle with complex integration of these ECUs using multiple in-vehicle networks including the Controller Area Network (CAN) [28]. ECUs receive inputs from numerous sensors, for instance, acceleration sensors, Tyre Pressure Monitoring Sensor (TPMS), and wheel speed sensors among others. Systematic connections and communications between sensors and control units gave rise to Cyber-Physical Systems (CPS). On the other hand, Vehicle to Vehicle (V2V) and Vehicle to infrastructure (V2I) communication needs a fusion of Bluetooth, Wi-Fi, and 4G/5G technologies [1]. This integration leads

us towards a more complex and vulnerable system as more attack surfaces will be available in a system [2]. Several published attacks show that it is possible to exploit these attack surfaces and these attacks can also affect the operational safety of a vehicle [3], [4].

According to available reports [28], it is possible to attack core functions of vehicles, such as disconnecting the brakes from the engine. In 2015 there were about 1.4 million cars recalled by Chrysler because of a discovered vulnerability using which hackers can remotely take control of the digital system of a Jeep over the Internet [5]. The Tesla Model S was hijacked remotely from 12 miles away as reported in [6]. Recently, researchers have found 14 vulnerabilities in the infotainment system of multiple BMWs series [9]. The above mentioned studies show that it is crucial to address automotive cybersecurity throughout the development process. The standard ISO/SAE 21434 was compiled to address the issues of integration of automotive cybersecurity in the whole product life cycle of a modern vehicle [7].

The complex infrastructure of modern vehicles increases the risk of cyber-attacks as the cyber risk of the whole system is composed of the risk of an individual interconnected component. ISO/SAE 21434 [15] suggests including cybersecurity aspects at multiple stages of vehicle development. It also includes risk determination and treatment of the assets. Clause 15, Threat analysis and risk assessment (TARA) method is designed for the risk assessment and the treatment decision. Currently, the standard considers the risk treatment decision as the very last step of TARA. Still, it does not advise identifying the residual risk after applying appropriate risk treatment decisions. Thus if a countermeasure is chosen there is no calculation of the residual risk.

In ISO 26262, there is consideration of residual risk (defined there as risk remaining after the deployment of safety measures) but ISO/SAE 21434 [15] has not included the corresponding security concept as of yet. We define residual risk as to the remaining risk after applying the chosen threat defenses [9]. It is vital to consider the effectiveness of the used control measures over the identified threat. According to [10] after evaluation, the mitigated risk after applying the defenses is less than expected. Multiple risk management frameworks are designed according to the standards such as ISO 31000 [11], NIST SP800-30 [12], but there is a need to have one that is aligned with the ISO/SAE 21434.

This work aims to fill the above gap by proposing a novel residual risk management framework. The framework considers the qualitative and recurrent process to reduce the residual risk to an acceptable level while considering the standard risk management practices. Possible threats of a component will be identified from the exploitable vulnerabilities, whereas the attack trees will be generated from the given architecture. Appropriate defenses will be applied against the generated attack paths to observe the residual risk. The contribution of this paper includes the proposed residual risk management framework considering continual risk assessment. We will also present a method to calculate the residual risk of a system. Lastly, we will apply the proposed method to a headlamp system example from ISO/SAE 21434 and evaluate its benefits.

Table 1: Threat Modeling Methods applicable to Automotive

Name	Definition	Reference Method	Required detail level
ATA Model [22]	Visualizing threats against a system in the form of a tree.	Attack Tree	Detailed system design
SW Vulnerability Analysis	Examining software to avoid vulnerabilities		Code examination
FMVEA [23]	Failure Mode and Failure Effect model for both safety and security	STRIDE	Detailed system design
SAHARA [24]	Combination of HARA and STRIDE, traces impact of security breaches on system safety.	STRIDE	High level design
SHIELD	Security, Privacy and Dependability assessing method.		Detailed system design
CHASSIS	Analysis Trade-off between safety and security.	Use Case Diagram	High level Design
BDMP	Combine Fault tree and Attack tree.	Attack Tree	Detailed system design
Threat Matrix [25]	Threat data is presented in the form of threats	FMEA	Detailed system design
BRA	10 binary decisions in the form of questions		High level design

The rest of the paper is structured as follows. Section 2 gives a brief introduction to ISO/SAE 21434 standard, requirements of the risk management framework, and related work. Section 3 walks through the proposed risk management framework and headlamp example, borrowed from ISO/SAE 21434. In Section 4 we discusses the scope of our work with respect to available methods. Finally, Section 5 gives a conclusion about the paper and discusses ways we might extend this work.

2 Background

This section will discuss the requirements of the risk management framework. Furthermore, it includes a brief introduction to ISO/SAE 21434 and summarizes the related work.

2.1 Requirements of Risk Management Framework

The induction of new technologies in the modern vehicle has revolutionized the automotive industry. Risk management frameworks play a vital role in building a more robust and resilient system. We have identified the following requirements of the risk management framework for the automotive based on work from [13, 14].

- The framework must follow well-established standards and practices for risk management such as ISO 31000 [11], NIST SP800-3 [12].
- It should be a comprehensive framework that ensures that the risk of the automotive system is managed effectively and efficiently.
- The risk management framework should be generic so that it can support the relations and entities involved in the process not bound to specific domain.

- It must be scalable as new interfaces and technology are integrated in the automotive domain.
- The framework should support automation and parameterization.
- It should also integrate the assurance to verify the effectiveness of the applied countermeasures.
- It should be a continual process so it can adopt any change in the respective environment.
- The risk management framework should handle the propagation of risk between different entities.
- There should be a mechanism that can give intuitive ranking indicators to measure the results obtained from the risk management framework considering the acceptable criteria.

2.2 ISO/SAE 21434

As discussed earlier, Connected and Autonomous Vehicles (CAV) have introduced new targets for hackers and therefore risks for users concerning the security and safety of a vehicle. To deal with these emerging problems, SAE and ISO have invested in the development of an industry Standard ISO/SAE 21434 [15] that is a successor of SAE J3061 [16]. The purpose for creating ISO/SAE 21434 [15] was to define a structured process for cyber-secure design, reducing risks of a successful attack and providing information regarding how to react while facing cybersecurity threats. To assess the risk of threats on a system there are various risk assessment methods which are discussed in detail in clause 15 of ISO/SAE 21434. Considering the vehicle life cycle for safety that is adopted from ISO 26262 [18], there are three major phases: the concept phase, product development phase, and production, operation, and maintenance phase. In the concept phase, an item is defined. An item represents a system or number of systems that are implemented in a vehicle considering ISO 26262 [18]. There are nested models in the product development phase, such as a) product development at the system level. b) product development at the hardware level. c) product development at a software level. The production, operation, and maintenance phase has to ensure that cybersecurity specifications are implemented in the development phase. It ensures that implemented processes prevent new vulnerabilities from being part of the system. Continual monitoring and incident response handling is also done in this phase.

2.3 Related Work

Cybersecurity engineering standards were developed in several projects, including EVITA and HEAVENS. The EVITA project [19] proposed a method for risk assessment for automotive that utilized the generic approaches from ISO/IEC 18045 [18]. Later on, it and HEAVENS were incorporated in SAE J3061 [20] - The Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. It was stated by the HEAVENS researchers in 2016 that EVITA was the project that made

the first move towards risk assessment in the automotive industry. The National Highway Traffic Safety Administration (NHTSA) [21] proposed a composite threat model designed for the automotive industry in 2014. SAE J3061 [20] was released in 2016, and EVITA and HEAVENS are recommended threat models in it. A few other mentioned models apply to automotive systems, such as Attack Tree Analysis and Software Vulnerability Analysis. A few other methods are not mentioned in SAE J3061 but those apply to automotive systems. A brief overview of the other methods can be found in Table 1.

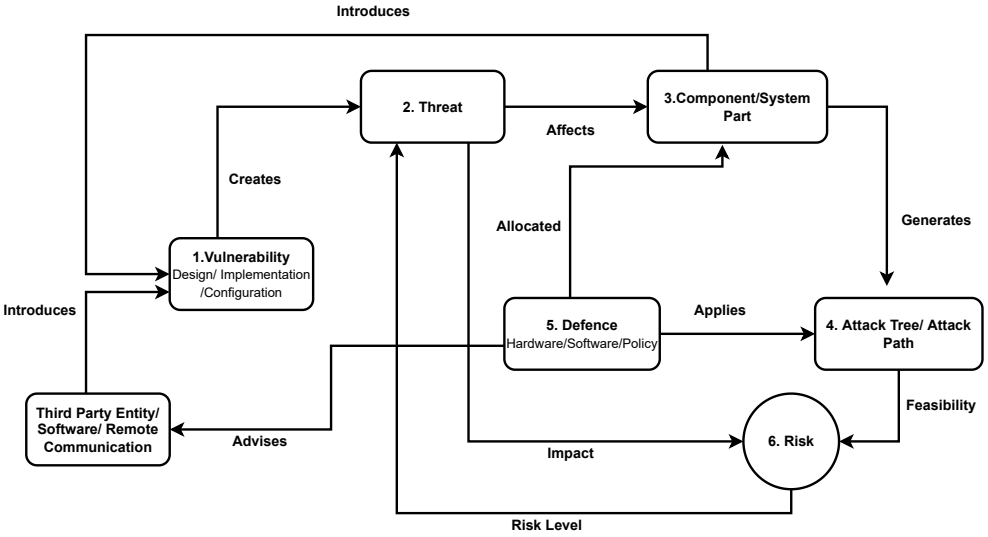


Fig. 1: Residual Risk Management Framework

The risk management process relies upon the set of guidelines and principles that can be followed across the organization to support design, implementation, integration, and evaluation. ISO 31000 [11] is an example of a general risk management framework. Cyber-physical systems are a complex integration of components required to perform respective functionality. This complex integration also increases the cyber risk of the system because there is a significant chance of an attack on the closely connected components. In [26] the authors proposed a risk assessment method for cyber-physical systems that can help to analyze the risk propagation as well as aggregation. In addition to risk assessment, they have proposed a technique utilizing evolutionary programming to select the appropriate control measures from the available list of measures. In paper [26], the authors have presented an integrated risk management framework that assesses and proactively manages the risk in a cyber-physical system. They followed the existing risk management practices and principles, such as identifying assets and then evaluating the effect of vulnerabilities over that asset. They have used the

power grid system as an example and followed the standard to determine the risk level and the impact of threats and vulnerabilities to the assets.

3 Residual Risk Management Framework

This section describes the proposed residual risk assessment framework for automotive systems, while considering ISO/SAE 21434. The framework is based on the taxonomy shown in Fig. 1.

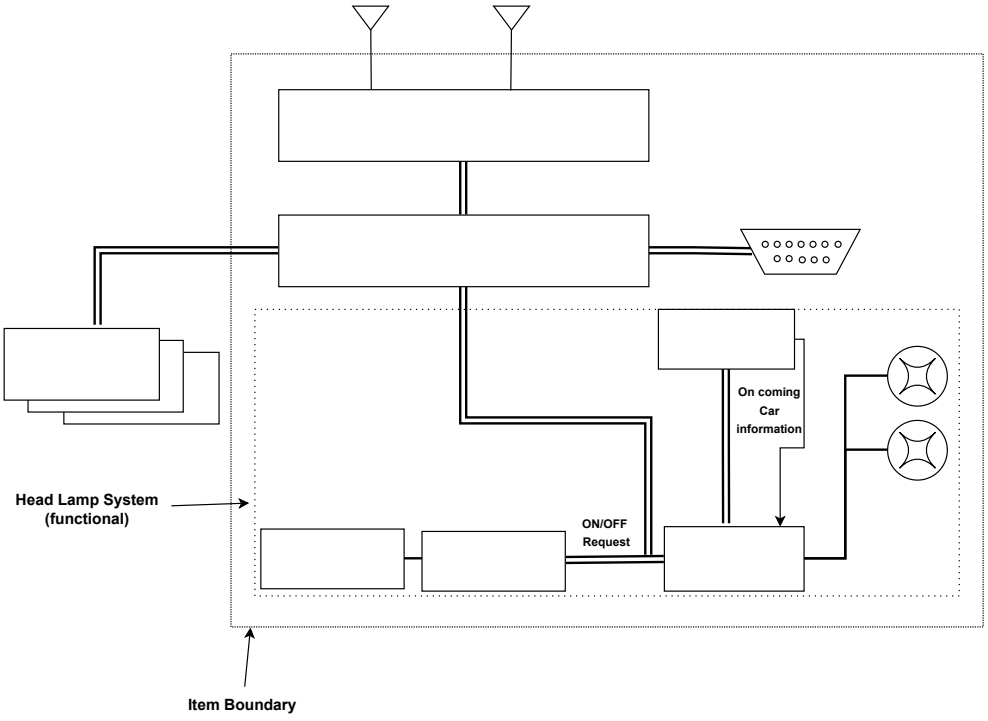
Vulnerabilities: The automotive system is the composition of multiple integrated components produced by different members of the Original Equipment Manufacturers (OEMs) supply chain. It is difficult to maintain the same level of assurance in such a widespread industry; that is why there is always a possibility of weaknesses in a system. Weakness can be in the system's design, implementation, or configuration. This weakness will become a vulnerability when someone can exploit it. Vulnerabilities are also possible due to adding some new component or defense in a system.

Threats: Vulnerabilities become threats when someone exploits them as shown in Fig. 1. It is essential to understand that every threat is for a specific component. Considering an example of GPS spoofing attack that can be done remotely requires broadcasting of synchronized signal with the original signal after that, the spoofed signal's power is increased. Later on, the target position is moved away from the original location. This threat is possible due to a vulnerability: GPS devices are programmed to follow high power signals.

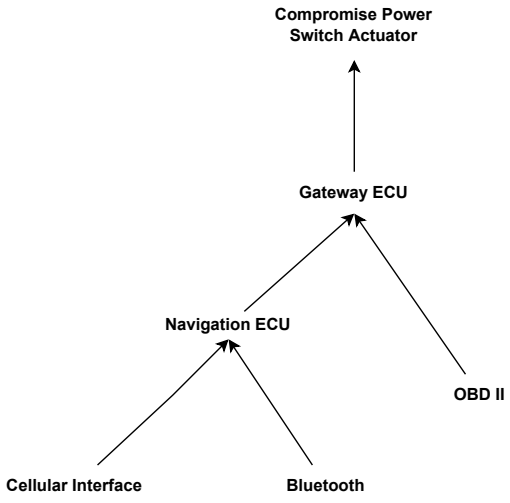
Components: To secure a component, we need to understand the possible ways to compromise it. We can generate attack trees to have a view of the possible ways. It is also possible to generate an attack tree if we know the architecture of a component. Considering the headlamp example from Fig. 2(a), where we know the architecture of the headlamp, we can generate attack trees shown in Fig. 2(b).

Attack Path: Every attack path has the feasibility of exploitation. Feasibility would be high or low considering the complexity of an attack path. There is a possibility that an attack path is relatively short, but its complexity is high. Therefore, we consider the feasibility of the attack path as a factor to calculate risk as suggested in ISO/SAE 21434.

Defense: To avoid those threats becoming an attack, defenses can be applied that could be an integration of new hardware or fixing some software bug. It is also possible that the cause of the threat is some third-party entity or software. In that case, we advises some policy for interaction. In Fig. 1., we can observe that defenses are connected to components and attack paths because one defense is for some specific component. It is connected to attack paths because it will help to visualize the placement of defense in the attack path. As discussed earlier, due to the widespread nature of the automotive industry, there is always a possibility of introducing new weaknesses that will become vulnerabilities into a system. There is also a possibility that applied defenses might introduce new vulnerabilities in a system, as shown by the link from component to the vulnerabilities in Fig. 1.



(a) Head Lamp Architecture



(b) Attack tree for headlamp system

Fig. 2: Example from ISO/SAE 21434 Annex-H [15]

We can calculate associated risk to a component of specific by considering the attack feasibility and the impact associated with that threat. The risk value will change after applying defenses. The efficacy depends upon the effectiveness of the defenses. There is also a possibility that the risk might increase than the acceptable level; therefore, if the risk level is high, we will consider it as a threat, as shown by a link from risk to threat in Fig. 1. We will calculate the residual risk by finding differences before and after applying defenses on the possible threats using flow graphs as suggested in [10].

According to the standard ISO/SAE 21434, we should select a risk treatment option when we have identified the risk. a) Avoidance of risk: we need to remove or update that component in this case. b) Risk reduction: we need to add suitable defenses to reduce risk. c) Sharing risk: sharing the risk with another party through contract. d) Retaining risk: takes responsibility for effects if a particular risk causes any damage. Our framework will only apply in the case where we consider risk reduction as the risk treatment option.

3.1 Residual Risk

To calculate the residual risk of a system, firstly, we need to compute the initial risk to a system. Considering the applicability of different threats on one asset, there is a need to examine all non-functional properties that can be compromised. Calculation of initial risk requires the following steps.

- Asset assessment
- Threat assessment
- Impact and Likelihood calculation

One system part/ component might have multiple assets A_i those are required to be identified first. We could have various assets in an automotive system such as CAN frame, firmware, etc. After identification of assets, there is a need to associate the non-functional properties P_i i.e (confidentiality, integrity, availability) those can be exploited given identified threats.

Every threat has associated severity/impact to it. Let us consider we have an asset A_i, and if its property P_i is being violated, then severity or impact I of that would be

$$Impact(I) = f\left(A_i, P_i\right) \tag{1}$$

The impact will be quantified as a score(1-4) for severe, major, moderate, negligible, respectively. If the impact of the threat is high, it means it can cause more damage to a system if it is successful.

To calculate risk to a system, it is essential to understand that considering the impact of a threat, what is the feasibility/likelihood of a threat T_i. The likelihood L_i of a threat on an asset will be

$$Likelihood(L) = f\left(A_i, P_i, T_i\right) \tag{2}$$

The risk is calculated as a lookup matrix in ISO/SAE 21434, and can also be defined by company (OEM). The total risk associated with an asset can be

considered as

$$R(_{A,P}) = \sum_{A_i,P_i,T_i} R(_{A_i,P_i}) \tag{3}$$

The residual risk is risk remaining after applying appropriate control measures against threats, and that would be updated risk as R_u. The residual risk would be

$$ResidualRisk = R_i - R_u \tag{4}$$

3.2 Head Lamp Example

We are considering a headlamp example from ISO 21434 annex H. The item boundary of this system is shown in Fig. 2(a) redrawn from ISO 21434. Navigation ECU is connected with Bluetooth and a cellular interface; those are two attack surfaces that can be used for compromising the headlamp system remotely. The other attack surface is the OBD-II connector which needs physical access to the system.

To specify the assets, we will follow the asset identification process as suggested in ISO 21434. In this example, two assets are specified, i.e CAN frame and firmware. Multiple damage scenarios are mentioned in the standard, whereas the impact of each scenario is identified. The impact rating process includes impact category as well as impact level. In the scope of this paper, we are only considering the damage scenario with a severe impact rating. The headlamp ON/OFF message malfunction is a severe safety hazard while night driving. The integrity and availability of the CAN frame are compromised in such a case. The next step will be an attack path generation and attack feasibility rating. Majorly three possible attack surfaces i.e, cellular, Bluetooth, and OBD-II can be exploited. The attack paths can be seen in Fig. 2(b). The attack path with the highest feasibility is the one with the cellular interface as an attack surface. Its feasibility value is high because an attacker has to be in a car or very close to a moving car for the other two attack paths, which does not have a high feasibility. As discussed in equation (3), the risk value will be determined as we have an impact and the likelihood of the attack paths. The next step in standard is suggesting to reduce the risk. We will reduce the risk by applying appropriate defense while considering their effectiveness.

3.3 Calculating Residual Risk Using Flow Graphs

We can model the residual risk problem as a maximum flow problem using flow graphs. In the maximum flow problem, we have to route the flow as much as possible from source to sink. Flow graphs are used in this problem, and we will be using them for calculating the residual risk of a system. A flow graph is a directed graph in which the arch has capacities indicating the link's upper bound. Flow originates from sources and ends at the sink without any dispersion in flow graph.

We define a graph G=(V, E, c) where V is composed of assets A_i, properties P_i, source s, sink t. E is associated with edges, and c is the capacity of each link.

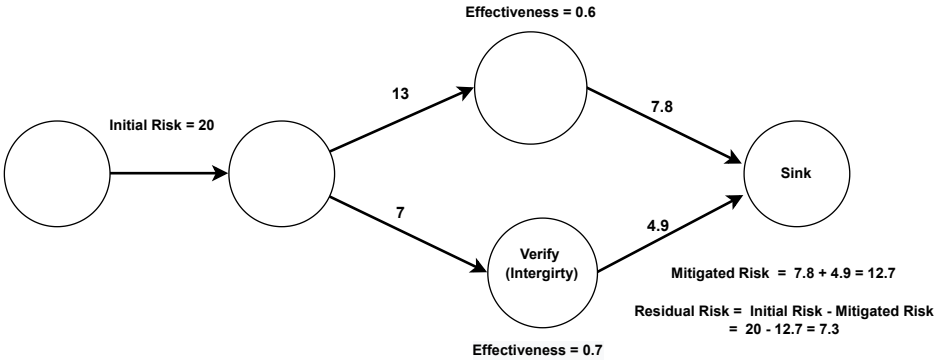


Fig. 3: Residual Risk Calculation using Flow Graph

We model a flow graph from standard practices; s and t are added to select the start and end of the flow graph. The remaining nodes follow the property of the bipartite graph.

We consider total risk as an inward flow of the flow graph, as shown in Fig. 3. Defense vertices should reduce the flow of risk after passing through them as every defense has respective effectiveness. So we can obtain the mitigated risk by multiplying the effectiveness of control measures against attacks. We have drawn Fig. 3. from the assets taken from the headlamp example in section 3.2. The asset is a CAN frame of the headlamp system, whereas the control measures are verification and anti-spoofing to improve the integrity and availability of the whole system. The incoming flow is 20, and the effectiveness of defenses is 60% and 70%. These mechanisms mitigate risk, and the remaining risk that reaches the sink is 7.3 as calculated using Equation 4.

3.4 Evaluation

To evaluate the proposed framework, we can compare it with the requirements of the risk management framework to understand that it satisfies all of the requirements as discussed in section 2.1.

- Our framework is well-aligned and following NIST-SP 800 as it considers the whole life cycle. Our proposed approach is also aligned with ISO 21434.
- Our framework is comprehensive enough to deal with risk reduction considering it as a risk treatment decision. In the scope of this work, our framework does not deal with other risk treatment decisions, e.g., risk avoidance, risk sharing, and risk retaining.
- Our proposed approach is quite generic as we can apply it to other domains, e.g., Cyber-Physical Systems.

- The proposed framework is scalable. We can consider multiple defenses and attacks against any type of threat. Our work focusses on risk reduction as the risk treatment option considered.
- In further work we will be designing automated and algorithmic solutions for combining attacks trees and finding appropriate defenses, and our intention is that this framework will support automation.
- Considering the effectiveness of the countermeasures to select it against specific attacks, we will be integrating assurance techniques with our approach.
- Our framework follows a continuous process, as shown in Fig. 1.
- We will be combining attack trees to improve visualization; this fusion will allow us to understand and handle the risk propagation from one asset to another.
- To calculate the severity level of any threat, we are using the look-up matrix discussed in ISO 21434 that gives the ranking indicators about the threat. In the future, we will be looking at graph-oriented techniques for ranking.

4 Discussion

Our proposed approach strictly follows the guidelines provided by ISO 31000 as discussed in section 2.1, a general framework that guides us to follow a set of standard practices to do a system's risk assessment. CAVs are one of the complex CPS, and our approach is generic enough that we can use it to do the risk assessment of other CPS. Currently, we are only using the application of automotive in the scope of this paper. There are a few other studies, such as [26], in which authors have proposed the risk assessment framework aligned with standards. [26] follows a manual approach to identify the vulnerabilities and appropriate countermeasures using the approach of the American National Highway Traffic Safety Administration; however, we are considering an automated process to generate attack trees and determine appropriate controls assessing their effectiveness. We integrated a continual process to reduce the risk to an acceptable level. Another work, [29], did a risk assessment for automotive but they did not consider residual risk. The major challenge in our work is to quantify threats and the effectiveness of controls as numerous defense mechanisms are proposed in the literature. Still, evaluating the countermeasures for effectiveness in some environments is very rarely available. This knowledge gap introduces a big challenge in our approach. To a great extent this approach requires considerable domain knowledge, and it will also complement TARA for better assessment.

5 Conclusion and Future Works

Identifying and mitigating risk is essential in developing the automotive system. Considering the remaining risk after applying defenses is vital as defenses are not usually 100% effective. In this paper, we have presented a modern risk management framework aligned with standards and requirements. It incorporates

the impact of the threats, the feasibility of the attacks, and vulnerabilities introduced by new defenses and third parties. Our approach is centered around the non-functional properties of the automotive system. We have presented the work by discussing it using the example available in ISO/SAE 21434. We have evaluated our proposed framework with the requirements of the risk management framework discussed in section 2.1 and found out that it is closely aligned with requirements. In the future, we will be increasing that alignment by introducing algorithms for attack tree combinations for some other examples that will lead us towards risk propagation, scalability, and a broader view of the whole system. We will also be considering the method to identify the most suitable defenses against attacks.

References

1. Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., ... & Yu, S. (2019). An overview of attacks and defences on intelligent connected vehicles. arXiv preprint arXiv:1907.07455.
2. Sommer, F., Dürrwang, J., & Kriesten, R. (2019). Survey and classification of automotive security attacks. Information, 10(4), 148.
3. Blank, R. M. (2011). Guide for conducting risk assessments.
4. Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.
5. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.
6. https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes.
7. Liedtke, Thomas. "Risk assessment according to the ISO/SAE 21434: 2021." (2021).
8. https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/.
9. Birch, John, Roger Rivett, Ibrahim Habli, Ben Bradshaw, John Botham, Dave Higham, Peter Jesty, Helen Monkhouse, and Robert Palin. "Safety cases and their role in ISO 26262 functional safety assessment." In International Conference on Computer Safety, Reliability, and Security, pp. 154-165. Springer, Berlin, Heidelberg, 2013.
10. Anisetti, Marco, Claudio A. Ardagna, Nicola Bena, and Andrea Foppiani. "An Assurance-Based Risk Management Framework for Distributed Systems." In 2021 IEEE International Conference on Web Services (ICWS), pp. 482-492. IEEE, 2021.
11. Risk management – Guidelines," International Organization for Stan-dardization, Geneva, CH, Standard, February 2018
12. Joint Task Force Transformation Initiative, "Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST Special Publication (SP) 800-30,Rev. 1, September 2012.
13. Nurse, Jason RC, Sadie Creese, and David De Roure. "Security risk assessment in Internet of Things systems." IT professional 19, no. 5 (2017): 20-26.
14. "Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies," European Telecommunications Standards Institute, Sophia Antipolis Cedex, France, Standard, January 2016.
15. ISO/IEC, ISO/SAE DIS 21434 — Road Vehicles — Cybersecurity Engineering,International Organization for Standardization, Geneva, CH, 2020.
16. SAE International, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,Tech. Rep. J3061, SAE International, 2016

17. ISO - International Organization for Standardization. ISO 26262 Road vehicles. Functional Safety Part 1–10 (2011)
18. ISO/IEC, ISO/IEC 18045:2008(E): Information technology – Security techniques–Methodology for IT security evaluation, International Organization forStandardization, Geneva, CH, 2008.
19. The EVITA consortium, EVITA Threat and risk analysis, 2009, https://www.evita-project.org.
20. SAE International, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,Tech. Rep. J3061, SAE International, 2016.
21. C.McCarthy, K. Harnett, A. Carter, Characterization of Potential Security Threatsin Modern Automobiles: A Composite Modeling Approach, National HighwayTraffic Safety Administration, 2014.
22. Schneier, Bruce. "Attack trees." Dr. Dobb's journal 24, no. 12 (1999): 21-29.
23. Schmittner, Christoph, Zhendong Ma, and Paul Smith. "FMVEA for safety and security analysis of intelligent and cooperative vehicles." In International Conference on Computer Safety, Reliability, and Security, pp. 282-288. Springer, Cham, 2014.
24. Macher, Georg, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Kreiner. "SAHARA a security-aware hazard and risk analysis method." In 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 621-624. IEEE, 2015.
25. McCarthy, Charlie, Kevin Harnett, and Art Carter. Characterization of potential security threats in modern automobiles: A composite modeling approach. No. DOT HS 812 074. United States. National Highway Traffic Safety Administration, 2014.
26. Kure, Halima Ibrahim, Shareeful Islam, and Mohammad Abdur Razzaque. "An integrated cyber security risk management approach for a cyber-physical system." Applied Sciences 8, no. 6 (2018): 898.
27. Number of Automotive Ecus Continues to Rise. Available online: https://www.eenewsautomotive.com/news/number-automotive-ecus-continues-rise
28. Koscher, Karl, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy et al. "Experimental security analysis of a modern automobile." In 2010 IEEE symposium on security and privacy, pp. 447-462. IEEE, 2010.
29. Wang, Yunpeng, Yinghui Wang, Hongmao Qin, Haojie Ji, Yanan Zhang, and Jian Wang. "A Systematic Risk Assessment Framework of Automotive Cybersecurity." Automotive Innovation 4, no. 3 (2021): 253-261.