vehicles

Article

STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System

Popy Das [1], Md. Rashid Al Asif [1,*], Sohely Jahan [1], Kawsar Ahmed [2,3,4,*], Francis M. Bui [2] and Rahamatullah Khondoker [5]

[1] Department of Computer Science and Engineering, University of Barishal, Barishal 8254, Bangladesh; pdas17.cse@bu.ac.bd (P.D.); sojahan@bu.ac.bd (S.J.)
[2] Department of Electrical and Computer Engineering, University of Saskatchewan, 57 Campus Drive, Saskatoon, SK S7N 5A9, Canada; francis.bui@usask.ca
[3] Health Informatics Research Lab, Department of Computer Science and Engineering, Daffodil International University, Daffodil Smart City, Dhaka 1216, Bangladesh
[4] Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Santosh, Tangail 1902, Bangladesh
[5] Department of Business Informatics, Faculty of Mathematics, Natural Science & Data Processing (MND), THM University of Applied Sciences, 61169 Friedberg, Germany; rahamatullah.khondoker@mnd.thm.de
* Correspondence: mraasif@bu.ac.bd (M.R.A.A.); k.ahmed.bd@ieee.org or k.ahmed@usask.ca or kawsar.ict@mbstu.ac.bd (K.A.)

Abstract: In modern automobiles, the infotainment system is crucial for enhancing driver and passenger capabilities, offering advanced features such as music, navigation, communication, and entertainment. Leveraging Wi-Fi, cellular networks, NFC, and Bluetooth, the system ensures continuous internet connectivity, providing seamless access to information. However, the increasing complexity of IT connectivity in vehicles raises significant cybersecurity concerns, including potential data breaches and exposure of sensitive information. To enhance security in infotainment systems, this study applied component-level threat modeling to a proposed infotainment system using the Microsoft STRIDE model. This approach illustrates potential component-level security issues impacting privacy and security concerns. The study also assessed these impacts using SAHARA and DREAD risk assessment methodologies. The threat modeling process identified 34 potential security threats, each accompanied by detailed information. Moreover, a comparative analysis is performed to compute risk values for prioritizing treatment, followed by recommending mitigation strategies for each identified threat. These identified threats and associated risks require careful consideration to prevent potential cyberattacks before deploying the infotainment system in automotive vehicles.

Keywords: cybersecurity; infotainment; threat modeling; risk assessment; threat mitigation

check for updates

Citation: Das, P.; Asif, M.R.A.; Jahan, S.; Ahmed, K.; Bui, F.M.; Khondoker, R. STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System. *Vehicles* **2024**, *6*, 1140–1163. https://doi.org/10.3390/vehicles6030054

Academic Editor: Mohammed Chadli

Received: 27 April 2024
Revised: 23 June 2024
Accepted: 28 June 2024
Published: 30 June 2024

1. Introduction

The infotainment system has integrated information and technology to enhance the safety and convenience of the drivers and passengers of automotive vehicles. The integration consists of various factors such as passenger's mobile devices, surrounding vehicles, remote servers, drivers, traffic infrastructure, environment, and so on. It is predicted that nearly all new cars made by 2035 will have internet connectivity [1]. The integration can provide many advantages, such as access to various information as the vehicle is always connected to the internet. But the problem is the system becomes vulnerable to cyberattacks from adversaries [2,3]. The interconnection of the wider range of services with automobiles increases security vulnerabilities and incidents of car hacking are being reported more frequently [4]. All these facts motivate the emphasis on security research in automotive vehicles.

The automotive vehicle's infotainment system intricately connects to complex networks, forming a sophisticated ecosystem that enhances the driving experience. These systems seamlessly integrate with various networks, including the internet, internal vehicle area networks (VANs) connecting electronic control units (ECUs), car sensors, and wireless technology like Wi-Fi as illustrated in Figure 1. Internet connectivity enables real-time navigation updates, streaming services, and over-the-air software updates. Internal VANs ensure efficient data exchange among different vehicle components, while Wi-Fi connectivity enables hands-free calling and media streaming with smartphones. Telematics systems utilize cellular networks for remote diagnostics and vehicle tracking, connecting to the cloud and using GPS for accessing location-related information. This network connectivity also facilitates communication with other vehicles, devices, and individuals. This intricate, heterogeneous network connectivity not only offers numerous features to drivers and passengers but also presents cybersecurity challenges, leading to continuous efforts to safeguard connected vehicles from potential threats.

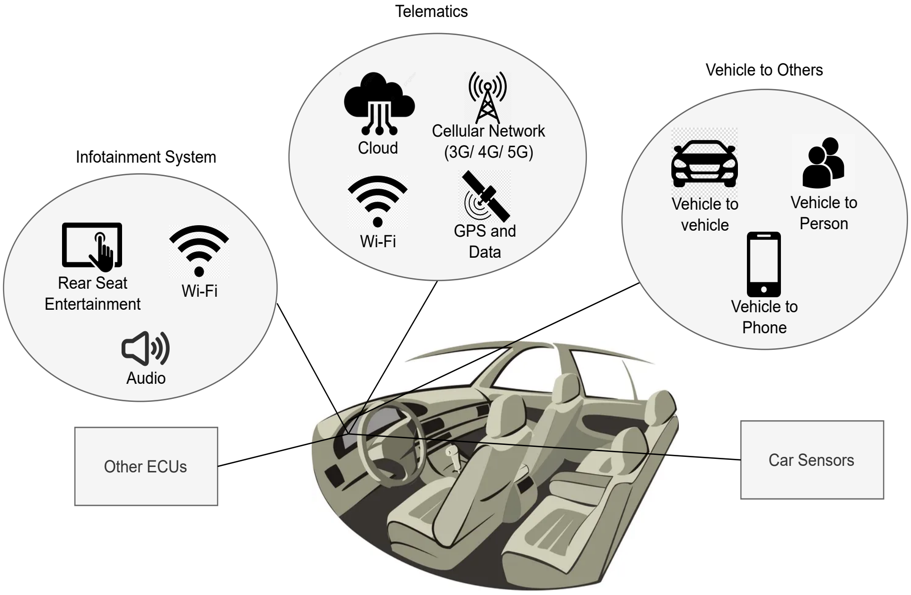

Figure 1. The heterogeneous connectivity of the infotainment system of an automotive vehicle.

The in-vehicle infotainment (IVI) system uses in-vehicle network services, including Wi-Fi connectivity, beside remote functionalities such as conventional navigation, radio playback, and multimedia functions to establish a link between the vehicle and the external world [5]. Because of the existence of these remote interfaces and interconnected services, the system might become susceptible to potential vulnerabilities. The adversaries might try to access the system's weaknesses by performing unauthorized manipulation from a remote location [6,7]. IVI system services were detected with a vulnerability as an adversary tried to attain root privileges and establish remote access through the Wi-Fi interface in [8]. Such access can result in manipulation of the system's configuration and the adversary might obtain access to sensitive user information [9,10]. As the users can access personal information through Bluetooth while driving, it can also be an attack surface for the adversary [11]. The existing countermeasures might not be sufficient to counter these forms of attacks.

The in-vehicle applications might face security challenges, especially those related to Inter-Component Communication (ICC), which have received concern in [12]. It is identified that malicious applications might be able to manipulate or deceive the system, resulting in the potential exposure of sensitive user data to unauthorized access. One vulnerability lies in the Controller Area Network (CAN) bus, where the broadcast transmission is at risk due to the network's bus topology. Messages are exchanged between ECUs across the entire network without authentication or encryption, posing a severe threat [13,14]. This vulnerability in the CAN bus could be exploited by adversaries, leading to potential vehicle attacks or even the complete takeover of ECUs through the transmission of spoofed messages [15]. In response to these challenges, researchers have developed frameworks aimed at mitigating these security risks.

An adversary can bypass safety-critical systems in vehicles, taking control of automotive functions and potentially compromising driving performance [16–18]. Khan et al. introduced a Microsoft STRIDE-based framework for cyber-physical systems that focuses on component vulnerabilities and their inter-dependencies, enhancing security [19]. However, addressing vulnerabilities in each component is crucial to prevent a loss of control over the entire security system. The incorporation of Threat Analysis and Risk Assessment (TARA) becomes crucial to maintaining an acceptable risk level by analyzing potential threats and implementing corresponding mitigation strategies [20]. Nevertheless, it is noteworthy that this framework primarily engages in theoretical threat analysis during the conceptual design phase and not during the security evaluation phase upon the vehicle's release. Based on these studies, it is needed to address these issues to enhance modern automotive security.

To improve the security of the IVI system, the paper has focused on identifying security vulnerabilities and threats using the Microsoft threat modeling tool STRIDE at the component level. It also focused on calculating risk value to determine the potential risk of the threats using risk assessment methodologies, specifically SAHARA and DREAD. It has provided a comparative analysis of the two methods and based on that it will be easy to understand which threats to prioritize first for mitigation. Finally, generalized mitigation strategies are provided that ultimately lead to an overall improvement in the IVI system's security [21,22].

The paper is arranged as follows: Section 2 outlines the research methodology, Section 3 outlines the details of different threat and risk assessment methodologies, Section 4 outlines the evaluation of threats and risk rating, Section 5 contains results and discussion, and finally, Section 6 directs the paper to the conclusion.

2. Methodology

The motivation of this research is to conduct threat modeling and risk assessment and provide mitigation strategies to counter potential threats to the IVI system. This is achieved by adopting the approach sequentially at the component level, as illustrated in Figure 2.

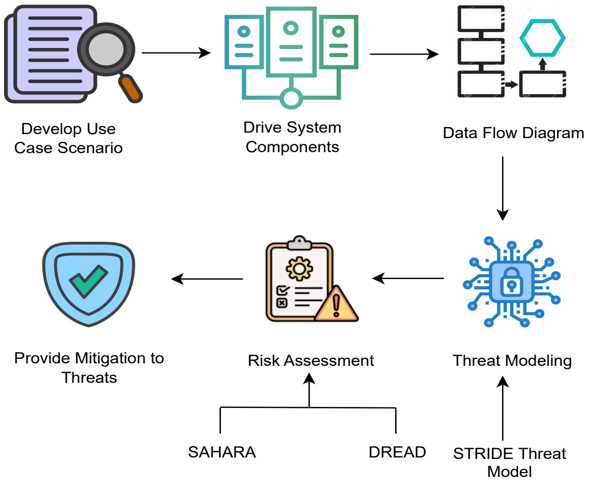

Figure 2. The step-by-step research methodology.

During the procedure, the use case scenario explains the way in which the attack may occur by the adversary. It is important to consider the components that are proposed to develop an infotainment system. To achieve the research objective, the first step involved the identification and outlining of the system components, followed by creating a data flow diagram (DFD). Subsequently, STRIDE is employed to conduct threat modeling, resulting in the generation of a threat report that outlines the identified threats. Additionally, risk assessment is carried out using SAHARA and DREAD methodologies, allowing for the calculation of risk values. Based on the identified threats, general defense mechanisms are proposed to enhance security.

2.1. Use Case Scenario

The onboard computer controls all the operations that occur in the infotainment system of the automotive vehicle. The driver may use Near Field Communication (NFC), Bluetooth, Wi-Fi or a cellular network (3G/4G/5G) to transfer data and information. The CAN bus is used by the onboard computer to communicate with the sub-sections of the automotive vehicle. While communicating with the outside world or transferring data, the data paths can be attacked by the adversary, as illustrated in Figure 3. An attacker is any person, including an insider, group, or entity that engages in adverse acts to damage, expose, disable, steal, obtain unauthorized access to, or otherwise misuse a resource [23]. The paper considered only NFC, Bluetooth, Wi-Fi, cellular networks and the CAN bus as attack surfaces but other surfaces can also be attack points for the attackers.

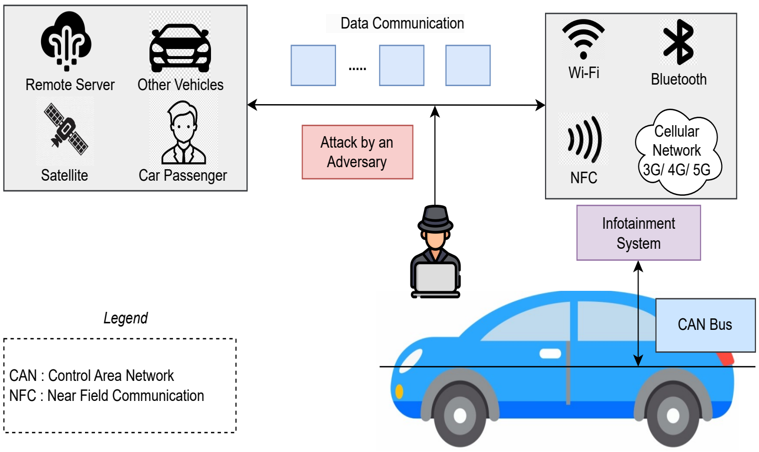

Figure 3. Use case scenario of research scope of an infotainment system of an automotive vehicle.

2.2. Proposed System Components

The key components of an infotainment system of an automotive vehicle with their functions and interactions are represented in Figure 4. Each component receives input and generates output to perform specific actions. The system includes an onboard computer, NFC, video buffer, touch screen controller, touch screen, rear screen, car audio system with microphone and speaker, camera, Wi-Fi and cellular network, digital radio, Bluetooth, USB interface, portable media player, CAN bus, car automation network, GPS and temperature sensor [24–27].

A typical IVI system is centered around an onboard computer that serves as the processor of the system, to which all other system elements are connected physically or wirelessly. The core human–machine interface (HMI) consists of a large touch screen placed on the dashboard for easier access by the driver [28]. NFC enables wireless communication between devices, allowing for secure transactions, and device connectivity with a simple touch. Video buffering involves pre-loading data segments for streaming video content, which are stored in a reserved section of memory. A touchscreen controller is a circuit that connects the touchscreen sensor to the touchscreen device. If the vehicle is equipped with a rear seat, passengers can play media from various sources on monitors located behind the front-seat headrests, functioning similarly to a smart TV [29]. The video buffer, touchscreen controller, and rear screen are connected to both the touch screen and onboard computer, allowing for data processing by the onboard computer and input control through the touch screen.

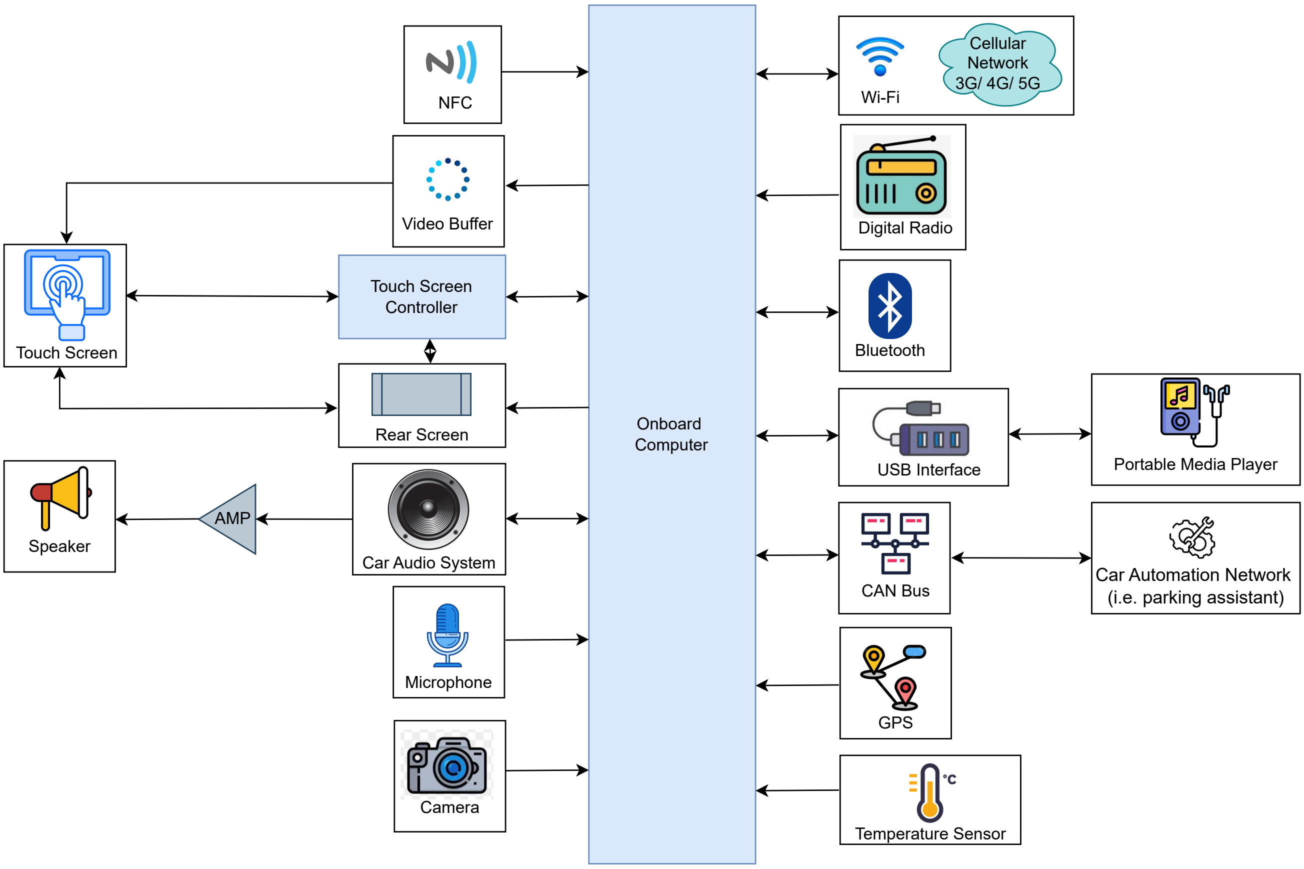

Figure 4. Proposed system components needed to design IVI system.

The car's audio system is equipped with a microphone and speaker for audio input and output by the user, allowing for multimedia playback and hands-free calling. The camera captures visual data for functions like rear view display and driver assistance [30]. The Wi-Fi and cellular network provide wireless connectivity for data communication and internet access, enabling access to web content, streaming, and email while driving [31]. The digital radio receives and processes digital signals for audio playback. Bluetooth enables wireless communication with external devices like smartphones, while the USB interface allows for data transfer and device charging.

The portable media player plays multimedia content from external devices [32]. The CAN bus facilitates communication among different ECUs in the vehicle, while the car automation network enables communication among different vehicle systems for automation and control. A car automation network can include a range of driver assist technologies such as parking assistant, lane keeping, driving assistant and traffic jam assistant, etc. These systems enhance driving convenience and safety, but the driver must continuously monitor the roadway and be ready to intervene immediately to maintain safety. Finally, the GPS and temperature sensor provide location and temperature data, which are used for navigation and climate control functions. Overall, the proposed infotainment system includes a wide range of components that work together to provide a better infotainment experience for users in the car.

2.3. DFD

In Figure 5, the DFD presents a detailed depiction of the system components under consideration for threat modeling and their associated data flows. It illustrates processes such as the onboard computer, NFC, Bluetooth, Wi-Fi and cellular network, and CAN bus, highlighting how they receive input data, perform actions, and produce output. The diagram shows data flows as arrows, representing the transfer of information between various system components, with processes symbolized by circles.

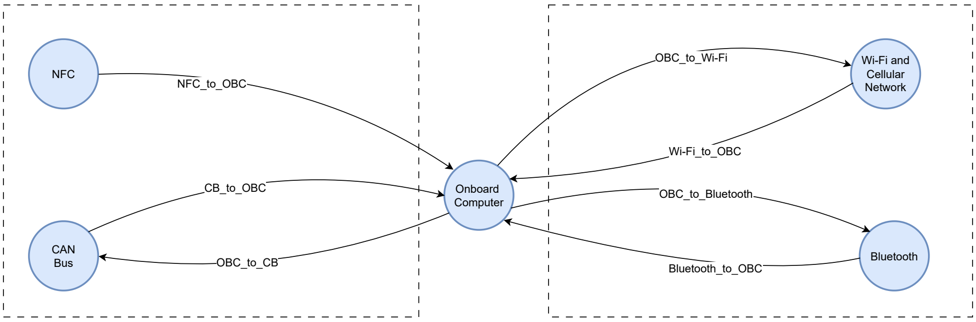

Figure 5. DFD based on the considered components of IVI system for threat modeling (considered components: onboard computer, NFC, Wi-Fi and cellular network, Bluetooth, CAN BUS).

3. Threat and Risk Assessment Methodologies

This section represents an overview of different threat modeling and risk assessment methodologies.

3.1. Threat Modeling Tools

Threat modeling is the method to identify, catalog, and prioritize dangers that assist in the way of development of effective defenses against threats. Simply, it aims to address questions like "Where could the system be vulnerable to threats?", "Which threats are most significant?", and "Where are the system's weaknesses?". According to a specialized document from the National Institute of Standards and Technology (NIST), a threat model encompasses the ability to address both offensive and defensive aspects of a logical entity. This entity could be data, a host, an application, a system, or an entire environment [33]. There are various threat models available such as PASTA (Process for Attack Simulation and Threat Analysis), Attack Tree, CVSS (Common Vulnerability Scoring System), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), VAST (Visual, Agile and Simple Threat modeling), LINDDUN (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance), STRIDE, and so on.

3.1.1. PASTA

PASTA, created by Tony UcedaVélez in 2012, is a framework for threat modeling that focuses on risks [34]. Although UcedaVélez categorizes it as risk-centric, PASTA takes an attacker-focused approach but ultimately produces results centered on assets. The framework aims to provide a comprehensive strategy for addressing risks from diverse and advanced threats.

PASTA is structured into seven stages, each comprising various activities. The first stage focuses on developing risk profiles by setting objectives that include business, financial, and operational goals, along with security and compliance requirements. This phase also involves conducting a Business Impact Analysis (BIA) and concludes with the creation of a comprehensive risk profile. In the second stage, the technical scope is outlined through a series of five activities designed to understand the technology framework and define the boundaries of the technical environment. This stage involves identifying dependencies across infrastructure, applications, and software. It includes cataloging software components, system-level services, and third-party infrastructure while ensuring the secure design's integrity.

In the third stage, the focus shifts to the internal structure of the software system, where the model analyzes its components and their interactions, encompassing both computational and data aspects. Moving to the fourth stage, the emphasis is on identifying threats and understanding their impact on the attack surface. In PASTA, threats are identified through analyst insights, threat intelligence reports, and known attack databases, prioritizing those proven in real-world scenarios.

In the fifth stage, the primary objective is to map identified vulnerabilities across various assets, including the application and its infrastructure, to the previously identified threats and attack scenarios. This process uses formal methodologies like threat trees to establish connections between threats and different categories of vulnerabilities. Once vulnerabilities are identified, they are systematically listed and evaluated using standard methods for enumeration and scoring. In the sixth stage, threats are specifically linked to vulnerabilities using an Attack Tree. This diagram outlines the conditions required for an attack to succeed, with the root representing the final outcome. The final stage synthesizes information from all previous steps. This involves assessing risks to business practices, identifying gaps in security controls, and determining how to effectively mitigate these risks.

PASTA involves key decision-makers and incorporates security input from various domains. It concentrates on understanding business impact, researching threats, and developing effective countermeasures [35]. However, its main drawback lies in its complexity and resource-intensive nature, which can overwhelm organizations with limited cybersecurity expertise and resources, potentially leading to analysis and inaccurate risk assessments.

3.1.2. Attack Tree

Attack Trees or attack graphs, devised by Bruce Schneier in 1999, were initially introduced as a standalone methodology and have since been integrated with other frameworks and approaches. They depict attacks on a system using a hierarchical structure, where the attack objective forms the root and the methods to achieve it extend as branches or leaves. Despite their effectiveness in identifying threats, creating adaptable Attack Trees can pose challenges. Nodes are meticulously analyzed to assess their impact, often employing data flow diagrams for clarity [23]. Constructing the tree typically involves iterative decomposition of the attack goal. Once all leaf nodes are identified, likelihood markers can be assigned, a step requiring thorough research into each aspect [36]. During the exploration of various methods to achieve the goal, it frequently becomes evident that multiple pathways exist to achieve it.

Attack graphs illustrate intricate attack scenarios but tend to be visually dense [37]. On the other hand, Attack Trees excel in simulating "what-if" scenarios but may encounter difficulties with interactive profiling [38]. In complex systems, Attack Trees can be constructed for individual components rather than the entire system. When utilized, Attack Trees facilitate making informed security decisions, assessing system vulnerabilities, and evaluating specific types of attacks [36]. Therefore, Attack Trees are especially valuable for assessing threats from an attack perspective [39].

3.1.3. CVSS

CVSS is a methodology utilized to assess the severity of vulnerabilities through numerical scores, providing a standardized system across various cyber platforms. It comprises three metric groups: Base, Temporal, and Environmental, each incorporating specific metrics [40]. Analysts assign values to these metrics to compute a CVSS score. The Base metrics produce a score between 0 and 10, which can be further adjusted by incorporating the Temporal and Environmental metrics. Additionally, a CVSS score is represented as a vector string, providing a concise textual summary of the values used in the calculation.

CVSS scores assess the fundamental attributes of a threat and the effects of risk factors, taking into consideration the time elapsed since the vulnerability was identified. It includes mechanisms for security teams to customize risk scores based on specific system configurations. Despite its widespread use, there are concerns about the transparency of score calculations and potential discrepancies among different experts' interpretations [41]. CVSS is commonly complemented by other threat modeling methodologies in practice.

3.1.4. OCTAVE

OCTAVE, launched by Carnegie Mellon University (Pittsburgh, PA, USA) and the CERT Division of the Software Engineering Institute (SEI), Pittsburgh, PA, USA in 2003, was crafted to create a streamlined and efficient process for assessing information security risks. It prioritizes minimizing resource investment in terms of time and personnel. In contrast to solely concentrating on technological risks, OCTAVE places significant emphasis on evaluating organizational risks.

The original OCTAVE methodology consists of three phases. Initially, it begins with the creation of asset-based threat profiles. This step entails identifying the valuable information assets within an organization, assessing their existing protection measures, and prioritizing them based on their importance. The most critical assets are selected, and their specific security requirements are documented. Moving to the second phase, the analysis team evaluates the organization's information infrastructure. Vulnerabilities are identified based on the insights gathered from the threat profiles developed in the first phase. Finally, in the last phase, the team devises a comprehensive security strategy and implements plans to mitigate risks associated with the protection of critical assets [42].

3.1.5. VAST

VAST, developed by Anurag Agarwal, is rooted in the commercial threat modeling platform, ThreatModeler, which heavily employs automation [43]. This method is suitable for large organizations, enabling comprehensive coverage of both software development lifecycles and entire infrastructures, yielding actionable results for various stakeholders. In addition to automation, VAST emphasizes integration and collaboration. In practice, VAST entails developing two types of models: application threat models and operational threat models. Application threat models utilize process flow diagrams to illustrate the architecture, whereas operational threat models adopt an attacker-centric perspective derived from these diagrams [35].

3.1.6. LINDDUN

LINDDUN, akin to STRIDE for security vulnerabilities, is a threat modeling technique emphasizing privacy and data security. It identifies privacy breaches by considering aspects like linkability, where attackers merge information to connect with specific systems. Identifiability associates potential subjects with items of interest. Non-Repudiation poses a threat where attackers make credible yet false claims that are difficult to refute. Detectability enables attackers to determine the presence of an item. Disclosure of information occurs when personal or sensitive data is unintentionally or intentionally exposed to unauthorized parties. Content unawareness poses a threat when users share excessive information, potentially aiding attacker identification or leading to erroneous user actions due to inaccurate data. Moreover, policy and content noncompliance indicate situations where personal and sensitive information might be disclosed despite the presence of privacy policies [44].

3.1.7. STRIDE

Microsoft STRIDE is a robust tool designed to identify cybersecurity threats, structured around an acronym that encapsulates six primary threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. These categories correspond to key security objectives: authenticity, integrity, non-repudiation, confidentiality, availability, and authorization. Using the STRIDE method, each component of an infotainment system undergoes thorough analysis, highlighting vulnerabilities susceptible to one or more threats from each category. This approach ensures comprehensive coverage of potential security risks across all system elements. Table 1 outlines the security properties linked to specific threat categories. As shown in Table 1, an external entity is exposed to two threat categories, a process is susceptible to all six threat categories, a unidirectional data flow contends with three threat categories, and a data store is vulnerable to three threat categories [45,46]. Notably, a component may confront multiple threats within a single category.

Table 1. Categorization of threats for each DFD element.

STRIDE Category	External Entity	Process	Data Flow	Data Store
Spoofing	✓	✓		
Tampering		✓	✓	✓
Repudiation	✓	✓		
Information Disclosure		✓	✓	✓
Denial of Service		✓	✓	✓
Elevation of Privilege		✓		

The STRIDE tool initiates the threat modeling process by presenting a DFD. Subsequently, a threat report is generated based on this DFD, encompassing information about threat categories, threat descriptions, and proposed mitigation strategies. For instance, Figure 5 illustrates an interaction involving STRIDE, specifically from NFC to the onboard computer (NFC_to_OBC). According to the STRIDE tool, three distinct threats are identified for this interaction: Denial of Service, Information Disclosure, and Tampering. As data flow from the NFC to the onboard computer, it can become a target for attackers in these ways. Similarly, threat reports are generated for other interactions within the infotainment system.

Despite the availability of these models, the paper used the STRIDE threat modeling tool. This choice is based on the tool's wide acceptance in both academia and industry, as well as its ability to identify threats at the component level. It is an open-source tool provided by Microsoft and is free [47]. It specifically focuses on identifying vulnerabilities and weaknesses in application security. A comprehensive analysis of these threat modeling methods is given in Table 2.

Table 2. Advantages and disadvantages of the threat modeling methods.

Threat Modeling Methodology	Attack Perspective	Advantages	Disadvantages
PASTA [34]	Risk centric	The model is DFD-based and suggests mitigation techniques.	The model is not automatic.
Attack Tree [36]	Attacker	The model identifies all possible attack vectors.	The model is not DFD-based and does not suggest mitigation techniques. The model lacks automation and may become overly complex for large systems.
CVSS [48]	Scoring	The model is automatic and provides a standardized method for evaluating vulnerabilities.	The model is not DFD-based and does not suggest mitigation techniques.
OCTAVE [42,49]	Operational risks	The model offers four threat trees to aid threat modelers in contemplating additional threats: human actors employing technical means, human actors utilizing physical access, technical problems, and miscellaneous issues.	The model is not DFD-based and automatic.

Table 2. *Cont.*

Threat Modeling Methodology	Attack Perspective	Advantages	Disadvantages
VAST [50]	Attacker	The model is DFD-based, automatic, and suggests mitigation techniques.	The requirement to create two types of models may increase the complexity and resource requirements for organizations.
LINDDUN [51]	Privacy concerns	The model is DFD-based, and suggests mitigation techniques.	The model is not automatic.
STRIDE [52,53]	Defender	The model is DFD-based and suggests mitigation techniques. The model is automatic and identifies vulnerabilities at the component level.	The results may be inconsistent.

3.2. *Risk Assessment Methodologies*

The complex architecture of modern vehicles can be vulnerable to cyberattacks as the entire system is a combination of the risks associated with each interconnected component [54]. Recently, researchers have brought to light 14 vulnerabilities found in the infotainment systems across various BMW series [55]. This underscores the urgent need to address the risks associated with threats throughout the entire development process. According to the definition provided by the NIST, the risk is defined as "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" [56]. Meanwhile, risk assessment is explained as "The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, resulting from the operation of a system" [57]. Various risk assessment methodologies provide frameworks for evaluating cybersecurity risks in automotive systems, including FMVEA, SHIELD, CHASSIS, SAHARA, DREAD, the TARA approach outlined in SAE J3061, and so on.

3.2.1. FMVEA

The FMVEA method which is based on FMEA (Failure Mode and Effects Analysis) is outlined in IEC 60812 [58]. It was developed by Schmittner et al. to address safety and security cause-effect analysis [59]. This methodology categorizes threats by quantifying threat agents, threat modes using the STRIDE model, effects, and attack probabilities. It starts by identifying critical assets and then analyzing these assets to identify potential failure modes and related vulnerabilities. The subsequent step involves assessing the potential severity of these failure modes and their impacts. Risks are prioritized based on their likelihood and impact, enabling the organization to address the most critical issues first. Mitigation strategies are then formulated and implemented to manage these prioritized risks. The process concludes with continuous monitoring and regular reviews to ensure the effectiveness of the mitigation strategies and to adapt to new risks or changes in the system. This structured approach helps organizations proactively enhance the security and reliability of their systems and processes.

However, a key limitation of FMVEA is its focus on analyzing single causes of an effect, potentially overlooking multi-stage attacks. To mitigate this, a combination of FTA (Fault Tree Analysis) and ATA (Attack Tree Analysis) is proposed to support FMVEA. Despite its effectiveness, FMVEA's reliance on FMEA makes it unsuitable for early development phases, such as those covered in TARA.

3.2.2. SHIELD

SHIELD is a methodology developed through a European collaboration to assess the security, privacy, and dependability (SPD) of embedded systems. This security assessment framework is designed to identify, evaluate, and mitigate potential threats to a system or organization. It employs a multi-metric approach to assess the SPD level of a system, evaluating it against predefined goals tailored to different use cases. The primary aim of SHIELD is to analyze different system configurations and select those that meet or exceed these objectives. However, the method becomes more effective with increased details and variants of a system, making it less suitable for the early design phase TARA [60].

3.2.3. CHASSIS

The CHASSIS method is a structured framework employed for assessing and managing the security of information systems. It integrates safety and security methodologies to offer a comprehensive assessment approach. CHASSIS integrates the modeling of misuse cases and misuse sequence diagrams within UML behavior diagrams, a process that may escalate modeling costs during early development phases. The method is designed to blend safety and security considerations into trade-off analyses, assessing the interdependencies or independence of system features [60]. Emphasizing the integration of security measures into system design and operation, CHASSIS ensures they are robust and aligned with organizational goals. Continuous monitoring and updating of security measures are also prioritized to address evolving threats and system changes. However, CHASSIS provides a holistic approach to bolstering the security posture of information systems.

3.2.4. HEAVENS

TARA approaches from SAE J3061 encompass the HEAVENS security model and the EVITA method, tailored for automotive cybersecurity. HEAVENS utilizes Microsoft's STRIDE approach to assess threats and rank them through a rigorous risk assessment comprising the determination of threat level (TL), impact level (IL), and security level (SL). However, this method requires extensive analysis, especially in determining SL, which often prompts significant discussion on IL and TL factors. TL is assessed based on attacker expertise, system knowledge, opportunity window, and equipment factors. TL and IL together inform the SL and subsequent risk rankings [60]. HEAVENS utilizes a structured approach to evaluate both the functional and non-functional security aspects within embedded systems. It requires fewer classification efforts compared to the EVITA method.

3.2.5. EVITA

EVITA is a security process outlined in the EVITA project, proposing a security model for analyzing risks in vehicular IT security systems [61]. It incorporates ISO 26262 HAZOP analysis into Threat and Operability Analysis (THROP), which evaluates threats at a functional level. THROP utilizes Attack Trees to identify potential malicious behaviors and worst-case scenario outcomes, making it particularly suitable for analyzing features or systems in embedded automotive systems [60]. EVITA's primary objective is to safeguard electronic vehicle components from cyber threats by implementing robust security measures and industry-specific standards.

3.2.6. SAHARA

The SAHARA methodology integrates the automotive HARA (Hazard Analysis and Risk Assessment) approach with the security-oriented STRIDE framework. The SAHARA method employs a fundamental element from the HARA approach, specifically the definition of Automotive Safety Integrity Levels (ASILs), to evaluate the outcomes of the STRIDE analysis. Threats are assessed in a manner concerning ASIL quantification, considering the required resources (R) and expertise (K) to execute the threat, along with its threat criticality (T). Security threats that have the potential to compromise safety objectives (T = 3) can be handed over to the HARA process for further safety analysis [62].

Table 3 provides instances of resources, expertise, and threat levels for each quantification tier of K, R, and T values [60]. These three factors collectively define a security level

(SecL), as detailed in Table 4 [63]. This SecL aids in determining the appropriate number of countermeasures that should be taken into account.

Table 3. Examples illustrating the classification of K, R, and T values of security threats.

Level	Knowledge Example	Resources Example	Threat Criticality Example
0	No previous knowledge	No tools required	No impact
1	Basic knowledge of system	Standard tools, screwdriver	Partial service disruption
2	Proficient knowledge of internals with focused interests	Simple tools like sniffer, oscilloscope	Significant damage, manipulation of invoice and privacy
3		Advanced tools like bus communication simulators, flasher	High security impact possible

Table 4. SecL determination matrix—deriving the security level by evaluating the values of R, K, and T.

R	K	T			
		0	**1**	**2**	**3**
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

Color code: green indicates low threat criticality, yellow represents medium threat criticality, orange signifies elevated threat criticality, and red denotes high threat criticality.

3.2.7. DREAD

DREAD constitutes a method for assessing risk, where its name corresponds to five assessment criteria: damage, reproducibility, exploitability, affected users, and discoverability [64]. DREAD holds the potential for conducting a more comprehensive analysis of system design. The DREAD acronym delineates:

- Damage (D): Signifying the potential impact of an attack.
- Reproducibility (R): Indicating the ease of replicating the attack.
- Exploitability (E): Assessing the effort required to execute the attack.
- Affected Users (A): The number of individuals who are going to experience the impact.
- Discoverability (D): Measuring the ease of identifying the threat.

As illustrated in Table 5, the DREAD method's rating scheme for each threat involves assigning points from 1 to 3, with a cumulative of 15 points indicating the most severe risk.

The DREAD risk can be calculated as follows:

$$Risk = (D + R + E + A + D) \tag{1}$$

After summing up the scores, the outcome can vary within the 5–15 range. Subsequently, threats can be categorized: those with total ratings of 12–15 are considered high risk, ratings of 8–11 indicate medium risk, and ratings of 5–7 are considered low risk [65].

Table 5. DREAD model rating scheme (3 for high risk, 2 for medium risk, and 1 for low risk).

Rating	High	Medium	Low
Damage (D)	Extensive data loss, compromise of full system	Moderate data loss, potential compromise of personal or sensitive data	Limited data loss, minor information
Reproducibility (R)	Highly unlikely to be reproduced, requires extremely specific and uncommon circumstances	Possible to reproduce, but requires specialized knowledge or specific conditions	Easily reproducible with minimal effort
Exploitability (E)	Requires extensive knowledge, sophisticated tools and complex methods	Requires moderate technical skills, advanced tools and some effort	Requires basic technical knowledge and commonly available tools
Affected Users (A)	Many users affected, substantial impact on user privacy or security	Some users affected, potential inconvenience or minimal harm	Few users affected, limited impact on individuals
Discoverability (D)	Highly hidden, requires specialized expertise, extensive analysis, or insider knowledge	Hidden but discoverable with careful examination or targeted testing	Easily detected

Despite the availability of numerous risk assessment methodologies, the paper chose to utilize SAHARA and DREAD due to their ability to quantify the security impact on the development of safety-related automotive vehicles at the system level. These methodologies are particularly well suited for evaluating remote cybersecurity attacks that can impact the operation of the vehicle. A comprehensive analysis of these risk assessment methodologies is given in Table 6.

Table 6. Advantages and disadvantages of the risk assessment methods.

Risk Assessment Methodology	Application Phase	Advantages	Disadvantages
FMVEA [59]	System	The model identifies the effects of threats and attack possibilities.	The model is not suitable for concept phase as it can easily overlook multi-stage attacks.
SHIELD [60]	System	The model is a security, privacy and dependability assessing method.	The model is not suitable for early design phase.
CHASSIS [60]	Concept	The model uses HAZOP tables in combination with the BDMP (boolean logic-driven Markov Processes) technique.	The model requires modeling of misuse cases and misuse sequence diagrams.
HEAVENS [60]	System	The model utilizes the STRIDE threat modeling approach, providing enhanced support for estimating threat scenarios.	The likelihood of an attack is determined by evaluating the complexity involved in executing a particular attack scenario. In the conceptual phase, system architecture details and hardware/software components may still be subject to change or remain undetermined.
EVITA [60]	Concept	The model categorizes threats into various classes, including functional, safety, privacy, and operational severity.	The severity classification does not comply with the ISO 26262 standard and the accuracy of attack potential measure may not be determined.
SAHARA [60,63]	Concept	Combining STRIDE threat modeling, the model simplifies threat classification, requiring minimal effort and employing a simple quantification scheme.	The model might fail to account for multi-stage attacks.
DREAD [64]	Concept	The model is suitable for evaluating remote cybersecurity attacks and attacks that affect entire vehicle operations.	The model may oversimplify complex threat scenarios and overlook certain aspects of security.

4. Evaluation of Threats and Risk Rating

This section represents an overview of evaluating threats and the risks associated with the threats.

4.1. Analyzing Threats

Threat modeling is performed to assess the possibility of cyberattacks associated with the major data flows and processes in the DFD. It is assumed that the two sides that are marked in the trust boundary are safe. However, not all components of the DFD are analyzed for potential threats. An asset, within the context of threat modeling, denotes any valuable entity requiring safeguarding within a system or environment. Notably, the identified assets in the DFD include the onboard computer, NFC, Wi-Fi and cellular network, Bluetooth, and CAN bus.

The onboard computer functions as the system's central processor, linking all other system elements physically or wirelessly. Potential attacks could aim to disrupt availability, compromise information, data integrity, or breach confidentiality. Information and commands are transmitted through NFC, Wi-Fi and cellular network, and Bluetooth, while the CAN bus is responsible for communication with the ECUs in a vehicle. So, these points can be potential targets for unauthorized access by adversaries. Such access could lead to manipulation of the infotainment system, unauthorized data access, vehicle component control, or disruption of system operations, potentially resulting in availability issues and data loss. Therefore, it is crucial to acknowledge the possibility of security issues in the infotainment system of an automotive vehicle.

Threat modeling is not performed on video buffers, touch screen controllers, rear screens, touch screens, car audio systems, speakers, cameras, microphones, digital radios, GPSs, and temperature sensors because there is no function of data or file transmission. Additionally, it is also not performed on USB interfaces and portable media players because they have to be physically inserted into the system. Only the threats that cross the trust boundary are considered, which means onboard computer, NFC to onboard computer (NFC_to_OBC), onboard computer to Wi-Fi and cellular network (OBC_to_Wi-Fi), Wi-Fi and cellular network to onboard computer (Wi-Fi_to_OBC), onboard computer to Bluetooth (OBC_to_Bluetooth), Bluetooth to onboard computer (Bluetooth_to_OBC), onboard computer to CAN Bus (OBC_to_CB), and CAN Bus to onboard computer (CB_to_OBC).

4.2. Identified Threats

The paper employs the Microsoft threat modeling tool, STRIDE, for conducting threat modeling. Input for the tool includes a DFD, as depicted in Figure 5. Subsequently, in the tool, the option to create a custom report is selected based on the considered components and data flows. This action leads to the generation of a threat modeling report containing threat categories and descriptions. Figure 6 illustrates the implementation of threat modeling using the STRIDE tool. Utilizing the generated threat descriptions and categories, Table 7 is generated in this paper.

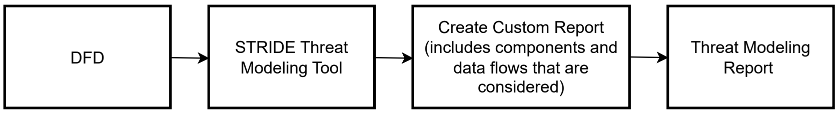
DFD
STRIDE Threat Modeling Tool
Create Custom Report (includes components and data flows that are considered)
Threat Modeling Report

Figure 6. Implementation of threat modeling using STRIDE tool.

Table 7. Listing of threats of components or interactions of infotainment system.

Components or Interactions	Threat No.	Threat Details	Threat Category
Onboard computer	1	An adversary can replicate the user actions to impersonate the process of onboard computer.	Spoofing
	2	An adversary may modify any given command and instruction resulting in the modification of the system such as NFC to onboard computer.	Tampering
	3	Without proper monitoring and control, the onboard computer can be subject to malicious exploitation.	Repudiation
	4	An adversary may steal or share any personal information with anyone, which may violate the user's privacy.	Information Disclosure
	5	In order to deny users of the onboard computer's services, an adversary may flood it with requests so normal traffic cannot be processed.	Denial of Service
	6	Without the required authorization, an adversary might obtain access to the onboard computer and carry out privileged operations.	Elevation of Privilege
NFC_to_OBC	7	Onboard computer may crash, halt, stop, or run slowly because of the fake requests sent by the adversary through NFC.	Denial of Service
	8	An adversary may interrupt data flowing across NFC to onboard computer with a snipping device and send a massive volume of data over the communication channel.	Denial of Service
	9	An adversary can intercept NFC data and use it to attack other parts of the system.	Information Disclosure
	10	An adversary may tamper the data flow from NFC to onboard computer in order to gain a particular advantage (not unlocking the door).	Tampering
OBC_to_Wi-Fi	11	Wi-Fi and cellular network may crash or halt due to the overflow of traffic causing not connecting to the network.	Denial of Service
	12	An adversary may interrupt data flowing across onboard computer to Wi-Fi and cellular network with a snipping device, and session hijacking may occur.	Denial of Service
	13	The data passing from onboard computer to Wi-Fi and cellular network may sniffed by the adversary causing the leakage of personal information.	Information Disclosure
	14	An adversary may tamper the data flow from onboard computer to Wi-Fi and cellular network and modify information to take remote control of the device.	Tampering
Wi-Fi_to_OBC	15	Onboard computer may crash, halt, stop, or run slowly due to the adversary making the resources and services unavailable.	Denial of Service
	16	An adversary can disrupt the onboard computer's performance by overwhelming its communication channels with a high volume of data, interrupting Wi-Fi and cellular network data flow.	Denial of Service
	17	The data passing from Wi-Fi and cellular network to onboard computer may sniffed by the adversary. This may lead to compliance violations.	Information Disclosure
	18	An adversary may tamper the data flow from Wi-Fi and cellular network to onboard computer and alter information.	Tampering

Table 7. *Cont.*

Components or Interactions	Threat No.	Threat Details	Threat Category
OBC_to_Bluetooth	19	Bluetooth may crash, halt, stop, or run slowly due to the adversary making the resources and services unavailable.	Denial of Service
	20	An external adversary may interrupt data flowing across a trust boundary by sending a large amount of data over communication channel.	Denial of Service
	21	The data passing from onboard computer to Bluetooth may sniffed by the adversary and disclose call logs or messages.	Information Disclosure
	22	An adversary may tamper the data flow from onboard computer to Bluetooth and alter information.	Tampering
Bluetooth_to_OBC	23	Onboard computer may crash, halt, stop, or run slowly because of the fake requests sent by the adversary.	Denial of Service
	24	An external adversary may interrupt data flow and keep the system busy to respond to fake requests.	Denial of Service
	25	The data passing from onboard computer to Bluetooth may sniffed by the adversary. Based on the type of Information Disclosure, this may lead to attacks on other parts of the system.	Information Disclosure
	26	An adversary may tamper with the data flow from Bluetooth to onboard computer and make unauthorized manipulation to the system.	Tampering
OBC_to_CB	27	An adversary may tamper the data flow from onboard computer to CAN bus and disclose the system information.	Denial of Service
	28	An adversary may interrupt data flowing across onboard computer to CAN bus in either direction.	Denial of Service
	29	An adversary may tamper the data flow from onboard computer to CAN bus and disclose the system information.	Information Disclosure
	30	An adversary can manipulate Bluetooth data to cause a Denial of Service or Elevation of Privilege on the CAN bus.	Tampering
CB_to_OBC	31	Onboard computer may crash, halt, stop, or run slowly due to the adversary making the resources and services unavailable.	Denial of Service
	32	An adversary may interrupt data flow across CAN bus to onboard computer in either direction.	Denial of Service
	33	An adversary can sniff the data flow, potentially enabling attacks on other system components based on the disclosed information.	Information Disclosure
	34	An adversary may tamper the data flow from CAN bus to onboard computer and alter information.	Tampering

By leveraging the STRIDE threat modeling tool, organizations can systematically identify and evaluate potential threats across six distinct categories. This comprehensive approach enables organizations to assess the likelihood and impact of attacks within each category, facilitating the prioritization of security measures. With this insight, organizations can then develop possible mitigation strategies to fortify their systems and networks against a diverse range of potential threats.

For instance, if an adversary attempts to compromise an onboard computer by mimicking user actions, it may execute a Spoofing attack. Similarly, the adversary might target the data flow NFC_to_OBC, aiming to disrupt the onboard computer by flooding it with counterfeit requests via NFC, potentially leading to a Denial of Service attack. A detailed breakdown of all possible threats associated with the considered components and data flows, along with their respective threat categories, is provided in Table 7. This comprehensive overview equips organizations with the necessary insights to proactively address potential vulnerabilities and bolster the resilience of their systems against cyber threats. The term "adversary" is frequently used in this context, referring to a person or organization that is unauthorized to access or modify information, or that attempts to bypass any security measures implemented to safeguard the system [66].

4.3. Rating Threats

The SAHARA method, previously discussed, caters to the requirements of analyzing security threats in the early stages of automotive development (concept level). Despite its concentration on individual vehicle development and identifying security threats and safety risks during initial development phases, the method's inter-dependencies are noteworthy. Validation of the SAHARA approach's suitability within ISO 26262 compliant development was exhibited through a battery management system use-case, revealing a 34% increase in the identification of hazardous situations compared to traditional HARA methodologies [67]. Therefore, the SAHARA method is integrated into this work for risk assessment.

Consequently, another risk assessment method, DREAD is adopted for quantifying threats. By quantifying threats in accordance with their associated risks, threats with the highest risk levels will be prioritized. This strategic approach optimizes risk management by tackling the most impacting threats first. That is why the DREAD classification scheme is adopted, showing promise in facilitating a more intricate analysis of system design.

The SAHARA analysis is conducted through a conventional process, involving the determination of SecL. Additionally, the DREAD approach is employed to contrast the differences between these two rating systems. Notably, the adapted DREAD threat classification scheme proves more suitable for evaluating remote cybersecurity attacks and attacks that affect entire vehicle operations. This suitability arises from its classification factors related to potential damage and the impact on affected users.

The SAHARA method designates k value of 2, indicating a moderate requirement, an R value of 2, signifying moderate resources for the computation of risk values associated with Threat No. 1. However, due to the T value being 3, the threat of an adversary Spoofing processes on the onboard computer results in a high level of criticality. The cumulative values contribute to a SecL value of 1, signifying high priority.

In parallel, D, R, E, and A all receive a DREAD value of 3, signaling high impact, while D obtains a value of 2, indicating medium impact. The cumulative score reaches 13, categorizing it as a high-priority threat. The computed risk values for all threats, utilizing both the SAHARA and DREAD methodologies, are presented in Table 8.

Table 8. Categorization of threats using the SAHARA and DREAD threat rating methodologies.

Threat No.	SAHARA					DREAD						
	K	**R**	**T**	**SecL**	**Priority**	**D**	**R**	**E**	**A**	**D**	**Sum**	**Priority**
1	2	2	3	1	High	3	3	3	3	2	13	High
2	2	2	2	0	Low	3	2	3	2	2	10	Medium
3	2	3	3	1	High	3	2	3	2	2	12	High
4	2	2	3	1	High	3	2	2	3	2	12	High
5	1	2	2	1	Low	2	2	3	2	2	11	Medium
6	2	3	3	1	High	3	2	2	2	3	12	High
7	1	2	2	1	Low	2	3	2	3	2	12	High
8	2	3	3	1	High	3	3	2	3	1	12	High
9	2	2	3	1	High	3	2	3	2	2	12	High
10	2	1	3	2	High	3	2	3	3	2	13	High

Table 8. *Cont.*

Threat No.	SAHARA					DREAD						
	K	**R**	**T**	**SecL**	**Priority**	**D**	**R**	**E**	**A**	**D**	**Sum**	**Priority**
11	1	3	2	0	Low	2	3	1	2	2	10	Medium
12	2	3	3	1	High	2	2	3	3	2	12	High
13	1	2	3	2	High	3	2	3	3	2	13	High
14	2	3	3	1	High	3	2	3	2	2	12	High
15	2	3	3	1	High	3	2	2	3	2	12	High
16	2	3	3	1	High	2	3	2	3	2	12	High
17	2	2	3	1	High	3	2	2	2	3	12	High
18	2	3	3	1	High	3	2	3	2	2	12	High
19	1	2	2	1	Low	3	2	2	3	2	12	High
20	2	3	3	1	High	2	2	3	3	2	12	High
21	2	2	3	1	High	3	2	2	3	2	12	High
22	2	2	3	1	High	3	2	3	2	2	12	High
23	1	2	3	2	High	2	3	2	3	2	12	High
24	2	2	3	1	High	2	3	2	3	2	12	High
25	2	2	3	1	High	3	2	2	2	2	12	High
26	2	2	3	1	High	3	2	2	3	2	12	High
27	1	2	3	2	High	3	2	3	3	2	13	High
28	2	2	3	1	High	2	2	3	3	2	12	High
29	2	2	3	1	High	3	2	3	2	2	12	High
30	2	3	3	1	High	3	2	3	3	2	13	High
31	1	3	3	1	High	3	2	2	3	2	12	High
32	2	2	3	1	High	3	2	3	3	2	13	High
33	2	2	3	1	High	3	2	2	3	2	12	High
34	2	2	3	1	High	3	2	2	3	2	12	High

5. Results and Discussion

In this section, the resultant threats and risks are discussed after applying the STRIDE threat model to the DFD and risk assessment methodologies, SAHARA, and DREAD to the threats. Additionally, the proposed defense mechanisms against the STRIDE threat category are outlined.

5.1. Resultant Threats and Risks

In the process of identifying cybersecurity threats within the context of an infotainment system, the Microsoft STRIDE tool is systematically applied to analyze various components, data flows, data stores, and external entities depicted in the DFD. Through this meticulous examination, a total of 34 threats are identified based on the considered components and their data flows and subsequently classified into six distinct categories corresponding to the STRIDE acronym. These recognized threats, meticulously categorized, serve as a crucial foundation for understanding and addressing potential vulnerabilities within the system. It is essential to emphasize that while these threats are derived from a specific use case scenario, they inherently possess a degree of subjectivity and may manifest differently in alternative scenarios. Therefore, the applicability and severity of these threats may vary based on the specific context in which the infotainment system is deployed. Before the deployment of the infotainment system in real-world automotive vehicles, it is imperative to thoroughly consider and mitigate these identified threats to ensure the safety and security of the system and its users.

To further assess the risks associated with the identified threats, a comprehensive analysis is conducted utilizing both the SAHARA and DREAD methodologies. These methodologies offer structured frameworks for evaluating the severity and potential impact of each threat. In Table 8, the outcomes of the risk assessments are presented, categorizing the threats based on their priority levels: high, medium, and low. Employing the SAHARA methodology, 29 threats are flagged as high-priority, signifying a significant level of risk that demands immediate attention. Conversely, no threats fall within the medium-risk category, while five are categorized as low-priority. In parallel, the DREAD methodology identifies 31 threats as high-priority, aligning closely with the findings of the SAHARA methodology. Additionally, three threats are classified as medium-priority, highlighting a moderate level of risk, while none are categorized as low-priority. Despite minor variations between the methodologies, the overall consensus underscores the critical importance of addressing high-priority threats promptly. These threats pose substantial risks to the security and integrity of the infotainment system, necessitating the swift implementation of robust countermeasures to mitigate potential vulnerabilities and safeguard against malicious exploitation.

5.2. Generalized Defense Mechanisms against STRIDE

To ensure system security and integrity against potential compromises, a range of defense mechanisms should be implemented. Multi-factor or biometric authentication effectively mitigates Spoofing threats. For example, if a passenger connects to the vehicle's Wi-Fi or Bluetooth via cell phone, an adversary could gain root access by exploiting weak passwords, but multi-factor authentication can prevent this unauthorized access. Additionally, attackers may intercept and modify the transmitted data between the cell phone and the vehicle, potentially altering data to mislead the navigation system. To address these Tampering attacks, encryption and digital signatures bolster the system's resistance against unauthorized alterations and data manipulation.

If a passenger makes a purchase or accesses sensitive information through the infotainment system, an adversary could exploit this opportunity to alter system settings without leaving a trace. Logging and auditing user actions can mitigate such Repudiation attacks. Access controls and permissions are crucial for preventing Information Disclosure attacks. For example, when a passenger connects their smartphone to sync contacts or access navigation data, an adversary could exploit vulnerabilities to access sensitive information stored on the infotainment system. Strong access controls can limit unauthorized access to these data.

Denial of Service attacks can be mitigated by implementing traffic limitations and load balancing. If a vehicle's infotainment system provides internet connectivity and various online services, an adversary could launch a Denial of Service attack to disrupt these services. However, distributing traffic across multiple servers helps maintain system responsiveness and availability. To prevent Elevation of Privilege attacks, user activity monitoring and logging are essential. For example, if an adversary gains initial access with low-level privileges by exploiting a compromised user account or an insecure Wi-Fi connection, monitoring and logging can detect and mitigate attempts to escalate privileges. A comprehensive overview of the complete set of defense mechanisms is provided in Table 9. These strategies collectively work to enhance the security of the system and minimize its vulnerabilities to various types of cyber threats.

Table 9. Cybersecurity defense mechanisms against threats.

Components or Interactions	Threat No.	Threat Category	Mitigation Strategy
Onboard Computer	1	Spoofing	A standard authentication mechanism, like multifactor authentication or biometric authentication, can be used to identify and prevent unauthorized access.
	2	Tampering	Digital signatures to ensure that the data has not been changed by the malicious users.
	3	Repudiation	Logging to record the tasks of the users is recommended.
	4	Information Disclosure	Encryption and access controls mechanisms to limit access to sensitive data are recommended.
	5	Denial of Service	Implemention of throttling mechanisms and load balancing through the distribution of traffic across multiple servers are state-of-the art methods.
	6	Elevation of Privileges	Proper access control mechanisms considering "need to know principles" are used for the prevention. For the detection, user activity monitoring and logging for potential privilege escalation attempts.
NFC_to_OBC	7, 8	Denial of Service	Multiple communication channels with diverse technologies between NFC and OBC are required.
	9	Information Disclosure	Encrypting the data flow between the NFC and OBC is recommended.
	10	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the NFC and OBC.
OBC_to_Wi-Fi	11, 12	Denial of Service	Multiple communication channels with diverse technologies between OBC and WiFi are required.
	13	Information Disclosure	Encrypting the data flow between the OBC and WiFi is needed.
	14	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the OBC and WiFi.
Wi-Fi_to_OBC	15, 16	Denial of Service	Multiple communication channels with diverse technologies between WiFi and OBC are required.
	17	Information Disclosure	Encrypting the data flow between the WiFi and OBC is needed.
	18	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the WiFi and OBC.
OBC_to_Bluetooth	19, 20	Denial of Service	Multiple communication channels with diverse technologies between OBC and Bluetooth are required.
	21	Information Disclosure	Encrypting the data flow between the OBC and Bluetooth is needed.
	22	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the OBC and Bluetooth.
Bluetooth_to_OBC	23, 24	Denial of Service	Multiple communication channels with diverse technologies between Bluetooth and OBC are required.
	25	Information Disclosure	Encrypting the data flow between the Bluetooth and OBC is needed.
	26	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the Bluetooth and OBC.
OBC_to_CB	27, 28	Denial of Service	Implementing traffic limitation and load balancing through the distribution of traffic across multiple servers between OBC and CB are required.
	29	Information Disclosure	Encrypting the data flow between the Bluetooth and OBC is needed.
	30	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the OBC and CB.
CB_to_OBC	31,32	Denial of Service	Multiple communication channels with diverse technologies between CB and OBC are required.
	33	Information Disclosure	Encrypting the data flow between the CB and OBC is needed.
	34	Tampering	Message Authentication Code (MAC) or digital signatures are required for the detection of the Tampering of the data between the CB and OBC.

6. Conclusions

The convergence of security and safety considerations within the automotive industry introduces potential threats to infotainment systems. Safeguarding against cybersecurity and privacy breaches necessitates the development of proper approaches for threat detection and recovery in automotive systems. Addressing these concerns is important to the system's real-world implementation. Our research undertook the task of identifying, categorizing, and enumerating 34 cybersecurity threats to the infotainment systems, leveraging the STRIDE threat modeling tool. Risk assessment methodologies, SAHARA and DREAD, are also performed on resultant threats, and risk values are calculated to determine their priority. In response to the threat and risk categories, mitigation techniques are provided, aiming to enhance the equilibrium between security and safety concerns within the automotive sector while assuring the security of infotainment systems within automotive vehicles.

In future work, threat modeling on the hardware components connected to road vehicles can be conducted. By adhering to the ISO/SAE 21434 standard for road vehicles, attack feasibility ratings and impact ratings can be determined from threat identification scenarios. This approach will aid in making informed risk treatment decisions, enhancing the overall security of automotive vehicles.

Author Contributions: Conceptualization, M.R.A.A., S.J., K.A. and F.M.B.; methodology, P.D.; software, P.D., M.R.A.A. and S.J.; validation, K.A., M.R.A.A., S.J., F.M.B. and R.K.; formal analysis, P.D.; investigation, P.D.; resources, P.D., M.R.A.A. and S.J.; data curation, P.D., M.R.A.A. and S.J.; writing—original draft preparation, P.D., M.R.A.A., S.J. and K.A.; writing—review and editing, M.R.A.A., S.J., R.K., K.A. and F.M.B.; visualization, P.D., M.R.A.A., S.J. and K.A.; supervision, M.R.A.A. and S.J.; project administration, K.A., M.R.A.A. and F.M.B.; funding acquisition, K.A. and F.M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

Data Availability Statement: Will be available upon proper request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Watabe, H.; Yamada, H. Efforts toward realization of connected car society. *Denso Ten Tech. Rev.* **2017**, *1*, 3–11.
2. Hackers Take Remote Control of Tesla's Brakes and Door Locks from 12 Miles Away. Available online: https://thehackernews.com/2016/09/hack-tesla-autopilot.html (accessed on 9 June 2023).
3. Vehicle Cybersecurity: The Jeep Hack and Beyond. Available online: https://insights.sei.cmu.edu/blog/vehicle-cybersecurity-the-jeep-hack-and-beyond (accessed on 10 June 2023).
4. Choi, J.; Jin, S.I. Security threats in connected car environment and proposal of in-vehicle infotainment-based access control mechanism. In *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2018 12*; Springer: Singapore, 2019; pp. 383–388.
5. Takahashi, J.; Iwamura, M.; Tanaka, M. Security threat analysis of automotive infotainment systems. In Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Virtual, 18 November–16 December 2020 ; pp. 1–7.
6. Nie, S.; Liu, L.; Du, Y. Free-fall: Hacking tesla from wireless to can bus. *Brief. Black Hat USA* **2017**, *25*, 16.
7. Kamkar, S. Drive it like you hacked it: New attacks and tools to wirelessly steal cars. *Present. Defcon* **2015**, *23*, 10.
8. Keuper, D.; Alkemade, T. *The Connected Car-Ways to Get Unauthorized Access and Potential Implications*; Research Paper; Computest: Zoetermeer, The Netherlands, 2018.
9. Smith, C. *The Car Hacker's Handbook: A Guide for the Penetration Tester*; No Starch Press: San Francisco, CA, USA, 2016.
10. Bolz, R.; Kriesten, R. Automotive vulnerability disclosure: Stakeholders, opportunities, challenges. *J. Cybersecur. Priv.* **2021**, *1*, 274–288. [CrossRef]
11. Renganathan, V.; Yurtsever, E.; Ahmed, Q.; Yener, A. Valet attack on privacy: A cybersecurity threat in automotive Bluetooth infotainment systems. *Cybersecurity* **2022**, *5*, 30. [CrossRef]
12. Moiz, A.; Alalfi, M.H. An approach for the identification of information leakage in automotive infotainment systems. In Proceedings of the 2020 IEEE 20th International Working Conference on Source Code Analysis and Manipulation (SCAM), Adelaide, Australia, 28 September–2 October 2020; pp. 110–114.
13. Scalas, M.; Giacinto, G. Automotive cybersecurity: Foundations for next-generation vehicles. In Proceedings of the 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), Amman, Jordan, 9–11 October 2019; pp. 1–6.

14. Iorio, M.; Reineri, M.; Risso, F.; Sisto, R.; Valenza, F. Securing SOME/IP for in-vehicle service protection. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13450–13466. [CrossRef]
15. Yang, Y.; Duan, Z.; Tehranipoor, M. Identify a spoofing attack on an in-vehicle CAN bus based on the deep features of an ECU fingerprint signal. *Smart Cities* **2020**, *3*, 17–30. [CrossRef]
16. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Berleley/Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
17. Dang, Q.A.; Khondoker, R.; Wong, K.; Kamijo, S. Threat analysis of an autonomous vehicle architecture. In Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 19–20 December 2020; pp. 1–6.
18. Pascale, F.; Adinolfi, E.A.; Coppola, S.; Santonicola, E. Cybersecurity in automotive: An intrusion detection system in connected vehicles. *Electronics* **2021**, *10*, 1765. [CrossRef]
19. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Torino, Italy, 26–29 September 2017; pp. 1–6.
20. Benyahya, M.; Lenard, T.; Collen, A.; Nijdam, N.A. A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2023; pp. 1–10.
21. Al Asif, M.R.; Hasan, K.F.; Islam, M.Z.; Khondoker, R. STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. In Proceedings of the 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 18–19 December 2021; pp. 1–6.
22. Salau, A.; Dantu, R.; Morozov, K.; Upadhyay, K.; Badruddoja, S. Towards a threat model and security analysis for data cooperatives. In Proceedings of the 19th International Conference on Security and Cryptography-SECRYPT, Lisbon, Portugal, 11–13 July 2022 ; pp. 707–713.
23. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
24. Alarcón, J.; Balcázar, I.; Collazos, C.A.; Luna, H.; Moreira, F. User interface design patterns for infotainment systems based on driver distraction: A Colombian case study. *Sustainability* **2022**, *14*, 8186. [CrossRef]
25. Quintal, F.; Lima, M. HapWheel: In-car infotainment system feedback using haptic and hovering techniques. *IEEE Trans. Haptics* **2021**, *15*, 121–130. [CrossRef] [PubMed]
26. Designing Infotainment Systems That Are Interactive, Not Distractive. Automotive Technical Articles—TI E2E Support Forums, 6 June 2019. Available online: https://e2e.ti.com/blog_/b/behind_the_wheel/posts/designing-infotainment-systems-that-are-interactive-not-distractive (accessed on 12 August 2023).
27. Designing in-Vehicle Infotainment Systems. Available online: https://my.avnet.com/abacus/solutions/markets/automotive-and-transportation/automotive/comfort-infotainment-and-safety/automotive-infotainment/ (accessed on 12 April 2024).
28. Meixner, G.; Häcker, C.; Decker, B.; Gerlach, S.; Hess, A.; Holl, K.; Klaus, A.; Lüddecke, D.; Mauser, D.; Orfgen, M.; et al. Retrospective and future automotive infotainment systems—100 years of user interface evolution. In *Automotive User Interfaces: Creating Interactive Experiences in the Car*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 3–53.
29. Berger, M.; Bernhaupt, R.; Pfleging, B. A tactile interaction concept for in-car passenger infotainment systems. In Proceedings of the 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications: Adjunct Proceedings, Utrecht, The Netherlands, 22–25 September 2019; pp. 109–114.
30. Sen, G.; Sener, B. Design for luxury front-seat passenger infotainment systems with experience prototyping through VR. *Int. J. Hum.–Comput. Interact.* **2020**, *36*, 1714–1733. [CrossRef]
31. Josephlal, E.F.M.; Adepu, S. Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability. In Proceedings of the 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), Hangzhou, China, 3–5 January 2019 ; pp. 241–246.
32. Tashev, I.; Seltzer, M.; Ju, Y. C.; Wang, Y.Y.; Acero, A. Commute UX: Voice Enabled In-Car Infotainment System. In Proceedings of the Mobile HCI'09: Workshop on Speech in Mobile and Pervasive Environments (SiMPE), Bonn, Germany, 15–18 September 2009. Available online: https://www.microsoft.com/en-us/research/publication/commute-ux-voice-enabled-in-car-infotainment-system/ (accessed on 5 June 2023).
33. Souppaya, M.; Scarfone, K. Guide to enterprise telework, remote access, and bring your own device (BYOD) security. *NIST Spec. Publ.* **2016**, *800*, 46.
34. UcedaVelez, T.; Morana, M.M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
35. Shevchenko, N.; Chick, T.A.; O'Riordan, P.; Scanlon, T.P.; Woody, C. *Threat Modeling: A Summary of Available Methods*; Carnegie Mellon University Software Engineering Institute Pittsburgh United States: Pittsburgh, PA, USA, 2018.
36. Schneier, B. Attack trees. *Dr Dobb's J.* **1999**, *24*, 21–29.
37. Noel, S.; Jajodia, S. Managing attack graph complexity through visual hierarchical aggregation. In Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, Washington, DC, USA, 29 October 2004; pp. 109–118.
38. Mauw, S.; Oostdijk, M. Foundations of attack trees. In *Proceedings of the Information Security and Cryptology-ICISC 2005: 8th International Conference, Seoul, Republic of Korea, 1–2 December 2005*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 186–198.

39. Wang, P.; Lin, W.H.; Kuo, P.T.; Lin, H.T.; Wang, T.C. Threat risk analysis for cloud security based on attack-defense trees. In Proceedings of the 2012 8th International Conference on Computing Technology and Information Management (NCM and ICNIT), Seoul, Republic of Korea, 24–26 April 2012; Volume 1, pp. 106–111.
40. Common Vulnerability Scoring System v3.0: Specification Document. Forum of Incident Response and Security Teams. Available online: https://www.first.org/cvss/specification-document (accessed on 25 July 2023).
41. Potteiger, B.; Martins, G.; Koutsoukos, X. Software and attack centric integrated threat modeling for quantitative risk assessment. In Proceedings of the Symposium and Bootcamp on the Science of Security, Pittsburgh, PA, USA, 19–21 April 2016; pp. 99–108.
42. Caralli, R.A.; Stevens, J.F.; Young, L.R.; Wilson, W.R. *Introducing Octave Allegro: Improving the Information Security Risk Assessment Process*; Carnegie Mellon University, Software Engineering Institute's Digital Library: Hansom AFB, MA, USA, 2007.
43. Mead, N.R.; Shull, F.; Vemuru, K.; Villadsen, O. *A Hybrid Threat Modeling Method*; Technical Report-CMU/SEI-2018-TN-002; Carnegie Mellon University-Software Engineering Institute: Pittsburgh, PA, USA, 2018.
44. Selin, J. Evaluation of Threat Modeling Methodologies. Master's Thesis, Jamk University of Applied Sciences, Jyväskylä, Finland, 2019. Available online: https://www.theseus.fi/bitstream/handle/10024/220967/Selin_Juuso.pdf (accessed on 1 June 2024).
45. Kim, K.H.; Kim, K.; Kim, H.K. STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI J.* **2022**, *44*, 991–1003. [CrossRef]
46. Tany, N.S.; Suresh, S.; Sinha, D.N.; Shinde, C.; Stolojescu-Crisan, C.; Khondoker, R. Cybersecurity Comparison of Brain-Based Automotive Electrical and Electronic Architectures. *Information* **2022**, *13*, 518. [CrossRef]
47. Asif, M.R.A.; Khondoker, R. Cyber Security Threat Modeling of A Telesurgery System. In Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry, Dhaka, Bangladesh, 19–20 December 2020; Volume 4, pp. 1–6.
48. Schiffman, M.; Wright, A.; Ahmad, D.; Eschelbeck, G. *The Common Vulnerability Scoring System*; National Infrastructure Advisory Council, Vulnerability Disclosure Working Group, Vulnerability Scoring: Washington, DC, USA, 2004.
49. Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C. *Introduction to the OCTAVE Approach*; Carnegie Mellon University: Pittsburgh, PA, USA, 2003; pp. 72–74.
50. Beyst, B. Which Threat Modeling Method. Available online: https://threatmodeler.com/threat-modeling-methodologies-vast/ (accessed on 9 June 2024).
51. Wuyts, K.; Joosen, W. *LINDDUN Privacy threat Modeling: A Tutorial*; CW Reports; KU Leuven: Leuven, Belgium , 2015.
52. Swiderski, F.; Snyder, W. *Threat Modeling*; Microsoft Press: Redmond, WA, USA, 2004.
53. AbuEmera, E.A.; ElZouka, H.A.; Saad, A.A. Security framework for identifying threats in smart manufacturing systems using STRIDE approach. In Proceedings of the 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 14–16 January 2022 ; pp. 605–612.
54. Khan, A.; Bryans, J.; Sabaliauskaite, G. Framework for calculating residual cybersecurity risk of threats to road vehicles in alignment with ISO/SAE 21434. In *Proceedings of the International Conference on Applied Cryptography and Network Security, Rome, Italy, 20–23 June 2022*; Springer International Publishing: Cham, Switzerland, 2022; pp. 235–247.
55. Birch, J.; Rivett, R.; Habli, I.; Bradshaw, B.; Botham, J.; Higham, D.; Jesty, P.; Monkhouse, H.; Palin, R. Safety cases and their role in ISO 26262 functional safety assessment. In *Proceedings of the Computer Safety, Reliability, and Security: 32nd International Conference, SAFECOMP 2013, Toulouse, France, 14–27 September 2013*; Proceedings 32; Springer: Berlin/Heidelberg, Germany, 2013; pp. 154–165.
56. Dempsey, K.L.; Johnson, L.A.; Scholl, M.A.; Stine, K.M.; Jones, A.C.; Orebaugh, A.; Chawla, N.S.; Johnston, R. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2011.
57. Grassi, P.A.; Fenton, J.L.; Garcia, M.E. Digital Identity Guidelines [Including Updates as of 12-01-2017]. 2017. Available online: https://www.nist.gov/publications/digital-identity-guidelines-including-updates-12-01-2017 (accessed on 25 July 2023).
58. *IEC 60812*; Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA). ISO—International Organization for Standardization: Geneva, Switzerland, 2006.
59. Schmittner, C.; Gruber, T.; Puschner, P.; Schoitsch, E. Security application of failure mode and effect analysis (FMEA). In *Computer Safety, Reliability, and Security: Proceedings of the 33rd International Conference, SAFECOMP 2014, Florence, Italy, 10–14 September 2014*; Springer International Publishing: Berlin/Heidelberg, Germany, 2014; pp. 310–325.
60. Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. A review of threat analysis and risk assessment methods in the automotive context. In *Computer Safety, Reliability, and Security: Proceedings of the 35th International Conference, SAFECOMP 2016, Trondheim, Norway, 21–23 September 2016*; Proceedings 35; Springer International Publishing: Berlin/Heidelberg, Germany, 2016.
61. Ruddle, A.; Ward, D.; Weyl, B.; Idrees, S.; Roudier, Y.; Friedewald, M.; Leimbach, T.; Fuchs, A.; Gürgens, S.; Henniger, O.; et al. Deliverable D2. 3: Security Requirements for Automotive On-Board Networks Based on Dark-Side Scenarios. EVITA Project. 2009. Available online: https://www.researchgate.net/profile/Gabriel-Pedroza/publication/304525166_Security_requirements_for_automotive_on-board_networks_based_on_dark-side_scenarios/links/57b06d4808ae15c76cba2666/Security-requirements-for-automotive-on-board-networks-based-on-dark-side-scenarios.pdf (accessed on 15 July 2023).
62. Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. Threat and risk assessment methodologies in the automotive domain. *Procedia Comput. Sci.* **2016**, *83*, 1288–1294. [CrossRef]

63. Macher, G.; Sporer, H.; Berlach, R.; Armengaud, E.; Kreiner, C. SAHARA: A security-aware hazard and risk analysis method. In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, Grenoble, France, 9–13 March 2015; pp. 621–624.
64. Threat Modeling Process. Available online: https://owasp.org/www-community/Threat_Modeling_Process#subjective-model-dread (accessed on 9 June 2023).
65. Cagnazzo, M.; Hertlein, M.; Holz, T.; Pohlmann, N. Threat modeling for mobile health systems. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Barcelona, Spain, 15–18 April 2018; pp. 314–319.
66. Dang, Q. *Recommendation for Applications Using Approved Hash Algorithms*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2008.
67. Macher, G.; Höller, A.; Sporer, H.; Armengaud, E.; Kreiner, C. A combined safety-hazards and security-threat analysis method for automotive systems. In *Computer Safety, Reliability, and Security: Proceedings of the SAFECOMP 2015 Workshops, ASSURE, DECSoS. ISSE, ReSA4CI, and SASSUR, Delft, The Netherlands, 22 September 2015*; Proceedings 34; Springer International Publishing: Berlin/Heidelberg, Germany, 2015; pp. 237–250.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.