Project Submission Pro-Forma

Student name:……Patrick Chou……

Student ID: ……2126529……

I wish the dissertation to be considered for the course (select one only):

☐ MSc in Cyber Security Management
☒ MSc in Cyber Security Engineering
☐ MSc in e-Business Management
☐ MSc in Engineering Business Management
☐ MSc in Healthcare Operational Management
☐ MSc in Innovation & Entrepreneurship
☐ MSc in Intelligent Manufacturing Systems
☐ MSc in International Trade, Strategy & Operations
☐ MSc in Management for Business Excellence
☐ MSc in Programme & Project Management
☐ MSc in Service Management & Design
☐ MSc in Supply Chain & Logistics Management
☐ MSc in Sustainable Automotive Engineering
☐ MSc in Smart, Connected and Autonomous Vehicles

I confirm that I have included in my dissertation:

☒ An abstract of the work completed
☒ A declaration of my contribution to the work and its suitability for the degree
☒ A table of contents
☒ A list of figures & tables (if applicable)
☒ A glossary of terms (where appropriate)
☒ A clear statement of my project objectives
☒ A full reference list (the Harvard referencing style is recommended for WMG)
☒ An appendix containing email confirmation of ethical approval or waiver

If receiving ethical approval, the ethical approval number for this research is: N/A

☒ I consent to ongoing storage of this dissertation and potential access by third parties (e.g. for staff/ student training purposes)

Signed: …… Patrick Chou …… Date: …05/09/2023……..

Threat Analysis and Risk Assessment (TARA) of Infotainment Systems Security of Smart Vehicles

by

Patrick Chou, MSc

Dissertation submitted in partial fulfilment for the Degree of Master of Science in Cyber Security Engineering

WMG
University of Warwick

Submitted September 2023

Declaration

I have read and understood the rules on cheating, plagiarism and appropriate referencing as outlined in my handbook and I declare that the work contained in this assignment is my own, unless otherwise acknowledged.

No substantial part of the work submitted here has also been submitted by me in other assessments for this or previous degree courses, and I acknowledge that if this has been done an appropriate reduction in the mark I might otherwise have received will be made.

Project definition for my degree (as copied from http://www2.warwick.ac.uk/fac/sci/wmg/globalcontent/general/project/requirement/)
The project for MSc Cyber Security Engineering must:

1.address a research question directly relating to cyber security, AND
2.demonstrate understanding of the particular issues around conducting research in the cyber domain, AND
3.conduct research in the cyber domain in an appropriate manner.

My project relates to this definition in the following way:

The research question of this project is: "How to conduct a comprehensive threat analysis and risk assessment for smart vehicles infotainment systems to reduce cybersecurity risks and enhance the systems security effectively?" Thus, this project will be based on the Threat Analysis and Risk Assessment (TARA) framework of ISO/SAE 21434 and delve into several steps within smart vehicles infotainment systems. The project aims to provide a clear and practical guide for automotive-related entities to understand risks associated with smart vehicles infotainment systems.

This project complies with the following two CyBOK Skills areas: Risk Management and Governance, Cyber Physical Systems Security.

Abstract

With the development of technology, smart vehicles have increasingly become a significant form of transportation globally. Smart vehicles have many complicated and essential systems, among which the infotainment systems are key components. It provides passengers with entertainment and essential vehicle information, such as driving assistance audio and video entertainment. However, the infotainment systems also raise cybersecurity issues, including personal data breaches, financial losses, and even life-threatening situations. Therefore, this project conducts a thorough threat analysis and risk assessment for the infotainment systems based on the Threat Analysis and Risk Assessment (TARA) framework of ISO/SAE 21434. This project aims to provide automotive organisations with a comprehensive threat analysis and risk assessment guideline to effectively mitigate the cybersecurity risks connected with the infotainment systems and improve user safety.

Acknowledgements

First, I must deeply thank my supervisor, Dr. Alaa Al Sebae. In the early stages of research, I faced divergent thoughts and unclear directions. However, under the careful guidance of Dr. Alaa Al Sebae, I gradually organised my ideas and determined the research direction. Your academic advice and in-depth insights enabled me to complete this high-quality project.

Secondly, I would like to express my deep gratitude to Warwick University. Warwick University provides many academic resources, which helped me become more familiar with the writing method of academic papers and avoid unnecessary mistakes.

Finally, I am especially grateful to my family, friends, and peers who have supported and accompanied me on this academic journey. Your help allowed me to overcome the pressure and difficulties during this project.

Table of Contents

List of Figures

1. Introduction

This chapter will introduce the comprehensive threat analysis and risk assessment of smart vehicles infotainment systems, including research background, motivation, questions, objectives, methodology approach, and project structure. The following will elaborate on each of these components.

1.1 Research Background

With the continuous advancement of technology, smart vehicles have been widely recognised as a significant innovation shaping the transportation industry's future (Kumar et al., 2019). In particular, the rapid development of sensors, communication technologies, and the practical application of object detection techniques and corresponding algorithms have laid a robust technological foundation for smart vehicles (Abdelkader et al., 2021). Among these components, the infotainment systems, as a core element of smart vehicles, has become more susceptible to attacks due to technological advancements, leading to unprecedented and escalating threats and attacks (Josephlal and Adepu, 2019). Therefore, conducting a comprehensive threat analysis and risk assessment of infotainment systems can mitigate the associated cyber-attack risks and enhance user security.

1.2 Research Motivation

The smart vehicles infotainment systems provide functionalities such as audio-video streaming, navigation, calling, driver assistance, and internet connectivity, offering entertainment and vehicle information to drivers and passengers (Meixner et al., 2017). However, alongside its convenience, the infotainment systems may also introduce vehicles cybersecurity concerns. For instance, adversaries could exploit browser vulnerabilities through wireless connections to remotely gain access and elevate their privileges over other subsystems within an autonomous vehicle, posing security threats to vehicle occupants (Takahashi et al., 2020).

Furthermore, in the current research landscape, there needs to be more comprehensive and in-depth threat analysis and risk assessment focused explicitly on smart vehicles infotainment systems. This research gap may lead to the general public overlooking this crucial issue, thereby subjecting smart vehicles to security risks. Consequently, in order to address the cybersecurity issues of smart vehicles infotainment systems and the current

limitations, conducting a comprehensive threat analysis and risk assessment of these systems aids in identifying their threats and vulnerabilities, mitigating potential attacker threats, and enhancing the safety of both drivers and passengers.

1.3 Research Questions

The core question of this project is: "How to conduct a comprehensive threat analysis and risk assessment for smart vehicles infotainment systems to reduce cybersecurity risks and enhance the systems security effectively?" Thus, this project will delve into the assets, threat scenarios, systems vulnerabilities, attacker attack paths, and risk values corresponding to assets within smart vehicles infotainment systems. Moreover, this project will focus on determining the overall cybersecurity risks associated with each asset and proposing appropriate risk mitigation strategies based on the analysis results.

1.4 Research Objectives

Based on the Threat Analysis and Risk Assessment (TARA) framework from ISO/SAE 21434 (ISO, 2021), this project presents a comprehensive process and outcomes of threat analysis and risk assessment for smart vehicles infotainment systems. The research aims to provide a clear and practical guideline for stakeholders such as vehicle manufacturers, suppliers, and cybersecurity experts in performing threat analysis and risk assessment for smart vehicles infotainment systems. This guideline makes it easier to lower the cybersecurity risks associated with infotainment systems, improve passenger and driver safety, and strengthen the security and resilience of smart vehicles infotainment systems.

1.5 Methodology Approach

The TARA framework from ISO/SAE 21434 encompasses identifying assets and threat scenarios, assessing the impact and feasibility of attacks, analysing attack paths, determining risks, and providing suitable risk treatment strategies (ISO, 2021). This aligns with the field of risk management and governance in the CyBOK knowledge (Burnap, 2021). It also corresponds to the cyber physical systems security domain in CyBOK knowledge, as it involves considerations of interactions between cyber physical systems (Cardenas and Cruz, 2021). Moreover, the National Institute of Standards and Technology (2018) also mentioned the importance of threat analysis and risk assessment for vehicle cybersecurity risk management.

The TARA framework in ISO/SAE 21434 serves as a method for automotive-related entities to understand risks associated with vehicles infotainment systems and how to take appropriate measures to mitigate them (ISO, 2021). This project progressively adapts the TARA framework to propose a series of processes and outcomes applicable to smart vehicles infotainment systems, enabling automotive-related entities to analyse and assess these systems comprehensively. Furthermore, the research aids in developing robust and effective protective strategies for safeguarding the safety of drivers, passengers and the overall cybersecurity of vehicles.

1.6 Project Structure

This project is divided into six main chapters. The first chapter serves as the introduction, delving into the background, motivation, core questions, objectives, and structure of conducting threat analysis and risk assessment for smart vehicles infotainment systems. Chapter two comprises the literature review, discussing relevant studies and developments, encompassing the origins and evolution of smart vehicles and their infotainment systems, critical issues in cybersecurity, and the TARA framework under ISO/SAE 21434. Additionally, this chapter will explore current research gaps and highlight the unique contributions of the research to the existing literature.

In chapter three, the research methodology will be detailed, covering the use of secondary data, strategies for data integration and analysis, rationale for selecting the TARA framework, and the implementation of the TARA framework. Furthermore, this chapter will explore selecting research tools and potential risks associated with this project. Chapter four will showcase the research outcomes, gradually presenting the implementation details and processes of conducting threat analysis and risk assessment for smart vehicles infotainment systems while elaborating on the results of each step.

Chapter five engages in discussions, analysing the main findings of the research and comparing them with other studies. Simultaneously, this chapter will detail the limitations of this project. Chapter six will describe the conclusions of the project, revisiting the research questions, objectives, and contributions while exploring the trends in developing the research topic and indicating potential future studies.

2. Literature Review

This chapter will focus on an in-depth literature review of threat analysis and risk assessment in the cybersecurity of smart vehicles infotainment systems. Firstly, the relevant literature concerning smart vehicles infotainment systems will be classified and thoroughly analysed, discussing the critical publications in each related area while highlighting the deficiencies within the existing literature. Furthermore, these analysis results will be synthesised, emphasising how this project contributes to filling the gaps in the existing literature on smart vehicles infotainment systems.

2.1 Related Works

This section will delve into the literature on threat analysis and risk assessment in smart vehicles infotainment systems. It will focus on the origins and development of smart vehicles and their infotainment systems. Subsequently, a comprehensive examination of the cybersecurity threats and challenges smart vehicles face will be conducted. This will be followed by an in-depth analysis of cybersecurity issues related to infotainment systems, uncovering potential vulnerabilities, risks, and potential solutions. Moreover, the principles and framework of the TARA framework within the ISO/SAE 21434 standard tailored for road vehicles (ISO, 2021) will be discussed, providing an understanding of how this framework aids in mitigating cybersecurity risks for vehicles. While analysing each relevant publication, critical thinking will be employed to address the literature's shortcomings explicitly.

2.1.1 Background of Smart Vehicles and Infotainment Systems

This subsection will delve into the background and development of smart vehicles and infotainment systems, focusing on the multi-layered complexity that technology introduces to the ecosystems of smart vehicles.

Abdelkader et al. (2021) highlight stakeholders' collaborative efforts to advance connected vehicle technology research and development. They posit that the implementation of adaptive routing, real-time navigation, and advanced driver assistance systems will contribute to creating a road environment that is safer and environmentally friendly. However, their research overlooks the role of infotainment systems within smart vehicles, particularly as their complexity and connectivity grow.

Yang et al. (2018) provide a comprehensive exploration of the foundational technologies of smart vehicles, highlighting critical stages of development, crucial electronic components, and core algorithms driving intelligent navigation. However, despite emphasising the combination of platform technologies with theoretical algorithms to accelerate the development of smart vehicles, they overlook the potential impact of evolving cybersecurity threats that could hinder this technology's further advancement.

Uhlemann (2016) describes an initiative by the World Economic Forum that involves consultations with urban policymakers and transportation agencies. Furthermore, the article mentions that urban management authorities generally believe using shared autonomous vehicles as a "last mile" public transport solution holds promise. However, in his research, Uhlemann needs to emphasise the role of infotainment systems in these autonomous vehicles. As the primary interface for user interaction, infotainment systems are critical in ensuring passenger experience and satisfaction. Therefore, its development and integration should be part of the discussion when introducing such vehicles.

Uhlemann (2015) outlines the genesis of smart vehicles, where vehicles are no longer viewed as isolated units but become part of a network, interacting with other devices and applications. Moreover, he also discusses various applications ranging from safety, efficiency, and infotainment to autonomous driving. However, Uhlemann's estimation of the critical role of infotainment systems in supporting these applications needs to be revised, and their significance throughout the systems may surpass his initial intent with these systems increasing integration and connectivity within smart vehicles.

Lu et al. (2014) argue that wireless connectivity is central to vehicle interaction and their internal and external surroundings. However, their challenges and potential solutions for vehicle-to-everything connections still need to address the continuously changing threats that smart vehicles face, which could impact the stability and reliability of wireless connections.

2.1.2 Cyber Security of Smart Vehicles

This subsection will delve into emerging cybersecurity scenarios within the smart vehicles environments, analysing in detail the types of threats, their scale, and potential attack

methods. Additionally, it discusses the significant challenges encountered in enhancing the ability of these smart vehicles systems to counter cybersecurity threats.

Rathore et al. (2022) provide an in-depth analysis of cybersecurity in vehicular communication systems, emphasising the importance of targeted security measures in mitigating potential risks. They combine machine learning, cryptography, and port-centric techniques to research network architecture, protocols, and security schemes, strongly advocating for establishing a multi-layer and protocol-agnostic security framework. However, their research falls short in exploring the dynamic changes in the threat landscape, particularly given that static security strategies may become ineffective against evolving threats.

El-Rewini et al. (2020) study attacks on sensors in autonomous vehicles, noting limited literature on many attack cases due to original equipment manufacturers (OEMs) swiftly addressing issues through software updates. These attack cases include intrusion via camera systems and manipulating road signs to deceive object detection algorithms. Their scope goes beyond vehicle sensor security to external vulnerabilities, such as hacking roadside infrastructure or unauthorised access to user data stored in the cloud. However, their analysis of potential security risks from infotainment systems and their direct or indirect connections to vehicle sensors is relatively limited.

Scalas and Giacinto (2019) offer comprehensive and systematic recommendations for addressing cybersecurity issues in smart vehicles designs, especially focusing on vehicle networks. They deeply explore this network's requirements, potential vulnerabilities, and common protocols while considering potential attacker strategies, laying a strong foundation for the future. However, they overlook the role of infotainment systems in-vehicle networks and related cybersecurity issues. Integrating security assessments of infotainment systems into their framework would provide a more thorough understanding of cybersecurity in smart vehicles.

Haas and Möller (2017) describe significant transformations in the automotive industry, mainly emphasising major innovation trends in recent years. They discuss technological advancements in internal combustion engines, transmissions, safety systems, and infotainment solutions. They also provide valuable insights into digital product engineering and manufacturing processes. However, they do not fully recognise that as vehicle

technology progresses and complexity increases, smart vehicles become more susceptible to cyber-attacks, making cybersecurity concerns more urgent.

Hashem Eiza and Ni (2017) thoroughly explore the driving factors behind the transformation of the vehicle industry, specifically highlighting cybersecurity threats faced by smart vehicles. While their research offers unique insights into electric vehicles, car-sharing, and automated valet parking, their focus on the potential cybersecurity issues brought about by infotainment systems remains lacking.

2.1.3 Cyber Security Issues of Smart Vehicles Infotainment Systems

This subsection will delve into the cybersecurity issues of smart vehicles infotainment systems, encompassing security vulnerabilities within various automotive systems and functionalities. It also discusses strategies and methods employed to enhance their security.

Jeong et al. (2023) focus on security and privacy issues in vehicular infotainment systems. They employ an automotive-grade Linux operating system and identify several reproducible and verified exploit codes targeting components of Linux-based infotainment systems in a testbed. The researchers successfully exploited these vulnerabilities, leading to data privacy breaches, manipulation of infotainment systems functionality, and denial of service (DoS) attacks. Additionally, they demonstrate lateral movement techniques between electronic control units and smartphones. However, this research focuses on the Linux operating systems. It does not include other infotainment systems operating systems, potentially limiting its ability to comprehensively describe security and privacy risks in the entire domain of infotainment applications.

Renganathan et al. (2022) focus on Bluetooth features in smart vehicles, uncovering security and privacy issues they introduce. They reveal potential vulnerabilities by in-depth analysis of the Bluetooth network within smart vehicles infotainment units. While they conduct a comprehensive analysis and propose corresponding protective measures, this research may greatly concentrate on Bluetooth connections, potentially overlooking vulnerabilities in other communication protocols within the infotainment systems.

Takahashi et al. (2020) investigate security concerns in smart vehicles, particularly potential vulnerabilities in vehicles infotainment systems. By assessing risks associated with remote control services, vehicle network connections, and attack vectors that could bypass existing

protective measures, they offer an insightful understanding of vulnerabilities within infotainment systems. However, their research heavily emphasises remote control services. It might not adequately cover other application services of infotainment systems, which could be equally important when assessing potential threats to the system.

Josephlal and Adepu (2019) focus on identifying vulnerabilities in the Wi-Fi functionality of vehicles infotainment systems. They present detailed findings from structured vulnerability testing and Wi-Fi attack surface analysis. However, this research concentrated on vulnerabilities in Wi-Fi functionality and did not conduct vulnerability analysis on the communication and connectivity features of other infotainment systems components.

Mandal et al. (2019) introduce a static analysis technique to explore security concerns in Android-based infotainment and OBD-II applications. Their research successfully uncovers security flaws in some highly rated applications. However, this research does not broadly cover other infotainment systems software platforms, thus not fully reflecting the security threats in the entire domain of infotainment applications.

Mandal et al. (2018) propose a static analysis technique for Android Auto infotainment applications to identify software vulnerabilities. While this research provides deep insights into Android Auto applications, its scope remains relatively narrow and does not encompass other infotainment systems software platforms. Future research could consider expanding this analysis approach for broader applicability across other mainstream platforms.

Costantino et al. (2018) study security vulnerabilities in user-to-vehicle and vehicle communications, focusing on infotainment systems. They introduce "CANDY", a Trojan application capable of infiltrating Android-based vehicles infotainment systems, allowing remote access and compromising user privacy. However, this research targets Android-based systems and does not account for potential vulnerabilities in infotainment systems based on platforms like iOS or Linux. To achieve a more comprehensive security assessment, an ideal research scope should encompass various platforms.

Pan et al. (2017) discuss the significance of the CAN bus in modern vehicles and the potential impacts when compromised. They demonstrate mobile malware containing attack code targeting the CAN bus and highlighted vehicle engineers' challenges in countering these security threats. While this project provides insights for enhancing the security of modern

vehicle systems, the practicality of the research findings remains to be confirmed as real-world vehicle attack validation was not performed.

Mazloom et al. (2016) conduct a detailed security analysis of the vehicles infotainment systems of a renowned vehicle manufacturer. While they successfully uncover security issues related to the MirrorLink protocol, this research mainly focuses on a specific model. This could imply that the applicability of the research's findings is limited across different vehicles and infotainment systems.

2.1.4 Threat Analysis and Risk Assessment (TARA) Framework in ISO/SAE 21434

This subsection will explore the principles and structure of the Threat Analysis and Risk Assessment (TARA) framework within the ISO/SAE 21434 standard, specifically tailored for road vehicles (ISO, 2021). It also describes its methodologies, applications, and effectiveness in the context of smart vehicles.

Ebrahimi et al. (2022) propose a TARA-based threat modelling approach to identify and assess potential security risks more accurately. This approach emphasis mapping vulnerabilities from the effective attack surface to assets, thereby identifying attack paths. They also demonstrate how to translate the ISO/SAE 21434 standard and R155 regulations into attack trees for assessing vehicle designs in practical contexts. However, due to a lack of complete modelling of actual cases for this approach, its application in large or complex vehicle systems might encounter challenges, especially when considering multiple vulnerabilities and potential attack paths.

Dantas et al. (2021) focus on the detailed process and required artefacts generated by the TARA framework within ISO/SAE 21434. This research provides specific operational methods for each step of the TARA framework, combined with particular cases and the generation of relevant artefacts, aiming to assist readers in comprehending the application of the TARA framework. However, while this research thoroughly describes the operational methods and related cases of the TARA framework, it still needs to address how to apply it within the context of smart vehicles infotainment systems.

Luo et al. (2021) conduct a comprehensive analysis and comparison of assessment tools within the TARA framework. They explore commonly used tools within the framework and examined how these tools interact with specific threats and corresponding mitigation

measures. Additionally, the research introduces a new approach called Attack-Defence Mapping, which aims to provide a more intuitive understanding of the relationship between threats and defence strategies. However, while introducing the new concept of Attack-Defence Mapping, they still need to offer more examples or concrete cases to illustrate its application in practical scenarios.

Macher et al. (2020) discuss the TARA framework in ISO/SAE 21434, providing an in-depth analysis and explanation of its structure and operational principles. This research not only focuses on the core concepts of the TARA framework but also offers practical application methods, enabling its successful implementation across various contexts. Additionally, they share a range of best practice strategies to assist professionals and organisations in adopting the framework effectively. However, while this research details various application methods and strategies for threat analysis and risk assessment, it still needs to provide complete real-world scenario examples to help readers in understanding potential difficulties in actual operational processes.

Bolovinou et al. (2019) develop an advanced assessment method called TARA+, building upon the TARA framework. This new framework delves into threats posed by new attack vectors and technological advancements, incorporating customised impact assessment for specific scenarios, especially in highly connected environments such as autonomous vehicles. However, TARA+ is designed for the specific application scenario of autonomous vehicles. Its precision might be challenged when applied in other domains or specific areas.

2.2 Research Gaps

This section will provide the literature gaps covered in subsections 2.1.1 through 2.1.4 and highlight the contributions of this project in addressing the deficiencies within the existing literature.

In subsection 2.1.1, Background of Smart Vehicles and Infotainment Systems: The current literature extensively delves into smart vehicles technological foundations and potential benefits. However, at the level of infotainment systems, the design and their implications have not received sufficient attention. Additionally, with the evolving threat landscape, there is a heightened urgency to study their impact on these systems. Hence, this project

endeavours to fill this gap by conducting an in-depth exploration of threat analysis and risk assessment for smart vehicles infotainment systems.

In subsection 2.1.2, Cyber Security of Smart Vehicles: The current literature offers valuable insights into cybersecurity threats for smart vehicles and corresponding defences. However, the cybersecurity issues of infotainment systems are often overlooked, leading to underestimating cybersecurity risks in smart vehicles. Furthermore, understanding dynamic and varied threat scenarios still needs to be improved in the current literature, hindering timely responses and risk mitigation against changing threats. Therefore, in addition to focusing on the security of smart vehicles infotainment systems, this project will thoroughly investigate the dynamics of cybersecurity threats through comprehensive threat analysis and risk assessment.

In subsection 2.1.3, Cyber Security Issues of Smart Vehicles Infotainment Systems: The existing literature provides valuable insights into cybersecurity for infotainment systems of smart vehicles. However, most studies concentrate on specific subsystems or environments, failing to comprehensively assess cybersecurity threats. To address these limitations, this project adopts a more holistic approach, considering a comprehensive range of infotainment systems assets, and conducts comprehensive threat analysis and risk assessment for all subsystems of infotainment to enhance the resilience of smart vehicles cybersecurity.

In subsection 2.1.4, Threat Analysis and Risk Assessment (TARA) Framework in ISO/SAE 21434: The TARA framework within ISO/SAE 21434 provides a solid foundation for threat analysis and risk assessment in smart vehicles cybersecurity. However, many studies focus on the framework's development rather than its practical application in real-world scenarios. This lack of practical application can result in challenges for users during actual implementation. Moreover, limited research exists regarding threat analysis and risk assessment for smart vehicles infotainment systems, leaving smart vehicles susceptible to security risks. To address these gaps, this project will perform a comprehensive threat analysis and risk assessment for smart vehicles infotainment systems, detailing the assessment process and outcomes. The project aims to facilitate smoother practical implementation for users and reduce potential challenges they might encounter.

2.3 Summary

Synthesising the related works, it is evident that the current research in smart vehicles has spanned several significant domains. However, notable research gaps persist. In cybersecurity, existing literature often overlooks the integrity of infotainment systems and systemic cybersecurity risks. Additionally, the dynamic threat landscape of smart vehicles cybersecurity is frequently ignored, potentially rendering current security strategies inadequate in responding to emerging threats. Furthermore, regarding ISO/SAE 21434 threat analysis and risk assessment, most studies focus on developing the TARA framework rather than its practical application in real-world scenarios. This might pose challenges for users during actual implementation. Thus, comprehensive and in-depth threat analysis and risk assessment for smart vehicles infotainment systems still need to be included in the current literature.

Therefore, this project not only conducts a thorough analysis of threats and assessment of cybersecurity risks in smart vehicles infotainment systems but also considers practical application scenarios and the evolving landscape of cybersecurity, offering a more practical and concrete application guide. This project aims to not only identify potential threats and vulnerabilities within infotainment systems, reducing threats from attackers and ensuring the safety of drivers and passengers, but also assist researchers and practitioners in the field of smart vehicles in more effectively addressing security challenges and enhancing the cybersecurity resilience of smart vehicles.

3. Methodology

This chapter will focus on the methodology of threat analysis and risk assessment for smart vehicles infotainment systems. It includes the use of secondary data and associated risks, data integration and analysis, thematic analysis, the selection of tools and techniques, and project execution and risks. The following sections will provide a detailed overview of each component.

3.1 Secondary Data and Risks

This project will employ secondary data, which brings about specific risks such as timeliness, quality, and completeness. For instance, certain academic databases pose challenges due to copyright or access restrictions, limiting access to critical information and compromising the project's comprehensiveness. Moreover, published literature might not encompass the latest infotainment systems threats technologies, or the research methods and outcomes may only align partially with the needs of this project.

To mitigate these risks, this project will prioritise selecting high-quality and representative literature from reputable databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. During the literature search, keywords like "TARA", "infotainment system", "autonomous vehicles", and "vulnerabilities" will be utilised to ensure alignment between research objectives and relevant literature. Additionally, pertinent information will be extracted from standards and guidelines provided by institutions like ISO and NIST. This project aims to collect and analyse around 50 relevant pieces of literature to understand and define the project's scope deeply. This number is based on the depth and breadth of the research and the feasibility within the project timeline.

3.2 Data Integration and Analysis

This project will accurately extract key data related to infotainment systems from the selected literature. This data will include various threat categories faced by infotainment systems, identified specific vulnerability types, and in-depth analyses of attackers' explicit classifications, motivations, and capabilities. Furthermore, this data will be integrated into a unified tabular format following established standards and guidelines, ensuring data consistency and ease of comprehension. This table will systematically present the threat types and vulnerabilities faced by infotainment systems, and identify various attacker

behaviour patterns, providing detailed insights into the threats and risks facing infotainment systems. By combining these data integration processes, this project strives to construct a more comprehensive and logically organised security analysis flow, serving as a robust experimental foundation for further refinement of the TARA framework.

3.3 Thematic Analysis

In this project, the methodology for threat analysis and risk assessment of smart vehicles infotainment systems is based on the ISO/SAE 21434 TARA framework. The adoption of the TARA framework is driven by its comprehensive and systematic approach, enabling a holistic analysis of security threats and potential risks associated with smart vehicles infotainment systems. This project begins by identifying assets of the infotainment systems through asset identification, which subsequently aids in recognising potential threat scenarios. Moreover, a thorough analysis of each asset's potential threats uses impact scoring, attack path analysis, and attack feasibility rating. Additionally, the collected data is utilised to determine the risk value of each asset, leading to the formulation of appropriate risk treatment strategies (ISO, 2021). Each threat analysis and risk assessment step requires different materials and produces distinct artefacts (Dantas et al., 2021) as follows:

- Asset Identification: This step aims to identify, categorise, and list relevant assets of the smart vehicles infotainment systems, describing their types and characteristics. The outcome of this step includes the infotainment systems Assets Categorisations List and Assets List.
- Threat Scenarios Identification: This step focuses on identifying and analysing potential threat scenarios against the infotainment systems. Within threat scenarios, elements such as threat, threat agent, motivation, and capability are examined in detail. The results of this step encompass the infotainment systems Threats List, Threat Agents List, Motivations List, Capabilities List, and Threat Scenarios List.
- Impact Rating: This step involves evaluating the impact of potential threat scenarios on the infotainment systems through impact scoring, assessing the potential level of impact on assets. The outcome includes the infotainment systems Impact Areas List and Impact Values List.

- Attack Path Analysis: This step elaborates on potential attack paths for assets of the infotainment systems and conducts analysis. Attack paths delve into different elements such as vulnerabilities/weaknesses and exploit Methods. The results include the infotainment systems Vulnerabilities/Weakness List, Exploit Methods List, and Attack Paths List.
- Attack Feasibility Rating: This step assesses the feasibility of attacks on assets of the infotainment systems through attack feasibility rating based on identified attack paths. The outcome comprises the infotainment systems Feasibility Areas List and Feasibility Values List.
- Risk Determination: This step combines impact scoring and attack feasibility rating, aligning with a risk matrix to determine the risk value of each asset. The results include the infotainment systems Risk Matrix and Risk Determinations List.
- Risk Treatment Decision: This step evaluates the attack paths for each asset of the infotainment systems and provides appropriate risk treatment strategies. The results encompass the infotainment systems Risk Treatment Decisions List.

Figure 1 illustrates the required and produced artefacts for different assessment steps in the TARA evaluation process (Dantas et al., 2021).

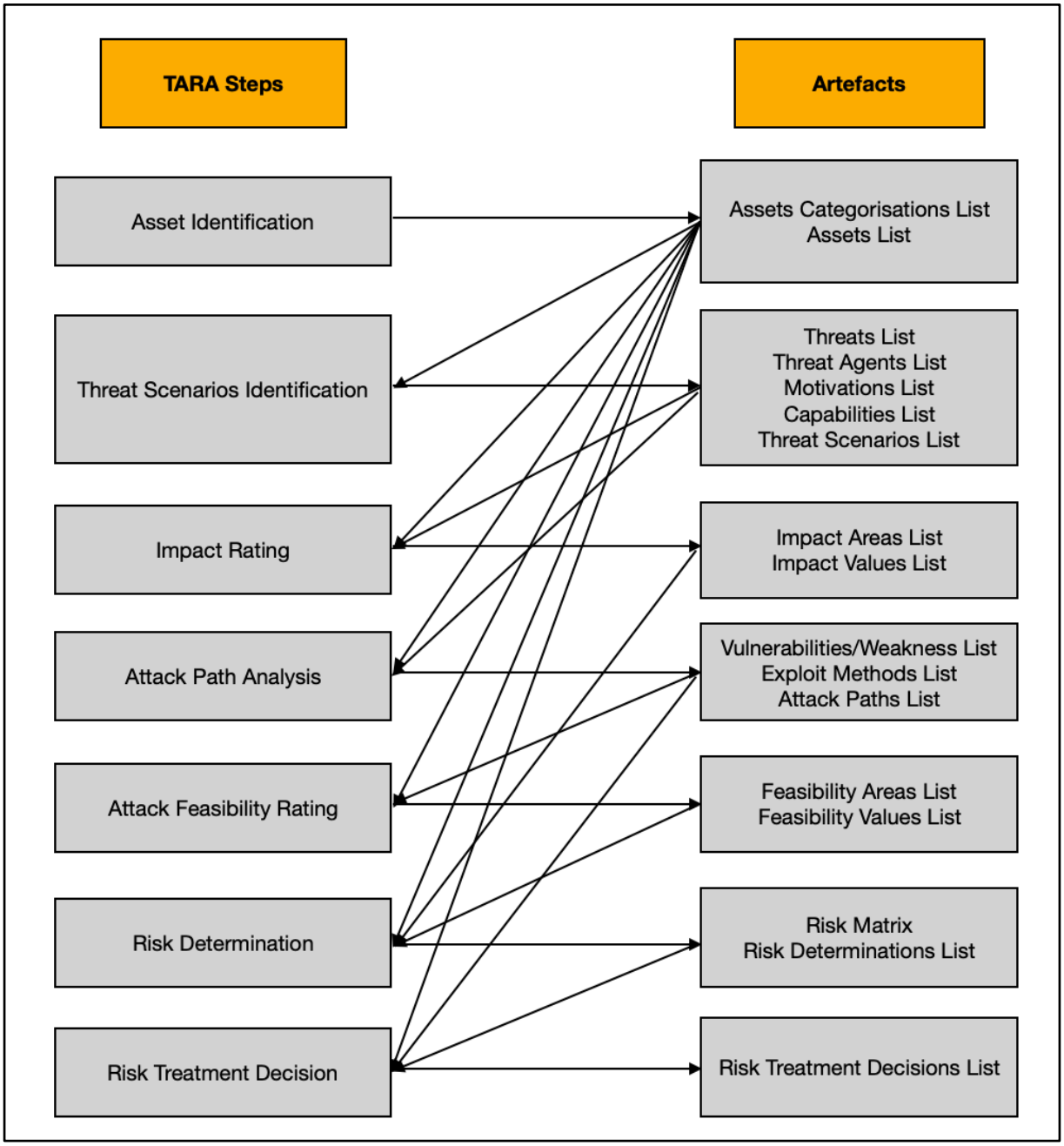


Figure 1. TARA Steps with Artefacts (Dantas et al., 2021)

3.4 Tools and Technologies Selection

During the data integration and analysis process in section 3.2 and thematic analysis in section 3.3, the choice of tools and technologies can significantly impact the research's accuracy, completeness, depth, breadth, and efficiency. Considering these factors, this project will use Excel as the data integration and analysis tool.

Excel is widely employed due to its versatility and flexibility (Guerrero, 2019). Its built-in functions enable rapid cross-referencing and analysis of infotainment systems data, allowing

for data presentation through automation. Furthermore, Excel's compatibility features are advantageous for data integration and analysis, especially considering the diversity of data sources and formats typically associated with infotainment systems. Excel can efficiently import data from these varied sources and facilitate customised formatting as needed, enhancing data integration and analysis efficiency.

3.5 Execution and Risks

The core of this project lies in presenting a comprehensive process and outcomes of threat analysis and risk assessment for smart vehicles infotainment systems, providing stakeholders with a clear and practical guide for such analyses. This guide deeply identifies systems assets, potential threats, and attack vectors, uncovering vulnerabilities that might be overlooked in fragmented analyses.

Furthermore, threat analysis and risk assessment methods must be adaptive rather than static due to the evolving cybersecurity threats and technologies. Therefore, this project employs an adaptive threat analysis and risk assessment approach. This approach efficiently integrates the data integration in section 3.2, emphasising the rapid iteration and adjustment of the TARA framework to address new threats and technological developments.

However, specific risks still exist even with the comprehensive and adaptive approach to threat analysis and risk assessment. When dealing with emerging technologies or complex multi-system attack strategies, there might be limitations in identifying threats within the threat analysis and risk assessment process. These risks are not inherent flaws in the method itself but are influenced by the quality and scope of the referenced literature. For instance, if the referenced literature needs more in-depth descriptions of certain technologies or attack strategies, the method's effectiveness could be constrained. Therefore, this project specialises in the evaluation and validation of research outcomes. This involves a thorough review of referenced literature and continuous monitoring and adjustment of the threat analysis and risk assessment process.

Through ongoing review, updates, and validation of research outcomes, this project ensures the integrity and adaptability of threat analysis and risk assessment methods in identifying and addressing security threats to infotainment systems. This further enhances cybersecurity measures. The project aims to empower automotive entities with the

necessary knowledge of infotainment systems cybersecurity, enabling them to formulate robust and effective protective strategies, ensuring the security of drivers, passengers, and the public in this era of vehicle-to-everything.

4. Results

This chapter will focus on the threat analysis of infotainment systems assets and risk assessment results. This chapter includes asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility rating, risk determination, and risk treatment decision (Dantas et al., 2021). The following will provide detailed descriptions of the outcomes generated in each section.

4.1 Asset Identification

This section will focus on the asset identification. Throughout the entire security risk assessment and threat analysis process, accurate identification and classification of assets are the primary steps and the foundation for ensuring efficiency and accuracy in subsequent work (Dantas et al., 2021).

Firstly, each infotainment system possesses unique characteristics, and as a result, it will face distinct threats and impacts. For example, a subsystem responsible for audio entertainment might face different threats compared to a subsystem responsible for vehicle navigation. When considering the impact, the consequences of disruption or data leakage in certain systems may be more severe than others due to the variations in asset characteristics and corresponding threats.

Furthermore, understanding asset identification and characteristics is essential when evaluating attack paths and feasibility. For instance, assets with external connectivity capabilities may have different potential threat paths and intrusion methods.

Additionally, during the stages of risk determination and risk treatment decision, thorough asset identification and classification enable the formulation of specific and clear asset risks and mitigation measures. In short, asset identification establishes the foundation of the threat analysis and risk assessment processes and ensures the entire process's precision and effectiveness, preventing ambiguity and misunderstandings from arising.

4.1.1 Asset Definition and Categorisation

This subsection will delve into the current infotainment systems (Meixner et al., 2017), categorised into five main domains based on their functions (Audio and Video

Entertainment, Navigation, Telephony and Messaging, Driver Assistance Systems, Internet and Wi-Fi), and list their significant subsystems along with descriptions.

Audio and Video Entertainment Systems: Providing audio and video entertainment for drivers and passengers.

- Terrestrial Radio Systems: These subsystems capture AM and FM broadcasts through ground-based wireless signals, featuring dynamic environments adaptation to ensure stable reception under various driving conditions.
- Satellite Radio Systems: These subsystems use high-orbit satellites to offer a broader reception range than traditional ground-based radio, ensuring signal quality and diverse channel selection.
- Media Playback Systems: These subsystems possess high-resolution decoding capabilities and can play a variety of audio and video formats from physical media to digital formats.
- Integrated Streaming Platforms: These platforms integrate popular music and video services, providing real-time and rich entertainment content.

Navigation Systems: Providing real-time navigation and mapping services, predicting and adjusting optimal routes.

- Satellite-based GPS Units: These subsystems provide real-time location tracking and route suggestions through advanced satellite technology and integrated ground data.
- Mapping and Visualisation Systems: These subsystems use geographic information systems technology, offering detailed and intuitive road and landmark visualisations, able to adjust displayed information in real-time.
- Traffic Data Systems: These subsystems can collect and analyse various traffic data to provide real-time traffic updates and predictions, aiding drivers in selecting the best routes.

Telephony and Messaging Systems: Providing built-in telephone and messaging functionalities in the vehicle.

- Bluetooth Connectivity Systems: These subsystems support audio and offer data transmissions, such as file sharing and contact synchronisation, while ensuring data security.

- Voice Command Systems: These subsystems can quickly understand and execute driver's commands using artificial intelligence and voice recognition technology.

Driver Assistance Systems: Providing driver assistance to enhance driving safety and convenience.

- Visual Systems: These subsystems utilise image processing technology, which can identify obstacles, pedestrians, or other vehicles on the roads and provide real-time feedback to the driver.
- Sensor Integration Systems: These subsystems Integrate various sensors, such as radar and infrared, which comprehensively monitor the vehicle's surrounding environment.
- Assistance Logic Systems: These subsystems can provide driving recommendations and warnings to the driver based on collected data.

Internet and Wi-Fi Systems: Providing internet connectivity, ensuring in-car network connectivity and data synchronisation.

- Connectivity Systems: These subsystems offer high-speed and stable network connections, enabling the vehicle to synchronise with external devices or the cloud.
- Over-the-Air (OTA) Update System: These subsystems update the vehicle software and operating systems in real-time to ensure functionality and security through encrypted channels.
- Integrated Browser and Apps: These subsystems are both the in-car browser and optimised applications, providing a smoother and more secure user experience.

Figure 2 and Figure 3 illustrate asset categorisations and descriptions of smart vehicles infotainment systems.

	Asset Categorisations (AC)	
No.	**Asset Categorisation (AC)**	**Description**
AC01	Audio and Video Entertainment Systems	These systems provide audio and video entertainment for drivers and passengers.These systems provide audio and video entertainment for drivers and passengers.
AC02	Navigation Systems	These systems provide real-time navigation and mapping services, predicting and adjusting optimal routes.
AC03	Telephony and Messaging Systems	These systems provide built-in telephone and messaging functionalities in the vehicle. These systems provide built-in telephone and messaging functionalities in the vehicle.
AC04	Driver Assistance Systems	These systems provide driver assistance to enhance driving safety and convenience.These systems provide driver assistance to enhance driving safety and convenience.
AC05	Internet and Wi-Fi Systems	These systems provide internet connectivity, ensuring in-car network connectivity and data synchronisation.

Figure 2. Asset Categorisations of Smart Vehicles Infotainment Systems

Assets (A)			
No.	Asset Categorisation (AC)	Asset (A)	Description
A01	Audio and Video Entertainment Systems	Terrestrial Radio Systems	These subsystems capture AM and FM broadcasts through ground-based wireless signals, featuring dynamic environment adaptation to ensure stable reception under various driving conditions.
A02	Audio and Video Entertainment Systems	Satellite Radio Systems	These subsystems use high-orbit satellites to offer a broader reception range than traditional ground-based radio, ensuring signal quality and diverse channel selection.
A03	Audio and Video Entertainment Systems	Media Playback Systems	These subsystems possess high-resolution decoding capabilities and can play a variety of audio and video formats from physical media to digital formats.
A04	Audio and Video Entertainment Systems	Integrated Streaming Platforms	These platforms integrate popular music and video services, providing real-time and rich entertainment content.
A05	Navigation Systems	Satellite-based GPS Units	These subsystems provide real-time location tracking and route suggestions through advanced satellite technology and integrated ground data.
A06	Navigation Systems	Mapping and Visualization Systems	These subsystems use geographic information systems technology, offering detailed and intuitive road and landmark visualisations, able to adjust displayed information in real-time.
A07	Navigation Systems	Traffic Data Systems	These subsystems can collect and analyse various traffic data to provide real-time traffic updates and predictions, aiding drivers in selecting the best routes.
A08	Telephony and Messaging Systems	Bluetooth Connectivity Systems	These subsystems support audio and offer data transmissions, such as file sharing and contact synchronisation, while ensuring data security.
A09	Telephony and Messaging Systems	Voice Command Systems	These subsystems can quickly understand and execute driver's commands using artificial intelligence and voice recognition technology.
A10	Driver Assistance Systems	Visual Systems	These subsystems utilise image processing technology, which can identify obstacles, pedestrians, or other vehicles on the roads and provide real-time feedback to the driver.
A11	Driver Assistance Systems	Sensor Integration Systems	These subsystems Integrate various sensors, such as radar and infrared, which comprehensively monitor the vehicle's surrounding environment.
A12	Driver Assistance Systems	Assistance Logic Systems	These subsystems can provide driving recommendations and warnings to the driver based on collected data.
A13	Internet and Wi-Fi Systems	Connectivity Systems	These subsystems offer high-speed and stable network connections, enabling the vehicle to synchronise with external devices or the cloud.
A14	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	These subsystems update the vehicle software and operating systems in real-time to ensure functionality and security through encrypted channels.
A15	Internet and Wi-Fi Systems	Integrated Browser and Apps	These subsystems are both the in-car browser and optimised applications, providing a smoother and more secure user experience.

Figure 3. Asset Descriptions of Smart Vehicles Infotainment Systems

4.2 Threat Scenarios Identification of Smart Vehicles Infotainment Systems

This section will focus on the stage of threat scenario identification. This stage involves identifying potential threats and analysing and combining the elements of threat scenarios (Threat, Threat Agent, Motivation, Capability) in depth (Dantas et al., 2021). This approach is crucial because considering only individual elements might provide a partial picture of threat risk. By considering all elements collectively, threat scenarios can be identified more accurately, leading to a more comprehensive risk assessment.

In this process, the first aspect to understand is the threat itself. For instance, a certain application might be vulnerable to the threat of denial of service (DoS), causing the application or browser to malfunction. Next, the consideration turns to threat agents, the individuals or organisations that could launch these attacks, for example, hackers, insiders, or competitors. Further, understanding the motivations of the threat agents is necessary, whether financial gain, espionage, political factors, or curiosity drives it. Lastly, evaluating the capability of the threat agents is crucial to determine whether they possess the technical skills and resources required for an attack.

Once all the combination elements have been thoroughly considered and analysed, this information can be integrated into complete threat scenarios. This process not only aids in a deeper understanding of all potential threat combinations but also provides a reference basis for the subsequent impact rating stage.

The following will outline the implementation process for all consideration elements (Threat, Threat Agent, Motivation, Capability) involved in threat scenario identification.

4.2.1 Threats

This subsection will focus on exploring and analysing potential threats to the infotainment systems. This project considers a constantly evolving threat landscape when analysing the

infotainment systems. Thus, the analysis employs the STRIDE model by Anwar et al. (2020) to ensure a comprehensive analysis of potential threats to the infotainment systems. This model is a recommended method within ISO/SAE 21434 (ISO, 2021), providing a structured approach to threat analysis. Through the six categories of the STRIDE model, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Anwar et al., 2020), threats can be comprehensively assessed from various perspectives, including their scope, origins, and potential impacts. Furthermore, the STRIDE model exhibits strong adaptability, covering multiple dimensions of threat types, making it highly suitable for analysing infotainment systems.

The following illustrates the relevance of the STRIDE threat model to smart vehicles infotainment systems (Anwar et al., 2020):

- Spoofing: This threat refers to the act of impersonating entities or services to deceive the systems or end-users. For example, an attacker might mimic the vehicle update systems and send forged software update notifications to users. This impersonation threatens environments that rely on trust for systems and user security.
- Tampering: This threat involves unauthorised alteration of data or systems functionality. For instance, an attacker might perform a man-in-the-middle attack to modify navigation systems route guidance, leading the driver to an unexpected destination. In infotainment systems, any functionality reliant on the integrity of input data could be affected.
- Repudiation: This threat refers to the act of a party denying that they have engaged in certain actions, even though evidence suggests otherwise. For example, an attacker might manipulate vehicles infotainment systems settings and deny any changes despite the systems logs indicating the modifications. This type of threat undermines trust in systems interactions.
- Information Disclosure: This threat involves unauthorised access and distributing sensitive information. For example, an attacker could read contact lists or recent navigation destinations within the vehicles through vulnerabilities. User privacy is a major concern in smart vehicles, making the consequences of such breaches particularly severe.

- Denial of Service (DoS): This threat focuses on disrupting the availability of services or functionalities. For instance, an attacker could overwhelm infotainment systems with a significant volume of requests, causing regular functions to become inaccessible.
- Elevation of Privilege: This threat involves unauthorised privileges within a system. For example, an attacker exploits a vulnerability in the infotainment systems to escalate from regular user to administrator privileges, thereby gaining full control over the system.

Figure 4 illustrates the structured threat assessment matrix of smart vehicles infotainment systems assets using the STRIDE model (Anwar et al., 2020).

Threats (T)				
No.	**Asset (A)**	**Threat (T) *[STRIDE]***	**Desciption**	**Combination**
T01	Terrestrial Radio Systems	Spoofing	Faking terrestrial broadcasts to send false messages or advertisements.	T01. Terrestrial Radio Systems. Spoofing
T02	Terrestrial Radio Systems	Tampering	Intercepting and altering terrestrial radio signals.	T02. Terrestrial Radio Systems. Tampering
T03	Terrestrial Radio Systems	Repudiation	Denying changes made after unauthorized broadcasting activities.	T03. Terrestrial Radio Systems. Repudiation
T04	Terrestrial Radio Systems	Information Disclosure	Eavesdropping on terrestrial radio communications to obtain sensitive information.	T04. Terrestrial Radio Systems. Information Disclosure
T05	Terrestrial Radio Systems	Denial of Service	Interfering with terrestrial broadcasts rendering them inoperative.	T05. Terrestrial Radio Systems. Denial of Service
T06	Terrestrial Radio Systems	Elevation of Privilege	Exploiting vulnerabilities in broadcasting systems to gain higher-level access.	T06. Terrestrial Radio Systems. Elevation of Privilege
T07	Satellite Radio Systems	Spoofing	Faking satellite radio signals to send false messages.	T07. Satellite Radio Systems. Spoofing
T08	Satellite Radio Systems	Tampering	Intercepting and altering satellite radio signals.	T08. Satellite Radio Systems. Tampering
T09	Satellite Radio Systems	Repudiation	Denying changes made after unauthorized broadcasting activities.	T09. Satellite Radio Systems. Repudiation
T10	Satellite Radio Systems	Information Disclosure	Eavesdropping on satellite radio communications to obtain sensitive information.	T10. Satellite Radio Systems. Information Disclosure
T11	Satellite Radio Systems	Denial of Service	Interfering with satellite radio systems making them unable to receive signals.	T11. Satellite Radio Systems. Denial of Service
T12	Satellite Radio Systems	Elevation of Privilege	Exploiting vulnerabilities in satellite radio systems to gain higher-level access.	T12. Satellite Radio Systems. Elevation of Privilege
T13	Media Playback Systems	Spoofing	Faking media content or metadata.	T13. Media Playback Systems. Spoofing
T14	Media Playback Systems	Tampering	Inserting malicious content or modifying media during playback.	T14. Media Playback Systems. Tampering
T15	Media Playback Systems	Repudiation	Modifying or deleting playback records.	T15. Media Playback Systems. Repudiation
T16	Media Playback Systems	Information Disclosure	Accessing playback history or user preferences.	T16. Media Playback Systems. Information Disclosure
T17	Media Playback Systems	Denial of Service	Crashing or freezing the media playback system.	T17. Media Playback Systems. Denial of Service
T18	Media Playback Systems	Elevation of Privilege	Exploiting vulnerabilities to change media settings or control playback.	T18. Media Playback Systems. Elevation of Privilege
T19	Integrated Streaming Platforms	Spoofing	Faking streaming content or metadata, trying to affect what users see.	T19. Integrated Streaming Platforms. Spoofing
T20	Integrated Streaming Platforms	Tampering	Inserting malicious ads or content into streams.	T20. Integrated Streaming Platforms. Tampering
T21	Integrated Streaming Platforms	Repudiation	Deleting or altering users' playback history or preference settings.	T21. Integrated Streaming Platforms. Repudiation
T22	Integrated Streaming Platforms	Information Disclosure	Eavesdropping on streaming communications to obtain user data or playback content.	T22. Integrated Streaming Platforms. Information Disclosure
T23	Integrated Streaming Platforms	Denial of Service	Disrupting streaming services, causing interruptions or slowness.	T23. Integrated Streaming Platforms. Denial of Service
T24	Integrated Streaming Platforms	Elevation of Privilege	Exploiting vulnerabilities to try changing streaming settings or controlling playback.	T24. Integrated Streaming Platforms. Elevation of Privilege
T25	Satellite-based GPS Units	Spoofing	Sending fake GPS signals attempting to mislead vehicles.	T25. Satellite-based GPS Units. Spoofing
T26	Satellite-based GPS Units	Tampering	Modifying GPS data to affect navigation outcomes.	T26. Satellite-based GPS Units. Tampering
T27	Satellite-based GPS Units	Repudiation	Deleting or altering navigation history.	T27. Satellite-based GPS Units. Repudiation
T28	Satellite-based GPS Units	Information Disclosure	Eavesdropping on GPS communications to obtain vehicle location data.	T28. Satellite-based GPS Units. Information Disclosure
T29	Satellite-based GPS Units	Denial of Service	Interfering with GPS signals, rendering them ineffective or inaccurate.	T29. Satellite-based GPS Units. Denial of Service
T30	Satellite-based GPS Units	Elevation of Privilege	Exploiting vulnerabilities in the GPS system to attempt to control other vehicle systems.	T30. Satellite-based GPS Units. Elevation of Privilege
T31	Mapping and Visualization Systems	Spoofing	Faking map data or visualisation content.	T31. Mapping and Visualization Systems. Spoofing
T32	Mapping and Visualization Systems	Tampering	Modifying maps or location information.	T32. Mapping and Visualization Systems. Tampering
T33	Mapping and Visualization Systems	Repudiation	Deleting or altering users' map history or preference settings.	T33. Mapping and Visualization Systems. Repudiation
T34	Mapping and Visualization Systems	Information Disclosure	Accessing users' map query history.	T34. Mapping and Visualization Systems. Information Disclosure
T35	Mapping and Visualization Systems	Denial of Service	Disabling or inaccurately displaying map or visualisation functions.	T35. Mapping and Visualization Systems. Denial of Service
T36	Mapping and Visualization Systems	Elevation of Privilege	Exploiting vulnerabilities to change map settings or control other features.	T36. Mapping and Visualization Systems. Elevation of Privilege
T37	Traffic Data Systems	Spoofing	Faking traffic data, leading to navigation misjudgment.	T37. Traffic Data Systems. Spoofing
T38	Traffic Data Systems	Tampering	Altering traffic information, such as road conditions, road closures, or accident news.	T38. Traffic Data Systems. Tampering
T39	Traffic Data Systems	Repudiation	Deleting or altering traffic data queried by users.	T39. Traffic Data Systems. Repudiation
T40	Traffic Data Systems	Information Disclosure	Accessing users' traffic query history.	T40. Traffic Data Systems. Information Disclosure
T41	Traffic Data Systems	Denial of Service	Disrupting traffic data services, rendering them inoperative.	T41. Traffic Data Systems. Denial of Service
T42	Traffic Data Systems	Elevation of Privilege	Exploiting vulnerabilities to change traffic settings or control other features.	T42. Traffic Data Systems. Elevation of Privilege
T43	Bluetooth Connectivity Systems	Spoofing	Faking Bluetooth devices trying to pair with the infotainment system.	T43. Bluetooth Connectivity Systems. Spoofing
T44	Bluetooth Connectivity Systems	Tampering	Altering communication data during transmission.	T44. Bluetooth Connectivity Systems. Tampering
T45	Bluetooth Connectivity Systems	Repudiation	Deleting or altering Bluetooth pairing history.	T45. Bluetooth Connectivity Systems. Repudiation
T46	Bluetooth Connectivity Systems	Information Disclosure	Eavesdropping on Bluetooth communications to obtain communication content.	T46. Bluetooth Connectivity Systems. Information Disclosure
T47	Bluetooth Connectivity Systems	Denial of Service	Interfering with Bluetooth signals, disrupting communications.	T47. Bluetooth Connectivity Systems. Denial of Service
T48	Bluetooth Connectivity Systems	Elevation of Privilege	Exploiting Bluetooth vulnerabilities to attempt control of the infotainment system.	T48. Bluetooth Connectivity Systems. Elevation of Privilege
T49	Voice Command Systems	Spoofing	Using recordings to mimic the user's voice for unauthorized commands.	T49. Voice Command Systems. Spoofing
T50	Voice Command Systems	Tampering	Inserting or modifying commands during voice command transmission.	T50. Voice Command Systems. Tampering
T51	Voice Command Systems	Repudiation	Deleting or altering voice command history.	T51. Voice Command Systems. Repudiation
T52	Voice Command Systems	Information Disclosure	Eavesdropping on voice commands.	T52. Voice Command Systems. Information Disclosure
T53	Voice Command Systems	Denial of Service	Disrupting voice recognition, making it unable to identify commands or responding inappropriately.	T53. Voice Command Systems. Denial of Service
T54	Voice Command Systems	Elevation of Privilege	Exploiting system vulnerabilities via voice commands to conduct unauthorized operations.	T54. Voice Command Systems. Elevation of Privilege
T55	Visual Systems	Spoofing	Faking videos or images in an attempt to mislead drivers.	T55. Visual Systems. Spoofing
T56	Visual Systems	Tampering	Altering or manipulating video streams.	T56. Visual Systems. Tampering
T57	Visual Systems	Repudiation	Deleting or altering video history.	T57. Visual Systems. Repudiation
T58	Visual Systems	Information Disclosure	Eavesdropping on video data.	T58. Visual Systems. Information Disclosure
T59	Visual Systems	Denial of Service	Interfering with video streams, rendering them ineffective or inaccurate.	T59. Visual Systems. Denial of Service
T60	Visual Systems	Elevation of Privilege	Exploiting vulnerabilities in the video system to attempt to control other features.	T60. Visual Systems. Elevation of Privilege
T61	Sensor Integration Systems	Spoofing	Faking sensor outputs.	T61. Sensor Integration Systems. Spoofing
T62	Sensor Integration Systems	Tampering	Modifying sensor data.	T62. Sensor Integration Systems. Tampering
T63	Sensor Integration Systems	Repudiation	Changing or deleting sensor history data.	T63. Sensor Integration Systems. Repudiation
T64	Sensor Integration Systems	Information Disclosure	Accessing sensor data.	T64. Sensor Integration Systems. Information Disclosure
T65	Sensor Integration Systems	Denial of Service	Interfering with sensors, rendering them inoperative.	T65. Sensor Integration Systems. Denial of Service
T66	Sensor Integration Systems	Elevation of Privilege	Exploiting sensor vulnerabilities to change settings or control other features.	T66. Sensor Integration Systems. Elevation of Privilege
T67	Assistance Logic Systems	Spoofing	Faking system prompts or warnings.	T67. Assistance Logic Systems. Spoofing
T68	Assistance Logic Systems	Tampering	Altering the decision-making process of the assistance logic.	T68. Assistance Logic Systems. Tampering
T69	Assistance Logic Systems	Repudiation	Deleting or altering system operation records.	T69. Assistance Logic Systems. Repudiation
T70	Assistance Logic Systems	Information Disclosure	Accessing system operation and decision logs.	T70. Assistance Logic Systems. Information Disclosure
T71	Assistance Logic Systems	Denial of Service	Disrupting the operation of the assistance logic system, causing it to malfunction or make wrong decisions.	T71. Assistance Logic Systems. Denial of Service
T72	Assistance Logic Systems	Elevation of Privilege	Exploiting vulnerabilities in the assistance logic system to gain unauthorized access or control.	T72. Assistance Logic Systems. Elevation of Privilege
T73	Connectivity Systems	Spoofing	Forging connection requests or masquerading as a trusted device.	T73. Connectivity Systems. Spoofing
T74	Connectivity Systems	Tampering	Modifying communication content during data transmission.	T74. Connectivity Systems. Tampering
T75	Connectivity Systems	Repudiation	Deleting or altering connection logs.	T75. Connectivity Systems. Repudiation
T76	Connectivity Systems	Information Disclosure	Eavesdropping on communications to obtain transmitted data.	T76. Connectivity Systems. Information Disclosure
T77	Connectivity Systems	Denial of Service	Disrupting the connection, causing it to break.	T77. Connectivity Systems. Denial of Service
T78	Connectivity Systems	Elevation of Privilege	Exploiting vulnerabilities in the connectivity system to gain higher system access rights.	T78. Connectivity Systems. Elevation of Privilege
T79	Over-the-Air (OTA) Update Systems	Spoofing	Forging update requests or providing counterfeit update packages.	T79. Over-the-Air (OTA) Update Systems. Spoofing
T80	Over-the-Air (OTA) Update Systems	Tampering	Inserting malicious code during the OTA update process.	T80. Over-the-Air (OTA) Update Systems. Tampering
T81	Over-the-Air (OTA) Update Systems	Repudiation	Deleting or altering update history.	T81. Over-the-Air (OTA) Update Systems. Repudiation
T82	Over-the-Air (OTA) Update Systems	Information Disclosure	Acquiring the content of OTA updates.	T82. Over-the-Air (OTA) Update Systems. Information Disclosure
T83	Over-the-Air (OTA) Update Systems	Denial of Service	Causing system crashes or failures to start through OTA updates.	T83. Over-the-Air (OTA) Update Systems. Denial of Service
T84	Over-the-Air (OTA) Update Systems	Elevation of Privilege	Exploiting vulnerabilities in the OTA update system to install unauthorized software.	T84. Over-the-Air (OTA) Update Systems. Elevation of Privilege
T85	Integrated Browser and Apps	Spoofing	Forging content of applications or websites in an attempt to mislead users.	T85. Integrated Browser and Apps. Spoofing
T86	Integrated Browser and Apps	Tampering	Modifying the operational logic of an application or browser.	T86. Integrated Browser and Apps. Tampering
T87	Integrated Browser and Apps	Repudiation	Deleting or altering usage records of the application.	T87. Integrated Browser and Apps. Repudiation
T88	Integrated Browser and Apps	Information Disclosure	Eavesdropping on app or browser communications to obtain user data.	T88. Integrated Browser and Apps. Information Disclosure
T89	Integrated Browser and Apps	Denial of Service	Disrupting the app or browser, causing it to become nonfunctional or crash.	T89. Integrated Browser and Apps. Denial of Service
T90	Integrated Browser and Apps	Elevation of Privilege	Exploiting vulnerabilities in the app or browser to gain higher system access rights.	T90. Integrated Browser and Apps. Elevation of Privilege

Figure 4. STRIDE Model of Smart Vehicles Infotainment Systems (Anwar et al., 2020)

4.2.2 Threat Agents

This subsection will focus on exploring and analysing potential threat agents and their characteristics. Threat agents are entities capable of posing threats to systems or data. These entities range from individual attackers and organised crime groups to organisations with specific purposes (Bugeja et al., 2017).

Each threat agent possesses unique behavioural and operational characteristics, leading to potential variations in behaviours and objectives concerning infotainment systems in threat scenarios. For instance, organised crime groups might exploit vulnerabilities in infotainment systems for economic theft, particularly concerning financial information related to vehicle owners. On the other hand, terrorist organisations might seek to exploit vulnerabilities in these systems to disrupt vehicle operations or compromise data critical to vehicle safety, causing widespread chaos or harm.

The scope of threat agents is extensive, ranging from individual attackers to specific organisations. The following list the classification and description of various threat agents to vehicles infotainment systems (Bugeja et al., 2017):

- Hackers: Experts with deep technical backgrounds familiar with the specific workings of infotainment systems. They specialise in identifying and exploiting systems vulnerabilities for various attacks.
- Script Kiddies: Rely heavily on ready-made tools available on the internet, without a full understanding of their operational principles. While their expertise in infotainment systems may be limited, random attack behaviours can still pose threats.
- Insiders: Individuals who may be current or former employees of vehicle manufacturers, possessing insights into the internal design and functionality of infotainment systems. Their in-depth knowledge makes them potential threats, especially when performing unauthorised actions.
- Nation-State Actors: Backed by national governments, these actors have ample resources to conduct in-depth research targeting infotainment systems. Their goals could range from intelligence gathering to sabotage or other political objectives.
- Organised Crime Groups: Highly organised groups with specific technical capabilities, potentially focused on theft of valuables or information from vehicles owners infotainment systems.
- Terrorists: Primarily aimed at creating panic and chaos. By manipulating infotainment systems, they might attempt to influence vehicle operations or acquire sensitive information.

- Competitors: Interested in technical details, features, or market strategies of vehicles infotainment systems to optimise their products or weaken competitors' positions.
- Hactivists: Motivated by social or political causes. By attacking the infotainment systems of specific brands or companies, they aim to draw attention to certain issues.
- Irresponsible Researchers: Seek vulnerabilities in infotainment systems, but may publicly disclose these vulnerabilities without proper channels, exposing the systems to risks.
- Privileged Users: Vehicle technicians or specific employees may possess advanced access privileges, enabling them to perform operations differently from regular users, but this also introduces potential risks of misuse of privileges.

Figure 5 illustrates the threat agents categorisations and descriptions of smart vehicles infotainment systems (Bugeja et al., 2017).

	Threat Agents (TA)		
No.	**Threat Agent (TA)**	**Description**	**Combination**
TA01	Hackers	Experts with deep technical backgrounds familiar with the specific workings of infotainment systems. They specialise in identifying and exploiting systems vulnerabilities for various attacks.	TA01. Hackers
TA02	Script Kiddies	Rely heavily on ready-made tools available on the internet, without a full understanding of their operational principles. While their expertise in infotainment systems may be limited, random attack behaviours can still pose threats.	TA02. Script Kiddies
TA03	Insiders	Individuals who may be current or former employees of vehicle manufacturers, possessing insights into the internal design and functionality of infotainment systems.	TA03. Insiders
TA04	Nation-State Actors	Backed by national governments, these actors have ample resources to conduct in-depth research targeting infotainment systems. Their goals could range from intelligence gathering to sabotage or other political objectives.	TA04. Nation-State Actors
TA05	Organised Crime Groups	Highly organised groups with specific technical capabilities, potentially focused on theft of valuables or information from vehicle owners using infotainment systems.	TA05. Organised Crime Groups
TA06	Terrorists	Primarily aimed at creating panic and chaos. By manipulating infotainment systems, they might attempt to influence vehicle operations or acquire sensitive information.	TA06. Terrorists
TA07	Competitors	Interested in technical details, features, or market strategies of vehicle infotainment systems to optimise their products or weaken competitors' positions.	TA07. Competitors
TA08	Hacktivists	Motivated by social or political causes. By attacking the infotainment systems of specific brands or companies, they aim to draw attention to certain issues.	TA08. Hacktivists
TA09	Irresponsible Researchers	Seek vulnerabilities in infotainment systems, but may publicly disclose these vulnerabilities without proper channels, exposing the systems to risks.	TA09. Irresponsible Researchers
TA10	Privileged Users	Vehicle technicians or specific employees may possess advanced access privileges, enabling them to perform operations differently from regular users, but this also introduces potential risks of misuse of privileges.	TA10. Privileged Users

Figure 5. Threat Agents of Smart Vehicles Infotainment Systems (Bugeja et al., 2017)

4.2.3 Motivations

This subsection will focus on the driving motivations behind potential attackers. The in-depth analysis in subsection 4.2.2 has already demonstrated the diverse motivations behind attackers, which directly influence their attack patterns and targets (Bugeja et al., 2017).

Motivations are the core of an attacker's behaviour, determining how, when, and why they target specific information systems. For instance, attackers motivated by financial gain may target user financial data within the infotainment systems. Such attackers seek opportunities that can get quick financial returns, like breaching security defences to steal credit card information. On the other hand, attackers driven by specific political might view the infotainment systems as a tool for propaganda or achieving other political objectives, which could involve large-scale attacks to destroy the entire system.

The motivations behind attackers span widely, revealing the reasons for choosing specific targets or strategies. The following categorisation and descriptions are based on the various motivations behind different types of attackers:

- Financial Gain: Attackers may seek economic returns, such as stealing credit card information from vehicles infotainment systems or launching ransomware attacks using the systems to demand ransom payments from vehicle owners.
- Espionage: Corporate or state spies might be interested in technical data or user behaviour data within the vehicles infotainment systems, particularly information related to navigation, communication, and other advanced features.
- Ideological Beliefs: Motivated by certain beliefs, attackers may target vehicles of specific brands, especially those with opposing stances on certain issues compared to the attacker's beliefs.
- Revenge: A disgruntled former employee or customer might launch an attack on the company's vehicles infotainment systems as revenge against the company.
- Curiosity: Novice attackers or script kiddies might engage in exploratory attacks out of curiosity about the vehicles infotainment systems.
- Notoriety: By launching attention-grabbing attacks on well-known vehicle brands' infotainment systems, attackers can gain recognition within the hacker community.
- Social or Political Activism: Hactivists might leverage vehicles infotainment systems as a medium to convey their message, drawing attention to certain social or political issues.
- Sabotage: Attackers might target the vehicles infotainment systems to hinder its proper functions, resulting in potential harm to users.
- Competitive Advantage: To gain a competitive edge in the vehicle market, certain companies might attempt to compromise or extract valuable data from a rival's vehicles infotainment systems for an advantage.
- Fear or Coercion: Individuals might be under external threats or influence, forcing them to compromise the infotainment systems to protect their interests.

Figure 6 illustrates the classifications and descriptions of motivations of smart vehicles infotainment systems.

	Motivations (M)		
No.	Motivation (M)	Description	Combination
M01	Financial Gain	Attackers may seek economic returns, such as stealing credit card information from vehicle infotainment systems or launching ransomware attacks using the systems to demand r	M01. Financial Gain
M02	Espionage	Corporate or state spies might be interested in technical data or user behaviour data within the vehicle infotainment system, particularly information related to navigation, communic	M02. Espionage
M03	Ideological Beliefs	Motivated by certain beliefs, attackers may target vehicles of specific brands, especially those with opposing stances on certain issues compared to the attacker's beliefs.	M03. Ideological Beliefs
M04	Revenge	A disgruntled former employee or customer might launch an attack on the company's vehicle infotainment systems as a form of retaliation against the company.	M04. Revenge
M05	Curiosity	Novice attackers or script kiddies might engage in exploratory attacks out of curiosity about the vehicle infotainment system.	M05. Curiosity
M06	Notoriety	By launching attention-grabbing attacks on well-known vehicle brands' infotainment systems, attackers can gain recognition within the hacker community.	M06. Notoriety
M07	Social or Political Activism	Hactivists might leverage vehicle infotainment systems as a medium to convey their message, drawing attention to certain societal or political issues.	M07. Social or Political Activism
M08	Sabotage	Attackers might target the vehicle infotainment systems to hinder its proper function, resulting in disturbances or potential harm to users.	M08. Sabotage
M09	Competitive Advantage	To gain a competitive edge in the vehicle market, certain companies might attempt to compromise or extract valuable data from a rival's infotainment systems for an advantage.	M09. Competitive Advantage
M10	Fear or Coercion	Individuals might be under external threats or influence, compelling them to compromise the infotainment systems to safeguard their interests or wellbeing.	M10. Fear or Coercion

Figure 6. Motivations of Attackers of Smart Vehicles Infotainment Systems

4.2.4 Capabilities

This subsection will focus on exploring the capabilities of potential attackers. Attacker capabilities are the technical skills and resources required to launch effective attacks (Bugeja et al., 2017). The information provided in subsections 4.2.2 and 4.2.3 shows that various threat agents have unique motivations and possess various technical skills and resources. These capabilities directly determine their methods and targets of attack. For example, an attacker with network skills may conduct sophisticated cyber-attacks, while a human skilled attacker may use social engineering tactics. In this project, attackers' abilities are categorised into four key domains: Network Capabilities, Software Capabilities, Physical Capabilities, and Social Engineering. These four domains encompass various techniques attackers may employ, such as man-in-the-middle attacks, malicious software installation, hardware tampering, and phishing attacks.

The following will delve into each capability domain and its associated attack techniques:

Network-based Capabilities: This domain involves attacks on the communication interfaces and protocols of the infotainment systems. In these techniques, the attacker targets the data flow between the infotainment systems and other systems to intercept, modify, or disrupt these communications.

- Packet Injection: Attackers can inject malicious packets into the communication of the infotainment systems, leading to hijacking certain functions or weakening the systems. For example, disrupting the vehicle navigation systems to provide incorrect directions.
- Wireless Sniffing: Infotainment systems often utilise wireless technologies such as Wi-Fi or Bluetooth. Attackers can detect and intercept these signals, attempting to gather sensitive data like destinations or contact lists (Josephlal and Adepu, 2019).
- Man-in-the-Middle Attacks: Attackers can intercept communication between the vehicle and external servers, modify its content, and transmit it again. For instance, when the

vehicle attempts to update maps from the cloud, attackers can modify map data, leading to navigation misdirection (El-Rewini et al., 2020).

Software-based Capabilities: This domain involves vulnerabilities within the infotainment systems software. This includes exploiting programming errors, software configurations, or inherent design flaws in applications. Attackers often aim to gain unauthorised access, control functions, or retrieve sensitive information from the systems.

- Exploiting Software Vulnerabilities: Attackers search for weaknesses in software and attempt to gain control of the systems through these vulnerabilities. For example, exploiting an unpatched vulnerability to take control of the vehicle audio and video entertainment systems (Jeong et al., 2023).
- Malware Installation: Through USB ports or other external storage devices, attackers may attempt to install malicious software on the infotainment systems, allowing them to monitor user behaviour or steal data stored within the systems (Costantino et al., 2018).
- Reverse Engineering: Attackers can analyse the infotainment systems software, uncover its operation principles, and discover new attack methods as a result.

Physical-based Capabilities: This domain involves physical interactions with the vehicles infotainment systems. Attackers may manipulate hardware components, connect malicious devices, or exploit physically accessible entry points.

- Physical Device Manipulation: If attackers can directly access the vehicles, they may attempt to physically manipulate certain parts of the infotainment systems, such as connecting external devices to systems ports (Pan et al., 2017).
- Hardware Tampering: Attackers can replace or modify certain hardware components of the infotainment systems, such as changing storage devices or modifying displays.

Social Engineering: This domain involves manipulating human psychology rather than exploiting systems vulnerabilities. Attackers deceive or manipulate individuals to perform actions related to the infotainment systems to disclose confidential information (Salahdine and Kaabouch, 2019).

- Deceptive Persuasion: Through deception or manipulation, attackers might induce vehicle owners or employees of vehicle manufacturers to grant them access to infotainment systems and get sensitive information.
- Phishing Attacks: Attackers attempt to deceive users into providing sensitive information through phishing emails, including fake infotainment systems update notifications, to gain sensitive information.

Figure 7 illustrates the classification and descriptions of capabilities to the smart vehicles infotainment systems.

Capabilities (C)				
No.	Capability Domain (CD)	Capability (C)	Description	Combination
C01	Network-based	Packet Injection	Attackers can inject malicious packets into the communication of the infotainment system, leading to hijacking certain functions or destabilising the system. For e	C01. Network-based. Packet Injection
C02	Network-based	Wireless Sniffing	Infotainment systems often utilise wireless technologies such as Wi-Fi or Bluetooth. Attackers can detect and intercept these signals, attempting to gather sensiti	C02. Network-based. Wireless Sniffing
C03	Network-based	Man-in-the-Middle Attacks	Attackers can intercept communication between the vehicle and external servers, modify its content, and transmit it again. For instance, when the vehicle attempt	C03. Network-based. Man-in-the-Middle Attacks
C04	Software-based	Exploiting Software Vulnerabilities	Attackers search for weaknesses in software and attempt to gain control of the systems through these vulnerabilities. For example, exploiting an unpatched vulne	C04. Software-based. Exploiting Software Vulnerabilities
C05	Software-based	Malware Installation	Through USB ports or other external storage devices, attackers may attempt to install malicious software on the infotainment system, allowing them to monitor use	C05. Software-based. Malware Installation
C06	Software-based	Reverse Engineering	Attackers can analyse the infotainment system's software, uncover its operation principles, and discover new attack methods as a result.	C06. Software-based. Reverse Engineering
C07	Physical-based	Physical Device Manipulation	If attackers can directly access the vehicle, they may attempt to physically manipulate certain parts of the infotainment system, such as connecting external devi	C07. Physical-based. Physical Device Manipulation
C08	Physical-based	Hardware Tampering	Attackers can replace or modify certain hardware components of the infotainment system, such as changing storage devices or modifying displays.	C08. Physical-based. Hardware Tampering
C09	Social Engineering	Deceptive Persuasion	Through deception or manipulation, attackers might induce vehicle owners or employees of vehicle manufacturers to grant them access to infotainment systems a	C09. Social Engineering. Deceptive Persuasion
C10	Social Engineering	Phishing Attacks	Attackers attempt to deceive users into providing sensitive information through phishing emails, including fake infotainment system update notifications.	C10. Social Engineering. Phishing Attacks

Figure 7. Capabilities of Attackers of Smart Vehicles Infotainment Systems

4.2.5 Threat Scenarios

This subsection will focus on threat scenarios related to smart vehicles infotainment systems. By integrating sections 4.2.1 through 4.2.4, a variety of threat scenarios can be derived through cross-pairing.

Figure 8 illustrates the threat scenarios of the smart vehicles infotainment systems.

Threat Scenarios (TS)				
No.	**Threat (T)**	**Threat Agent (TA)**	**Motivation (M)**	**Capacity (C)**
TS01	T01. Terrestrial Radio Systems. Spoofing	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS02	T02. Terrestrial Radio Systems. Tampering	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS03	T03. Terrestrial Radio Systems. Repudiation	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS04	T04. Terrestrial Radio Systems. Information Disclosure	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS05	T05. Terrestrial Radio Systems. Denial of Service	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS06	T06. Terrestrial Radio Systems. Elevation of Privilege	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS07	T07. Satellite Radio Systems. Spoofing	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS08	T08. Satellite Radio Systems. Tampering	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS09	T09. Satellite Radio Systems. Repudiation	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS10	T10. Satellite Radio Systems. Information Disclosure	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS11	T11. Satellite Radio Systems. Denial of Service	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS12	T12. Satellite Radio Systems. Elevation of Privilege	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS13	T13. Media Playback Systems. Spoofing	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS14	T14. Media Playback Systems. Tampering	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS15	T15. Media Playback Systems. Repudiation	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS16	T16. Media Playback Systems. Information Disclosure	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS17	T17. Media Playback Systems. Denial of Service	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS18	T18. Media Playback Systems. Elevation of Privilege	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS19	T19. Integrated Streaming Platforms. Spoofing	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS20	T20. Integrated Streaming Platforms. Tampering	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS21	T21. Integrated Streaming Platforms. Repudiation	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS22	T22. Integrated Streaming Platforms. Information Disclosure	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS23	T23. Integrated Streaming Platforms. Denial of Service	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS24	T24. Integrated Streaming Platforms. Elevation of Privilege	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS25	T25. Satellite-based GPS Units. Spoofing	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS26	T26. Satellite-based GPS Units. Tampering	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS27	T27. Satellite-based GPS Units. Repudiation	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS28	T28. Satellite-based GPS Units. Information Disclosure	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS29	T29. Satellite-based GPS Units. Denial of Service	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS30	T30. Satellite-based GPS Units. Elevation of Privilege	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS31	T31. Mapping and Visualization Systems. Spoofing	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS32	T32. Mapping and Visualization Systems. Tampering	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS33	T33. Mapping and Visualization Systems. Repudiation	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS34	T34. Mapping and Visualization Systems. Information Disclosure	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS35	T35. Mapping and Visualization Systems. Denial of Service	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS36	T36. Mapping and Visualization Systems. Elevation of Privilege	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS37	T37. Traffic Data Systems. Spoofing	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS38	T38. Traffic Data Systems. Tampering	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS39	T39. Traffic Data Systems. Repudiation	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS40	T40. Traffic Data Systems. Information Disclosure	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS41	T41. Traffic Data Systems. Denial of Service	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS42	T42. Traffic Data Systems. Elevation of Privilege	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS43	T43. Bluetooth Connectivity Systems. Spoofing	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS44	T44. Bluetooth Connectivity Systems. Tampering	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS45	T45. Bluetooth Connectivity Systems. Repudiation	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS46	T46. Bluetooth Connectivity Systems. Information Disclosure	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS47	T47. Bluetooth Connectivity Systems. Denial of Service	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS48	T48. Bluetooth Connectivity Systems. Elevation of Privilege	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS49	T49. Voice Command Systems. Spoofing	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS50	T50. Voice Command Systems. Tampering	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS51	T51. Voice Command Systems. Repudiation	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS52	T52. Voice Command Systems. Information Disclosure	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS53	T53. Voice Command Systems. Denial of Service	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS54	T54. Voice Command Systems. Elevation of Privilege	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS55	T55. Visual Systems. Spoofing	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS56	T56. Visual Systems. Tampering	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS57	T57. Visual Systems. Repudiation	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS58	T58. Visual Systems. Information Disclosure	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS59	T59. Visual Systems. Denial of Service	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS60	T60. Visual Systems. Elevation of Privilege	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS61	T61. Sensor Integration Systems. Spoofing	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS62	T62. Sensor Integration Systems. Tampering	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS63	T63. Sensor Integration Systems. Repudiation	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS64	T64. Sensor Integration Systems. Information Disclosure	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS65	T65. Sensor Integration Systems. Denial of Service	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS66	T66. Sensor Integration Systems. Elevation of Privilege	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS67	T67. Assistance Logic Systems. Spoofing	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS68	T68. Assistance Logic Systems. Tampering	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS69	T69. Assistance Logic Systems. Repudiation	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS70	T70. Assistance Logic Systems. Information Disclosure	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS71	T71. Assistance Logic Systems. Denial of Service	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS72	T72. Assistance Logic Systems. Elevation of Privilege	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS73	T73. Connectivity Systems. Spoofing	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS74	T74. Connectivity Systems. Tampering	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS75	T75. Connectivity Systems. Repudiation	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS76	T76. Connectivity Systems. Information Disclosure	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS77	T77. Connectivity Systems. Denial of Service	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS78	T78. Connectivity Systems. Elevation of Privilege	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS79	T79. Over-the-Air (OTA) Update Systems. Spoofing	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS80	T80. Over-the-Air (OTA) Update Systems. Tampering	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks
TS81	T81. Over-the-Air (OTA) Update Systems. Repudiation	TA01. Hackers	M01. Financial Gain	C01. Network-based. Packet Injection
TS82	T82. Over-the-Air (OTA) Update Systems. Information Disclosure	TA02. Script Kiddies	M02. Espionage	C02. Network-based. Wireless Sniffing
TS83	T83. Over-the-Air (OTA) Update Systems. Denial of Service	TA03. Insiders	M03. Ideological Beliefs	C03. Network-based. Man-in-the-Middle Attacks
TS84	T84. Over-the-Air (OTA) Update Systems. Elevation of Privilege	TA04. Nation-State Actors	M04. Revenge	C04. Software-based. Exploiting Software Vulnerabilities
TS85	T85. Integrated Browser and Apps. Spoofing	TA05. Organized Crime Groups	M05. Curiosity	C05. Software-based. Malware Installation
TS86	T86. Integrated Browser and Apps. Tampering	TA06. Terrorists	M06. Notoriety	C06. Software-based. Reverse Engineering
TS87	T87. Integrated Browser and Apps. Repudiation	TA07. Competitors	M07. Social or Political Activism	C07. Physical-based. Physical Device Manipulation
TS88	T88. Integrated Browser and Apps. Information Disclosure	TA08. Hacktivists	M08. Sabotage	C08. Physical-based. Hardware Tampering
TS89	T89. Integrated Browser and Apps. Denial of Service	TA09. Irresponsible Researchers	M09. Competitive Advantage	C09. Social Engineering. Deceptive Persuasion
TS90	T90. Integrated Browser and Apps. Elevation of Privilege	TA10. Privileged Users	M10. Fear or Coercion	C10. Social Engineering. Phishing Attacks

Figure 8. Threat Scenarios of Smart Vehicles Infotainment Systems

4.3 Impact Rating

This section will focus on the phase of impact rating for the infotainment systems assets. The work in this phase can be divided into two main steps. First, identifying and defining key areas of impact. In this step, it is necessary to comprehensively determine which areas are

associated with the vehicles infotainment systems and hold substantive significance, such as confidentiality, integrity, and availability issues from systems security perspectives (FIRST, 2023). Each selected impact area is related to the threats the infotainment systems might encounter.

After defining the impact areas, the next step involves delving into the specific correlations between these impacts and the infotainment systems assets. Referring to the threat scenarios outlined in section 4.2, a matrix of assessment can be established that correlates these impact areas with the infotainment systems assets (ENISA, 2010). This approach clearly identifies the impact values for each asset in the comprehensive threat scenarios. Furthermore, this information can serve as a reference for subsequent risk determinations.

4.3.1 Impact Areas

This subsection will focus on identifying and defining areas of impact. Considering various potential impact factors, a comprehensive perspective is necessary for the vehicles infotainment systems. The infotainment systems are linked to users' private data and integrated with the vehicles operational functionality and real-time interaction between users and the vehicle. As such, the focus is placed on CIA (Confidentiality, Integrity, Availability), regulatory compliance, and user safety (FIRST, 2023). Furthermore, complexity is increased due to the high correlation between the infotainment systems and other systems within the vehicles, and potential chain reactions across the systems are possible. Hence, during the assessment process, it is essential to consider the interdependencies between various systems and attempt to predict potential future risks and their consequences.

The identified infotainment systems impact areas and their definitions are as follows:

Confidentiality: The vehicles infotainment systems store a substantial amount of user data and sensitive information, such as data from connected phones, contacts, and call records. This dimension assesses the risk of information leakage if the systems are compromised.

- 1: Negligible - The system might inadvertently display or release non-critical confidential data.
- 2: Minor - Some confidential data might be accessed and leaked.

- 3: Moderate - Sensitive personal or system data might be accessed and leaked.
- 4: Significant - Critical confidential data is fully accessible and leaked.
- 5: Severe - All critical data is fully exposed, with wide-reaching repercussions.

Integrity: The vehicles infotainment systems offer various user settings, such as navigation routes and music playlists. This area considers unauthorised modification or damage to data or systems functionality, which could lead to driver misunderstanding or confusion.

- 1: Negligible - Non-critical data might be modified but does not affect system function.
- 2: Minor - Some important data might be modified, affecting partial system functionality.
- 3: Moderate - Sensitive system data can be modified, causing major malfunctions.
- 4: Significant - Critical system data is fully alterable, rendering the system inoperative.
- 5: Severe - The integrity of all critical system data is compromised, leading to total system failure.

Availability: Events that affect the normal operation of the infotainment systems, such as denial of service (DoS) attacks, are evaluated in this domain. Special consideration is given to the impact of these events on drive assistance, navigation, or other critical functionalities.

- 1: Negligible - System downtime only affects non-critical functions.
- 2: Minor - System downtime affects certain important vehicle functions.
- 3: Moderate - The system is critical to the vehicle's function but has some redundancy.
- 4: Significant - The system is indispensable, and its downtime halts the vehicle's primary function.
- 5: Severe - Complete system shutdown with irreversible effects.

Regulatory and Compliance: Considering the potential violations of data protection laws or standards that the infotainment systems may incur following an attack. Such violations could lead to fines or legal litigation.

- 1: Negligible - The system has few regulations, and non-compliance has few penalties.
- 2: Minor - The system must adhere to some regulations with potential penalties.
- 3: Moderate - The system is under stringent regulations with high penalties.

• 4: Significant - Non-compliance risks legal action, significant fines, or bans.

• 5: Severe - Legal and financial consequences could weaken the organisation.

Safety: Considering the potential interconnection between the vehicles infotainment systems and other control systems, this area assesses the tangible threats an attack poses to the safety of drivers and passengers.

• 1: Negligible - System issues might lead to minor inconveniences but no harm.

• 2: Minor - System malfunction can potentially cause minor injuries.

• 3: Moderate - System failure can cause serious injuries.

• 4: Significant - System failure can be fatal or lead to catastrophic events.

• 5: Severe - Potential for multiple fatalities and widespread harm.

Dependency: The infotainment systems within the vehicles may exhibit close interdependency with other systems, such as navigation or internet systems. This domain evaluates how compromised infotainment systems might lead to chain reactions within related systems.

• 1: Negligible - Relies on a few non-critical systems.

• 2: Minor - Linked to some major systems but can function partially without them.

• 3: Moderate - Relies heavily on other critical systems.

• 4: Significant - The system operation is tightly intertwined with other critical systems.

• 5: Severe - Complete reliance on multiple other critical systems for its function.

Future Threat Amplification: This area assesses how current security vulnerabilities might pose larger threats in the future.

• 1: Negligible - Potential for few emerging threats but with low impact.

• 2: Minor - Can be a target for future threats with some impact.

• 3: Moderate - Likely to face serious emerging threats.

• 4: Significant - Major vulnerabilities exposed to upcoming threats.

• 5: Severe - Prime target for advanced future threats with potentially devastating impact.

Average Impact: The average value derived from the impact of confidentiality, integrity, availability, regulatory and compliance, safety, dependency, and future threat amplification.

- <1.5: Negligible - The impact across all areas is minimal, and this value has a low risk of damage. It might involve minor inconveniences or issues, but they are not causing significant disruptions or harm.
- 1.5-2.4: Minor - There are some potential issues or risks, but they are contained. While there might be occasional disruptions, these are not damaging and can be easily mitigated.
- 2.5-3.4: Moderate - The overall impact is notable. This means there could be a substantial level of risk or potential damage. Regular attention is required to manage and address the identified impacts.
- 3.5-4.4: Significant - This value is associated with a significant level of risk or potential damage. Immediate action is necessary to prevent serious disruptions, such as financial losses or harm.
- 4.5-5: Severe - The highest level of risk or damage. This represents situations where the potential fallout could be catastrophic. Immediate and robust interventions are critical to prevent the impact.

Figure 9 illustrates the identifications and descriptions of impact areas of the smart vehicles infotainment systems.

	Impact Areas (IA)	
No.	**Impact Area (IA)**	**Description**
IA01	Confidentiality	The vehicle infotainment systems store a substantial amount of user data and sensitive information, such as data from connected phones, contacts, and call records. This dimension assesses the risk of information leakage if the systems are compromised.
		1: Negligible - The system might inadvertently display or release non-critical confidential data.
		2: Minor - Some confidential data might be accessed and leaked.
		3: Moderate - Sensitive personal or system data might be accessed and leaked.
		4: Significant - Critical confidential data is fully accessible and leaked.
		5: Severe - All critical data is fully exposed, with wide-reaching repercussions.
IA02	Integrity	The vehicle infotainment systems offer various user settings, such as navigation routes and music playlists. This area primarily considers unauthorized modification or damage to data or systems functionality, which could lead to driver misunderstanding or confusion.
		1: Negligible - Non-critical data might be modified but does not affect system function.
		2: Minor - Some important data might be modified, affecting partial system functionality.
		3: Moderate - Sensitive system data can be modified, causing major malfunctions.
		4: Significant - Critical system data is fully alterable, rendering the system inoperative.
		5: Severe - The integrity of all critical system data is compromised, leading to total system failure.
IA03	Availability	Any event that affects the normal operation of the infotainment system, such as Denial of Service (DoS) attacks, is evaluated in this domain. Special consideration is given to the impact of these events on music, navigation, or other critical functionalities.
		1: Negligible - System downtime only affects non-critical functions.
		2: Minor - System downtime affects certain important vehicle functions.
		3: Moderate - The system is critical to the vehicle's function but has some redundancy.
		4: Significant - The system is indispensable, and its downtime halts the vehicle's primary function.
		5: Severe - Complete system shutdown with irreversible effects.
IA04	Regulatory and Compliance	Considering the potential violations of data protection laws or standards that the infotainment systems may incur following an attack. Such violations could lead to fines or legal litigation.
		1: Negligible - The system has minor regulations, but non-compliance has few penalties.
		2: Minor - The system must adhere to major regulations with potential penalties.
		3: Moderate - The system is under stringent regulations with high penalties.
		4: Significant - Non-compliance risks legal action, significant fines, or bans.
		5: Severe - Legal and financial consequences could weaken the organisation.
IA05	Safety	Considering the potential interconnection between the vehicle infotainment systems and other control systems, this area primarily assesses the tangible threats an attack poses to the safety of drivers and passengers.
		1: Negligible - System issues might lead to minor inconveniences but no harm.
		2: Minor - System malfunction can potentially cause minor injuries.
		3: Moderate - System failure can cause serious injuries.
		4: Significant - System failure can be fatal or lead to catastrophic events.
		5: Severe - Potential for multiple fatalities and widespread harm.
IA06	Dependency	The infotainment systems within the vehicle may exhibit close interdependency with other systems, such as navigation or security systems. This domain evaluates how compromised infotainment systems might lead to chain reactions within related systems.
		1: Negligible - Relies on a few non-critical systems.
		2: Minor - Linked to some major systems but can function partially without them.
		3: Moderate - Relies heavily on other critical systems.
		4: Significant - The system's operation is tightly intertwined with other critical systems.
		5: Severe - Complete reliance on multiple other critical systems for its function.
IA07	Future Threat Magnification	Advancements in technology and the evolution of attack strategies mean that today's security events could amplify future risks. This area assesses how current security vulnerabilities might pose larger threats in the future.
		. Negligible - Potential for minor emerging threats but with low impact.
		2: Minor - Can be a target for future threats with moderate impact.
		3: Moderate - Likely to face serious emerging threats.
		4: Significant - Major vulnerabilities exposed to upcoming threats.
		5: Severe - Prime target for advanced future threats with potentially devastating impact.
IA Average	Average Impact	The average value derived from the impact of Confidentiality, Integrity, Availability, Regulatory and Compliance, Safety, Dependency, and Future Threat Magnification.
		<1.5: Negligible - The impact across all areas is minimal, and this value has a low risk of damage. It might involve minor inconveniences or issues, but they are not likely to cause significant disruptions or harm.
		1.5-2.4: Minor - There are some potential issues or risks, but they are contained. While there might be occasional disruptions, these are typically not damaging and can be easily managed or mitigated.
		2.5-3.4: Moderate - The overall impact is notable. This means there could be a substantial level of risk or potential damage. Regular attention is required to manage and address the identified risks or impacts.
		3.5-4.4: Significant - This value is associated with a significant level of risk or potential damage. Immediate action or regular monitoring is necessary to prevent serious disruptions, financial losses, or harm.
		4.5-5: Severe - The highest level of risk or damage. This represents situations or scenarios where the potential fallout could be catastrophic. Immediate and robust interventions are critical to prevent or mitigate the impact.

Figure 9. Impact Areas of Smart Vehicles Infotainment Systems

4.3.2 Impact Values

This subsection will focus on impact value assessments for the assets of the infotainment systems. Subsequently, a comprehensive assessment matrix is constructed based on the asset inventory and impact areas (ENISA, 2010). To successfully establish this assessment matrix, the following three core elements must be comprehensively considered:

- Infotainment Systems Asset Inventory: Based on the asset inventory proposed in section 4.1, the types and characteristics of the systems assets are clearly defined.
- Threat Scenarios: Analysing potential threats, threat agents, motivations, and capabilities as detailed in section 4.2 based on the threat scenarios and predicting the potential impacts these combinations of scenarios could have on the infotainment assets.
- Impact Areas: Combining the selected impact areas from subsection 4.3.1 with the asset inventory and considering the threat scenarios determines the impact values generated within each area.

Figure 10 shows that each category of the infotainment systems, such as audio and video entertainment systems and navigation systems, corresponds to specific assets, such as terrestrial radio, satellite radio systems, and satellite-based GPS units. Each asset is interconnected with impact areas, with values ranging from 1 to 5, indicating the impact level the asset experiences within the corresponding impact area. A higher value signifies a greater impact on the asset. Specific scoring criteria can be referred to in Figure 9.

Furthermore, from Figure 10, it can be observed that within the audio and video entertainment systems category, terrestrial radio receives a score of 1 in the IA01 (Confidentiality) impact area. In contrast, integrated browser and apps in the internet and Wi-Fi systems category receives a score of 5. This indicates a significantly higher impact level in the confidentiality impact area for the latter. Additionally, each asset is assigned an average impact value, calculated based on the values from the previous seven impact areas, aiming to represent the overall impact level of the asset across all impact areas. For instance, terrestrial radio has an average impact value of 1.9, while integrated browser and apps have a value of 4.0, indicating a notably higher overall impact for the latter. Consequently, during subsequent risk determination, it may exhibit a higher risk potential. This assessment matrix allows the impact values of infotainment systems assets under various potential threat

scenarios to be precisely and systematically evaluated, thereby providing a reference for subsequent risk decisions.

Impact Values (IV)									
No.	Asset Categorisation (AC)	Asset (A)	Impact Areas (IA)							Impact Value (IV)
			IA01	IA02	IA03	IA04	IA05	IA06	IA07	IA Average
IV01	Audio and Video Entertainment Systems	Terrestrial Radio Systems	1	2	3	1	2	2	2	1.9
IV02	Audio and Video Entertainment Systems	Satellite Radio Systems	1	2	4	1	2	3	2	2.1
IV03	Audio and Video Entertainment Systems	Media Playback Systems	2	3	3	1	2	2	2	2.1
IV04	Audio and Video Entertainment Systems	Integrated Streaming Platforms	3	3	4	2	2	3	3	2.9
IV05	Navigation Systems	Satellite-based GPS Units	3	4	5	2	4	5	4	3.9
IV06	Navigation Systems	Mapping and Visualization Systems	3	4	5	2	5	5	4	4.0
IV07	Navigation Systems	Traffic Data Systems	3	3	4	2	4	3	4	3.3
IV08	Telephony and Messaging Systems	Bluetooth Connectivity Systems	5	4	4	4	4	4	4	4.1
IV09	Telephony and Messaging Systems	Voice Command Systems	4	3	4	3	3	3	3	3.3
IV10	Driver Assistance Systems	Visual Systems	2	4	5	2	5	4	4	3.7
IV11	Driver Assistance Systems	Sensor Integration Systems	2	4	5	3	5	5	4	4.0
IV12	Driver Assistance Systems	Assistance Logic Systems	2	5	5	3	5	5	4	4.1
IV13	Internet and Wi-Fi Systems	Connectivity Systems	5	5	4	4	4	5	5	4.6
IV14	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	4	5	4	5	4	5	5	4.6
IV15	Internet and Wi-Fi Systems	Integrated Browser and Apps	5	4	4	4	3	4	4	4.0

Figure 10. Impact Values of Smart Vehicles Infotainment Systems

4.4 Attack Paths

This section will discuss the overall strategy and tactics that attackers employ, from starting initial attacks to achieving their ultimate objectives. Analysing this process provides deeper insights into the behaviour patterns of attackers. To comprehensively discuss this process, the following elements need to be considered (Dantas et al., 2021):

- Infotainment Systems Asset Inventory: Based on the asset inventory from section 4.1, the functionalities and characteristics of each asset should be clearly defined.
- Threats: Using the STRIDE model outlined in subsection 4.2.1, threats are assessed and matched with the infotainment systems assets inventory to ensure each asset is associated with the relevant STRIDE threat.
- Vulnerability/Weakness: Each threat might be linked to one or more vulnerabilities or weaknesses. These vulnerabilities may arise due to systems design, configuration, or other reasons. Attackers identify and exploit these vulnerabilities. This phase aims to establish clear associations between threats and relevant vulnerabilities/weaknesses (UNECE, 2021).
- Exploited Method: This part combines threats and corresponding vulnerabilities to speculate on possible attacker strategies or methods. Then, it further describes potential attack paths, covering the entire process from attackers initially exploring targets and selecting attack strategies to execute the complete attack.

- Attack Paths: Integrating the above elements, describe the potential attack paths, encompassing the entire process from attackers exploring targets and selecting attack strategies to execute the attack.

Figure 11 clearly displays the infotainment systems assets, such as terrestrial radio, facing a specific threat of spoofing. This threat could exploit the "Weak Signal Verification" vulnerability, utilising "Broadcast a Fake Station" as a method. Once the attacker successfully executes this method, they can create a fake broadcast station, connecting to the vehicle radio and providing misleading information or malicious payloads to the listeners. This analysis of attack paths gives a deeper understanding of the attacker's strategies and behavioural patterns.

Attack Paths (AP)						
No.	Asset Categorisation (AC)	Asset (A)	Threat (T)	Vulnerability/Weakness (VW)	Exploited Method (EM)	Attack Path (AP)
AP01	Audio and Video Entertainment Systems	Terrestrial Radio Systems	Spoofing	Weak Signal Verification	Broadcasta Fake Station	The attacker creates a fake station broadcast, causing the vehicle's radio to connectand deliver misinformation or malicious payloads to listeners.
AP02	Audio and Video Entertainment Systems	Terrestrial Radio Systems	Tampering	Lack of Encryption	Signal Interference	The attacker uses equipment to interfere with or modify the legitimate radio signal, altering or halting the broadcast for users.
AP03	Audio and Video Entertainment Systems	Terrestrial Radio Systems	Repudiation	No Playback Logging	Dispute Ad Broadcasts	An advertiser or user claims a certain messagead wasn'tplayed, exploiting the lack of playback logs as proof.
AP04	Audio and Video Entertainment Systems	Terrestrial Radio Systems	Information Disclosure	Unsecured Broadcasts	Eavesdrop on Private Channels	The attacker taps into unsecured or less-known channels to gather potentially sensitive information being shared.
AP05	Audio and Video Entertainment Systems	Terrestrial Radio Systems	Denial of Service	Signal Jamming Vulnerability	Radio Signal Jamming	The attacker uses jamming equipment to interruptor block the radio signal, preventing users from accessing the service.
AP06	Audio and Video Entertainment Systems	Terrestrial Radio Systems	Elevation of Privilege	Over-reliance on Signal Strength	Amplify a Fake Signal	The attacker amplifies a malicious or fake radio signal, causing the system to prioritize itover legitimate signals due to perceived strength.
AP07	Audio and Video Entertainment Systems	Satellite Radio Systems	Spoofing	Unverified Signal Source	Transmitting fake signals	An attacker transmits counterfeitsatellite signals, which the system processes as genuine, potentially providing fake information.
AP08	Audio and Video Entertainment Systems	Satellite Radio Systems	Tampering	Weak Encryption	Decrypting the signal	The attacker intercepts and decrypts weakly encrypted signals, altering the contentbefore itreaches the receiver.
AP09	Audio and Video Entertainment Systems	Satellite Radio Systems	Repudiation	Lack of Logging	Disputing transactions	After accessing or altering data, the attacker denies their actions due to a lack of proof from the system's side.
AP10	Audio and Video Entertainment Systems	Satellite Radio Systems	Information Disclosure	Insufficient Signal Protection	Signal Interception	The attacker captures the satellite radio signal, gaining access to potentially sensitive information.
AP11	Audio and Video Entertainment Systems	Satellite Radio Systems	Denial of Service	Signal Jamming Vulnerability	Using a jammer	An attacker employs a jamming device to interrupt the satellite radio service, causing outages and potentialhazards.
AP12	Audio and Video Entertainment Systems	Satellite Radio Systems	Elevation of Privilege	Firmware Vulnerability	Exploiting known firmware issues	The attacker exploits a known vulnerability in the radio system's firmware, gaining unauthorized access or privileges.
AP13	Audio and Video Entertainment Systems	Media Playback Systems	Spoofing	Weak File Validation	Malicious File Execution	Attacker tricks system into playing a malicious media file that contains embedded code. Once played, the code executes.
AP14	Audio and Video Entertainment Systems	Media Playback Systems	Tampering	No Digital Signatures on Media Files	Altered Media Content	Attacker alters the contentof media files, potentially embedding misinformation or malicious instructions.
AP15	Audio and Video Entertainment Systems	Media Playback Systems	Repudiation	Lack of Playback Logs	Denying Playback Actions	After playing malicious or unauthorized content, the attacker denies actions due to lack of concrete logs.
AP16	Audio and Video Entertainment Systems	Media Playback Systems	Information Disclosure	Unencrypted Media Transmission	Eavesdropping	Attacker intercepts the transmission of media files, leading to unauthorized access to potentially sensitive information within the media.
AP17	Audio and Video Entertainment Systems	Media Playback Systems	Denial of Service	Buffer Overflow Vulnerabilities	Malicious File Overload	Attacker sends media files designed to exploitbuffer overflow, causing system crashes or unintended behavior.
AP18	Audio and Video Entertainment Systems	Media Playback Systems	Elevation of Privilege	Weak User Privilege Settings	Exploiting Playback Controls	An attacker with basic access exploits lax privilege settings to control or alter media playback functionalities.
AP19	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Spoofing	Insecure Authorization Mechanism	Fake Streaming Server	The attacker sets up a counterfeitstreaming server, luring users to stream from it, which may lead to malware downloads or data exfiltration.
AP20	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Tampering	Lack of Input Validation	Manipulating Streaming Content	The attacker injects malicious scripts or manipulates streaming data to compromise user devices or data.
AP21	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Repudiation	Absence of Detailed Logging	Denial of Actions	After performing a malicious action, the attacker refutes itdue to a lack of proper logs thatcan prove their deed.
AP22	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Information Disclosure	Weak Encryption	Decryption of Streaming Data	The attacker decrypts the encrypted streaming data due to weak algorithms or keys, gaining access to proprietary or sensitive content.
AP23	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Denial of Service	Non-resilient Infrastructure	Overwhelming the Server	Attackers overload the platform servers with excessive requests, causing service interruptions for legitimate users.
AP24	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Elevation of Privilege	Outdated Platform Version	Exploiting Known Vulnerabilities	The attacker uses known vulnerabilities from outdated platform versions to gain unauthorized access or escalated privileges.
AP25	Navigation Systems	Satellite-based GPS Units	Spoofing	Inadequate Signal Authentication	Fake GPS Signal Broadcast	The attacker uses equipment to broadcasta stronger fake GPS signal to mislead the GPS receiver into calculating an incorrectlocation.
AP26	Navigation Systems	Satellite-based GPS Units	Tampering	Weak Encryption	Signal Interference	The attacker uses jamming equipment to block the GPS signals, causing the GPS unitto lose its location accuracy.
AP27	Navigation Systems	Satellite-based GPS Units	Repudiation	No Tracking of Manual Overrides	Disabling GPS Logs	After redirecting the GPS system, the attacker disables or deletes the logs to hide evidence of manipulation.
AP28	Navigation Systems	Satellite-based GPS Units	Information Disclosure	Unencrypted Data Transmission	Eavesdropping	An attacker intercepts unencrypted GPS data being transmitted, revealing sensitive details like the vehicle's currentand pastlocations.
AP29	Navigation Systems	Satellite-based GPS Units	Denial of Service	Over-reliance on GPS	GPS Signal Jamming	The attacker uses a jammer to block GPS signals, rendering the GPS unitnon-functional and potentially affecting vehicle operations thatrely on accurate location data.
AP30	Navigation Systems	Satellite-based GPS Units	Elevation of Privilege	Poorly Secured Firmware	Firmware Manipulation	An attacker finds an outdated or unsecured firmware version and uploads a malicious version, gaining control or manipulating the GPS functionalities.
AP31	Navigation Systems	Mapping and Visualization Systems	Spoofing	Insecure Map Data Transmission	Fake GPS signals	The attacker feeds the system with fake GPS signals, leading to false map updates or misdirection.
AP32	Navigation Systems	Mapping and Visualization Systems	Tampering	No Input Validation for User-Generated Content	Malicious Map Annotations	The attacker adds harmful or misleading annotations or pins to the map thatcan deceive the driver.
AP33	Navigation Systems	Mapping and Visualization Systems	Repudiation	No Activity Log for Map Updates	Denying Malicious Changes	After modifying map data maliciously, the attacker denies any changes due to the absence of a proper logging mechanism.
AP34	Navigation Systems	Mapping and Visualization Systems	Information Disclosure	No Encryption for Stored Locations	Access Recent Locations	The attacker accesses stored recentlocations, thereby compromising the privacy of the user.
AP35	Navigation Systems	Mapping and Visualization Systems	Denial of Service	Inefficient Map Rendering Process	Overload with Rapid Directions	The attacker sends rapid and numerous route requests, causing the map system to crash or freeze.
AP36	Navigation Systems	Mapping and Visualization Systems	Elevation of Privilege	No Proper User Permission Settings	Alter Map Settings	Using known exploits, the attacker accesses privileged map settings and makes unauthorized modifications.
AP37	Navigation Systems	Traffic Data Systems	Spoofing	Unauthenticated Data Sources	Use of fake traffic data	The attacker sends deceptive traffic information, misleading users about real-time road conditions.
AP38	Navigation Systems	Traffic Data Systems	Tampering	Unencrypted Data Transfer	Man-in-the-Middle Attack	The attacker intercepts and alters the traffic information being sentto the user's vehicle.
AP39	Navigation Systems	Traffic Data Systems	Repudiation	No Verification of Data Integrity	Altering traffic data	After sending malicious or altered traffic data, the attacker denies any involvementdue to the lack of data verification.
AP40	Navigation Systems	Traffic Data Systems	Information Disclosure	Lack of Data Anonymization	Data Mining	The attacker analyzes the received traffic data, extracting user patterns, habits, or frequently visited locations.
AP41	Navigation Systems	Traffic Data Systems	Denial of Service	Inadequate Server Protection	Overloading the server	The attacker sends overwhelming amounts of data to the traffic server, causing service disruptions for users.
AP42	Navigation Systems	Traffic Data Systems	Elevation of Privilege	Insufficient User Role Definitions	Exploiting system permissions	The attacker uses a lower-level user account to gain unauthorized access to more critical system functions.
AP43	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Spoofing	Weak Pairing Process	Use of Bluetooth Sniffing Tools	An attacker intercepts the initial pairing process, impersonating a legitimate device and establishing a connection.
AP44	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Tampering	Insufficient Encryption	Replay Attack	After intercepting data, the attacker retransmits the saved data packets, causing unintended actions.
AP45	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Repudiation	Lack of Logging	Deleting Bluetooth Logs	An attacker, after performing malicious activities, deletes Bluetooth activity logs, erasing any evidence.
AP46	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Information Disclosure	Open Bluetooth Discovery	Bluetooth Eavesdropping	The attacker continuously scans for open Bluetooth devices, intercepting any unencrypted data being transmitted.
AP47	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Denial of Service	Overloading Buffer	Sending Large Data Packets	The attacker sends large or malformed data packets to the system, causing its crash or become unresponsive.
AP48	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Elevation of Privilege	Outdated Bluetooth Protocol	Exploiting Known Vulnerabilities	Attackers exploitknown vulnerabilities in outdated Bluetooth protocols to gain unauthorized access or higher privileges.
AP49	Telephony and Messaging Systems	Voice Command Systems	Eavesdropping	Inadequate Encryption	Passive Listening	An attacker captures unencrypted voice commands to infer user habits, preferences, or private information.
AP50	Telephony and Messaging Systems	Voice Command Systems	Spoofing	Lack of Voice Recognition Security	Voice Mimicry	The attacker uses a recording or mimics the user's voice to issue unauthorized commands.
AP51	Telephony and Messaging Systems	Voice Command Systems	Misinterpretation	System Flaws in Voice Interpretation	Deliberate Ambiguous Commands	The attacker exploits the system's interpretation flaws to execute unintended actions.
AP52	Telephony and Messaging Systems	Voice Command Systems	Information Disclosure	Insecure Storage of Voice Data	Direct System Access	The attacker accesses stored voice command data to retrieve sensitive information.
AP53	Telephony and Messaging Systems	Voice Command Systems	Denial of Service	Inability to Filter Noise	Loud Noise Disruption	The attacker casts loud noises or disruptive sounds to inhibitthe system's ability to receive or interpretcommands.
AP54	Telephony and Messaging Systems	Voice Command Systems	Elevation of Privilege	Flaws in Command Authorization	Issuing Unauthorized Commands	The attacker bypasses normal command authorization processes to execute privileged actions.
AP55	Driver Assistance Systems	Visual Systems	Spoofing	Unauthenticated Display Access	Displaying Fake Information	The attacker broadcasts fake visual data to confuse the driver or passengers.
AP56	Driver Assistance Systems	Visual Systems	Tampering	No Image Validation	Inserting Malicious Image/Video	The attacker inserts a harmful image/video, possibly containing malicious code, into the display system.
AP57	Driver Assistance Systems	Visual Systems	Repudiation	Absence of User Interaction Logs	Deleting Visual Interaction Logs	After accessing the system, the attacker eliminates their interaction records, removing any evidence of tampering.
AP58	Driver Assistance Systems	Visual Systems	Information Disclosure	Insecure Data Handling	Exposing User Preferences	The attacker retrieves personal user preferences, e.g., frequently visited places, by exploiting unsecured data practices.
AP59	Driver Assistance Systems	Visual Systems	Denial of Service	Inadequate System Resource Management	Overloading the Display	The attacker sends excessive data or commands to the visual system, causing its freeze or malfunction.
AP60	Driver Assistance Systems	Visual Systems	Elevation of Privilege	No Multi-level User Permissions	Accessing Restricted Visual Modes	An attacker gains access to visual modes or settings reserved for administrators or technicians.
AP61	Driver Assistance Systems	Sensor Integration Systems	Spoofing	External Sensor Manipulation	Sensor Jamming	Attacker jams or floods sensor frequencies causing false readings or non-functionality.
AP62	Driver Assistance Systems	Sensor Integration Systems	Tampering	Insecure Data Transmission	Man-in-the-Middle Attack	Attacker intercepts sensor data during transmission, potentially altering itbefore sending to the main system.
AP63	Driver Assistance Systems	Sensor Integration Systems	Repudiation	Lack of Logging	Disable Logging	Attacker accesses system and disables logging of sensor data, thus leaving no trace of the data manipulation.
AP64	Driver Assistance Systems	Sensor Integration Systems	Information Disclosure	Unencrypted Sensor Data	Passive Eavesdropping	Attacker captures unencrypted sensor data as it's transmitted, gaining unauthorized knowledge.
AP65	Driver Assistance Systems	Sensor Integration Systems	Denial of Service	Sensor Overload	Continuous Invalid Inputs	Attacker continuously sends invalid inputs to the sensors, causing them to malfunction or shutdown.
AP66	Driver Assistance Systems	Sensor Integration Systems	Elevation of Privilege	Sensor Calibration Access	Adjusting Calibration	Attacker gains access to sensor calibration settings, adjusting them to provide inaccurate data.
AP67	Driver Assistance Systems	Assistance Logic Systems	Spoofing	Weak Sensor Verification	Sensor Spoofing	The attacker sends false data to the system, tricking it into making incorrectdecisions or actions.
AP68	Driver Assistance Systems	Assistance Logic Systems	Tampering	Inadequate Update Mechanism	Malicious Firmware Update	Attacker inserts malicious firmware updates, potentially altering system behaviors or extracting data.
AP69	Driver Assistance Systems	Assistance Logic Systems	Repudiation	No Activity Monitoring	Deleting or Altering Logs	Attacker, after accessing the system, deletes or changes logs to cover traces of their actions.
AP70	Driver Assistance Systems	Assistance Logic Systems	Information Disclosure	Unencrypted Inter-component Communication	Sniffing Communication	The attacker intercepts internal communication between components to gain valuable information.
AP71	Driver Assistance Systems	Assistance Logic Systems	Denial of Service	Resource Exhaustion	Overloading System	The attacker sends numerous requests or data to exhaustthe system's resources and cause malfunctions.
AP72	Driver Assistance Systems	Assistance Logic Systems	Elevation of Privilege	Insufficient Access Control	Bypassing Privilege Restrictions	The attacker finds ways to gain unauthorized access to functionalities restricted to higher-level users.
AP73	Internet and Wi-Fi Systems	Connectivity Systems	Spoofing	Weak Authentication Protocols	Use of easily guessed credentials	The attacker guesses or brute-forces credentials, impersonating a trusted device or user to connectto the system.
AP74	Internet and Wi-Fi Systems	Connectivity Systems	Tampering	Lack of Data Integrity Checks	Manipulating data packets	The attacker intercepts and alters data packets during transmission, leading to misinformation or undesired actions.
AP75	Internet and Wi-Fi Systems	Connectivity Systems	Repudiation	No Digital Signatures	Denying previous actions	An attacker performs malicious actions butlater denies having done so due to lack of traceability.
AP76	Internet and Wi-Fi Systems	Connectivity Systems	Information Disclosure	Open Ports & Lack of Encryption	Sniffing data packets	The attacker identifies open ports and captures data packets transmitted, accessing sensitive information.
AP77	Internet and Wi-Fi Systems	Connectivity Systems	Denial of Service	System Overload	Flooding with excessive requests	The attacker sends a large number of requests in a short time to overwhelm and crash the system.
AP78	Internet and Wi-Fi Systems	Connectivity Systems	Elevation of Privilege	Software Vulnerabilities	Exploiting unpatched issues	The attacker identifies and exploits known vulnerabilities in the connectivity software to gain higher privileges.
AP79	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Spoofing	Lack of Secure Communication	Fake Update Server	Attacker sets up a malicious server, deceiving the vehicle into downloading malicious updates.
AP80	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Tampering	Inadequate Update Verification	Malicious Update Injection	Attacker intercepts an OTA update and injects malicious code, which then gets installed in the system.
AP81	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Repudiation	Lack of Update Logs	Deleting or Modifying Update Logs	Attacker accesses the system post-update and alters or deletes logs to remove traces of malicious activities.
AP82	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Information Disclosure	No Encryption in Transit	Eavesdropping on Update Data	Attacker intercepts the OTA update transmission to gather confidential information or update details.
AP83	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Denial of Service	Update Server Overload	Massive Fake Update Requests	Attacker sends numerous fake update requests to the server, causing genuine requests to be delayed or denied.
AP84	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Elevation of Privilege	Update Without Adequate Permission Checks	Malicious Update with Elevated Privileges	Attacker sends an OTA update which, when installed, grants them higher system privileges.
AP85	Internet and Wi-Fi Systems	Integrated Browser and Apps	Spoofing	Identity Deception	Use of forged certificates	The attacker impersonates a trusted organization or individual, successfully deceiving the server or users to access sensitive information.
AP86	Internet and Wi-Fi Systems	Integrated Browser and Apps	Tampering	Invalid Data Input Validation	SQL Injection	The attacker inputs SQL commands in inputfields, attempting to control the database and execute unintended commands.
AP87	Internet and Wi-Fi Systems	Integrated Browser and Apps	Repudiation	Lack of Audit Trail	Deleting Log Files	After gaining system access, the attacker deletes or modifies their activity logs, thereby erasing evidence of their malicious actions.
AP88	Internet and Wi-Fi Systems	Integrated Browser and Apps	Information Disclosure	Unencrypted Data Transmission	Man-in-the-Middle Attack	The attacker establishes a connection between the user and the server, intercepting and/or modifying information transmitted over this connection.
AP89	Internet and Wi-Fi Systems	Integrated Browser and Apps	Denial of Service	Unoptimized Queries	Sending Massive Requests	The attacker overwhelms the system by continuously sending a large number of queries or requests, aiming to cause service interruptions.
AP90	Internet and Wi-Fi Systems	Integrated Browser and Apps	Elevation of Privilege	Outdated Browser Engine	Exploiting known browser vulnerabilities	The attacker explores and exploits known vulnerabilities in the browser or its engine to gain higher privileges than their original access.

Figure 11. Attack Paths of Smart Vehicles Infotainment Systems

4.5 Feasibility Rating

This section will focus on assessing the feasibility rating for infotainment systems assets. This assessment can be divided into two main steps. The first step involves identifying and

defining the feasibility areas. During this step, it is essential to deeply consider which domains are closely related to attacks on the vehicles infotainment systems. After defining these feasibility areas based on the attack paths described in section 4.4, a detailed examination of the relationship between these feasibility areas and different asset attack paths will be conducted. This leads to constructing an assessment matrix (ENISA, 2010). This matrix makes it possible to clearly identify the feasibility rating of infotainment systems assets across various feasibility areas in different attack paths. Additionally, this matrix can be combined with the impact rating from section 4.3, providing a more comprehensive reference for subsequent risk determinations.

4.5.1 Feasibility Areas

This subsection will focus on identifying and defining feasibility areas. According to Security Engineering for ISO/SAE 21434 (Dantas et al., 2021), a comprehensive consideration of attack factors against vehicles infotainment systems has been made to determine feasibility areas. These areas include expertise, time, equipment, knowledge, and opportunity. The definitions are defined from the attacker's perspective, so from the user's viewpoint, there's an inverse relationship.

The determined feasibility areas and their definitions are as follows:

Expertise: Assesses the complexity of skills and experience required to attack the vehicles infotainment systems. If an attack demands a high degree of expertise, its feasibility on the vehicles infotainment systems may be reduced.

- 1: Master - Requires deep knowledge and extensive experience, considered top-tier.
- 2: Expert - Highly proficient, can complete tasks independently with minimal referencing.
- 3: Intermediate - Has a degree of proficiency but may still need to reference or consult.
- 4: Basic - Possesses some basic understanding and experience.
- 5: Novice - Little to no relevant experience or skills.

Time: Estimates the time an attacker needs to complete an attack on the vehicles infotainment systems. Lengthy time requirements could lower the feasibility of a particular attack technique on the systems.

- 1: Very Long - Requires months or even longer.

- 2: Long - Requires weeks.
- 3: Moderate - Spanning days.
- 4: Short - A matter of hours.
- 5: Quick - This can be accomplished in minutes.

Equipment: Evaluate the equipment needed to attack the vehicles infotainment systems. Specific rare or expensive equipment requirements might decrease the feasibility of the attack.

- 1: Highly Specialised Equipment - Extremely expensive, regulated, or available only in specific domains or countries.
- 2: Specialised Equipment – High cost and hard to obtain.
- 3: Moderate Equipment - Requires specific software or hardware that may come at some cost and time.
- 4: Basic Equipment - Requires some specialised tools or devices, but easily accessible.
- 5: No Special Equipment - Usable with daily technology, like a general computer or mobile device.

Knowledge: Measures the knowledge an attacker needs to attack the vehicles infotainment systems. The difficulty of acquiring knowledge may affect the feasibility of the attack.

- 1: Expert Level - Requires in-depth studies or long-term professional experience.
- 2: Advanced - Highly specialised knowledge, likely limited to specific professions.
- 3: Moderate - Requires deeper learning, research, or training.
- 4: Elementary - Involves some specific learning or research.
- 5: Basic - Easily accessible public knowledge.

Opportunity: Assesses the frequency with which attackers have opportunities to conduct attacks on the vehicles infotainment systems. The lack of opportunities might reduce the feasibility of certain attacks.

- 1: Rarely or None - Virtually no opportunity or only under extremely rare conditions.

• 2: Rarely Present - Opportunities are infrequent and may require specific timing, locations, or conditions.

• 3: Occasionally Present - Requires specific situations or conditions.

• 4: Frequently Present - Present in most situations.

• 5: Always Present - Almost any time and place.

Average Feasibility: The average value considering an attacker's expertise, time, knowledge, and opportunity required to attack infotainment systems.

• <1.5: Very Unlikely - Very little chance of success.

• 1.5-2.4: Unlikely - Some chance but with risks and challenges.

• 2.5-3.4: Moderately Possible - A fair chance of success but requires conditions.

• 3.5-4.4: Likely - A significant chance of success with minimal conditions.

• 4.5-5: Very Likely - Almost certain to succeed.

Figure 12 illustrates the identifications and descriptions of feasibility areas of the smart vehicles infotainment systems.

	Feasibilities Areas (FA)	
No.	**Impact Area (IA)**	**Description**
F01	Expertise	Assesses the complexity of skills and experience required to attack the vehicle infotainment system. If an attack demands a high degree of expertise, its feasibility on the vehicle infotainment systems may be reduced.
		1: Master - Requires deep knowledge and extensive experience, considered top-tier in the domain.
		2: Expert - Highly proficient, can complete tasks independently with minimal referencing.
		3: Intermediate - Has a degree of proficiency but may still need to reference or consult.
		4: Basic - Possesses some basic understanding and experience.
		5: Novice - Little to no relevant experience or skills.
F02	Time	Estimates the time an attacker needs to complete an attack on the vehicle infotainment system. Lengthy time requirements could lower the feasibility of a particular attack technique on the system.
		1: Very Long - Requires months or even longer.
		2: Long - Requires weeks.
		3: Moderate - Spanning days.
		4: Short - A matter of hours.
		5: Quick - Can be accomplished in minutes.
F03	Equipment	Evaluate the tools or equipment needed to attack the vehicle infotainment system. Specific rare or expensive equipment requirements might decrease the feasibility of the attack.
		1: Highly Specialized Equipment - Extremely expensive, regulated, or available only in specific domains or countries.
		2: Specialized Equipment - High-cost and/or hard-to-obtain.
		3: Moderate Equipment - Requires specific software or hardware that may come at some cost and time.
		4: Basic Equipment - Requires some specialized tools or devices, but easily accessible.
		5: No Special Equipment - Usable with everyday technology, like a general computer or mobile device.
F04	Knowledge	Measures the knowledge or information an attacker needs to attack the vehicle infotainment system. The difficulty of acquiring information may affect the feasibility of the attack.
		1: Expert Level - Requires in-depth studies or long-term professional experience.
		2: Advanced - Highly specialized knowledge, likely limited to specific professions.
		3: Moderate - Requires deeper learning, research, or training.
		4: Elementary - Involves some specific learning or research.
		5: Basic - General or easily accessible public knowledge.
F05	Opportunity	Assesses the frequency with which attackers have opportunities to conduct attacks on the vehicle infotainment system. The scarcity of opportunities might reduce the feasibility of certain attacks.
		1: Almost Never or None - Virtually no opportunity or only under extremely rare conditions.
		2: Rarely Present - Opportunities are infrequent and may require specific timing, locations, or conditions.
		3: Occasionally Present - Requires specific situations or conditions.
		4: Frequently Present - Present in most situations.
		5: Always Present - Almost any time and place.
F Average	Average Feasibility	The average value considering an attacker's Expertise, Time, Knowledge, and Opportunity required to target infotainment systems.
		<1.5: Highly Unlikely - Almost no chance of success.
		1.5-2.4: Unlikely - Some chance but with risks and challenges.
		2.5-3.4: Moderately Possible - A fair chance of success but requires conditions.
		3.5-4.4: Likely - A significant chance of success with minimal conditions.
		4.5-5: Highly Likely - Almost certain to succeed.

Figure 12. Feasibility Areas of Smart Vehicles Infotainment Systems

4.5.2 Feasibility Values

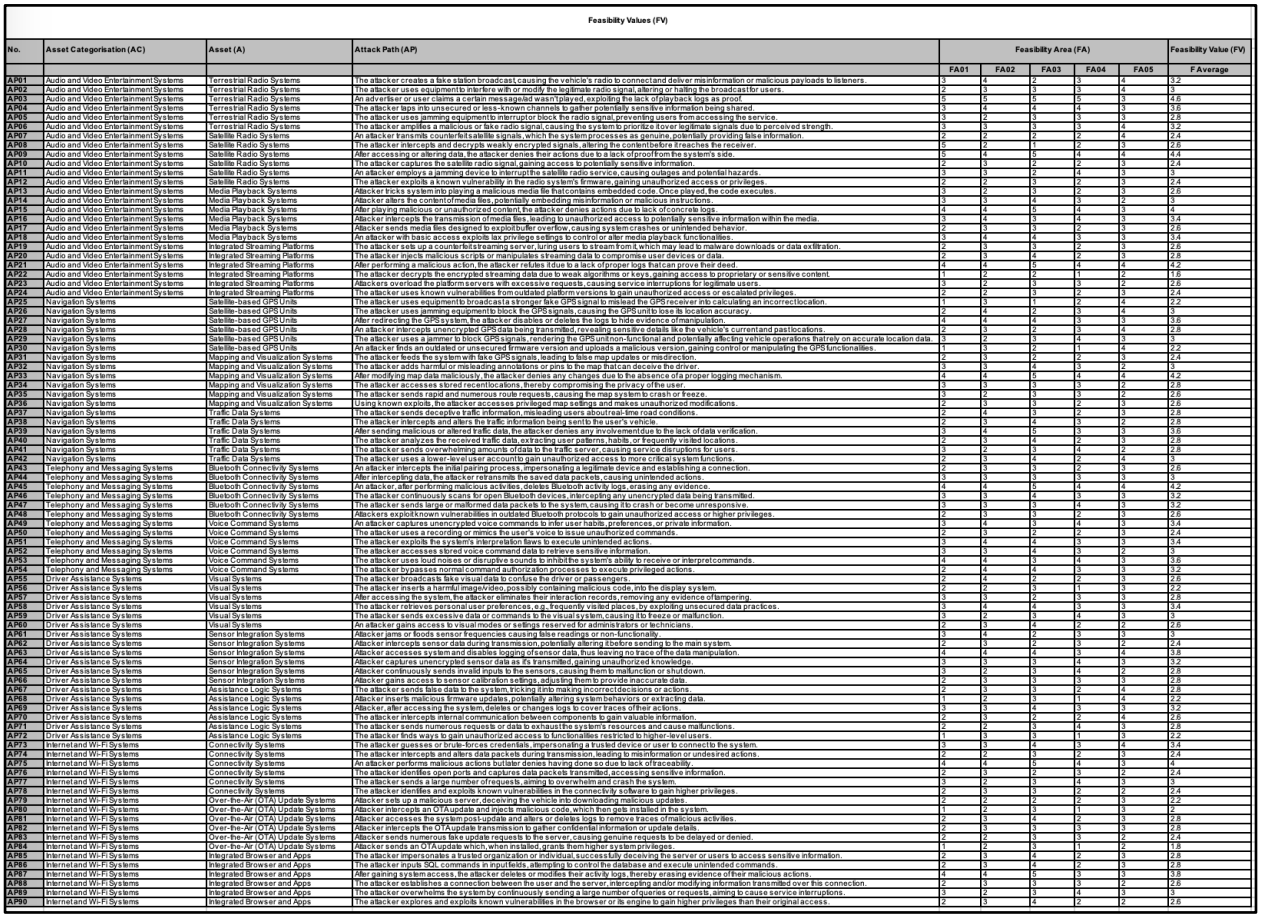
This subsection will focus on assessing feasibility values for the vehicles infotainment systems assets and, subsequently, creating a comprehensive assessment matrix based on

the asset inventory and feasibility areas (ENISA, 2010). To successfully establish this assessment matrix, the following core elements must be considered:

- Infotainment Systems Asset Inventory: Clearly defining the types and characteristics of assets as presented in section 4.1.
- Attack Paths: Analysing the relevance between potential attack paths described in section 4.4 and the asset inventory.
- Feasibility Areas: Integrating the selected feasibility areas from subsection 4.5.1 with the asset inventory and attack paths to determine the feasibility values in each domain.

Figure 13 shows that each attack path correlates with feasibility areas, and the numerical range spans from 1 to 5, indicating the feasibility assessment of the attack paths within the corresponding feasibility area. Higher values signify greater feasibility. Specific scoring criteria can be referred to in Figure 12.

Further observations from Figure 13 reveal that the AP01 attack path in the terrestrial radio systems scores 3 in feasibility area FA01 (Expertise), while AP03 attack path scores 5. This indicates the higher feasibility of the latter attack path in the expertise domain. Additionally, each asset concludes with an average feasibility value, calculated based on the preceding domain values to present an overall feasibility assessment of the asset across all feasibility areas. For instance, the first path for terrestrial radio has an average feasibility value of 3.2, while the FA03 attack path is 4.6, signifying significantly higher overall feasibility of the latter. Consequently, the risk may be more elevated during subsequent risk determinations. Through this assessment matrix, it is possible to systematically evaluate the feasibility values of vehicles infotainment systems assets across various potential attack paths, thereby providing a reference for subsequent risk decisions.



Feasibility Values (FV)

No.	Asset Categorisation (AC)	Asset (A)	Attack Path (AP)	Feasibility Area (FA)						Feasibility Value (FV)
				FA01	FA02	FA03	FA04	FA05	FA06	FAverage
AP01	Audio and Video Entertainment Systems	Terrestrial Radio Systems	The attacker creates a fake station broadcast,causing the vehicle's radio to connect and deliver misinformation or malicious payloads to listeners.	3	4	2	3	4	3	3.2
AP02	Audio and Video Entertainment Systems	Terrestrial Radio Systems	The attacker uses equipment to interfere with or modify the legitimate radio signal,altering or halting the broadcastfor users.	2	3	3	3	3	3	3
AP03	Audio and Video Entertainment Systems	Terrestrial Radio Systems	An advertiser or user claims a certain messagedid wasn'tplayed,exploiting the lack of playback logs as proof.	5	5	5	5	3	4	4.8
AP04	Audio and Video Entertainment Systems	Terrestrial Radio Systems	The attacker taps into unsecured or less-known channels to gather potentially sensitive information being shared.	3	4	4	4	3	3	3.8
AP05	Audio and Video Entertainment Systems	Terrestrial Radio Systems	The attacker uses jamming equipment to interrupt or block the radio signal,preventing users from accessing the service.	3	2	3	3	3	2	2.8
AP06	Audio and Video Entertainment Systems	Terrestrial Radio Systems	The attacker amplifies a malicious or fake radio signal,causing the system to prioritize itover legitimate signals due to perceived strength.	3	3	3	3	4	3	3.2
AP07	Audio and Video Entertainment Systems	Satellite Radio Systems	An attacker transmits counterfeit satellite signals, which the system processes as genuine, potentially providing false information.	2	2	2	2	4	2	2.4
AP08	Audio and Video Entertainment Systems	Satellite Radio Systems	The attacker intercepts and decrypts weakly encrypted signals, altering the contentbefore it reaches the receiver.	5	2	1	2	3	2	2.6
AP09	Audio and Video Entertainment Systems	Satellite Radio Systems	After accessing or altering data, the attacker denies their actions due to a lack of proof from the system's side.	5	4	5	4	4	4	4.4
AP10	Audio and Video Entertainment Systems	Satellite Radio Systems	The attacker captures the satellite radio signal, gaining access to potentially sensitive information.	2	3	2	2	3	2	2.4
AP11	Audio and Video Entertainment Systems	Satellite Radio Systems	An attacker employs a jamming device to interrupt the satellite radio service, causing outages and potential hazards.	3	3	2	4	3	3	3
AP12	Audio and Video Entertainment Systems	Satellite Radio Systems	The attacker exploits a known vulnerability in the radio system's firmware, gaining unauthorized access or privileges.	2	2	3	2	3	2	2.4
AP13	Audio and Video Entertainment Systems	Media Playback Systems	Attacker tricks system into playing a malicious media file thatcontains embedded code. Once played, the code executes.	3	2	3	2	3	2	2.6
AP14	Audio and Video Entertainment Systems	Media Playback Systems	Attacker alters the content of media files, potentially embedding misinformation or malicious instructions.	3	3	4	3	2	3	3
AP15	Audio and Video Entertainment Systems	Media Playback Systems	After playing malicious or unauthorized content,the attacker denies actions due to lack of concrete logs.	4	4	5	4	3	4	4
AP16	Audio and Video Entertainment Systems	Media Playback Systems	Attacker intercepts the transmission of media files, leading to unauthorized access to potentially sensitive information within the media.	3	4	3	4	3	3	3.4
AP17	Audio and Video Entertainment Systems	Media Playback Systems	Attacker sends media files designed to exploit buffer overflow, causing system crashes or unintended behavior.	2	3	3	2	3	2	2.6
AP18	Audio and Video Entertainment Systems	Media Playback Systems	An attacker with basic access exploits lax privilege settings to control or alter media playback functionalities.	3	4	4	3	3	3	3.4
AP19	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker sets up a counterfeit streaming server, luring users to stream from it, which may lead to malware downloads or data exfiltration.	2	3	3	2	3	2	2.6
AP20	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker injects malicious scripts or manipulates streaming data to compromise user devices or data.	2	3	4	2	3	2	2.8
AP21	Audio and Video Entertainment Systems	Integrated Streaming Platforms	After performing a malicious action, the attacker refutes it due to a lack of proper logs that can prove their deed.	4	4	5	4	4	4	4.2
AP22	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker decrypts the encrypted streaming data due to weak algorithms or keys, gaining access to proprietary or sensitive content.	1	2	2	1	2	1	1.6
AP23	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Attackers overload the platform servers with excessive requests, causing service interruptions for legitimate users.	3	2	3	3	2	2	2.6
AP24	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker uses known vulnerabilities from outdated platform versions to gain unauthorized access or escalated privileges.	2	2	3	2	3	2	2.4
AP25	Navigation Systems	Satellite-based GPS Units	The attacker uses equipment to broadcast a stronger fake GPS signal to mislead the GPS receiver into calculating an incorrect location.	1	3	1	2	4	2	2.2
AP26	Navigation Systems	Satellite-based GPS Units	The attacker uses jamming equipment to block the GPS signals, causing the GPS unit to lose its location accuracy.	2	4	2	3	4	3	3
AP27	Navigation Systems	Satellite-based GPS Units	After redirecting the GPS system, the attacker disables or deletes the logs to hide evidence of manipulation.	4	4	4	3	3	3	3.8
AP28	Navigation Systems	Satellite-based GPS Units	An attacker intercepts unencrypted GPS data being transmitted, revealing sensitive details like the vehicle's current and past locations.	2	3	2	3	4	3	2.8
AP29	Navigation Systems	Satellite-based GPS Units	The attacker uses a jammer to block GPS signals, rendering the GPS unit non-functional and potentially affecting vehicle operations that rely on accurate location data.	3	2	3	4	3	3	3
AP30	Navigation Systems	Satellite-based GPS Units	An attacker finds an outdated or unsecured firmware version and uploads a malicious version, gaining control or manipulating the GPS functionalities.	1	3	2	1	4	2	2.2
AP31	Navigation Systems	Mapping and Visualization Systems	The attacker feeds the system with fake GPS signals, leading to false map updates or misdirection.	2	3	2	2	3	2	2.4
AP32	Navigation Systems	Mapping and Visualization Systems	The attacker adds harmful or misleading annotations or pins to the map that can deceive the driver.	3	3	4	3	3	3	3
AP33	Navigation Systems	Mapping and Visualization Systems	After modifying map data maliciously, the attacker denies any changes due to the absence of a proper logging mechanism.	4	4	5	4	4	4	4.2
AP34	Navigation Systems	Mapping and Visualization Systems	The attacker accesses stored recent locations, thereby compromising the privacy of the user.	3	3	3	3	2	3	2.8
AP35	Navigation Systems	Mapping and Visualization Systems	The attacker sends rapid and numerous route requests, causing the map system to crash or freeze.	3	2	3	3	2	2	2.6
AP36	Navigation Systems	Mapping and Visualization Systems	Using known exploits, the attacker accesses privileged map settings and makes unauthorized modifications.	2	3	3	2	3	2	2.6
AP37	Navigation Systems	Traffic Data Systems	The attacker sends deceptive traffic information, misleading users about real-time road conditions.	2	4	3	2	3	2	2.8
AP38	Navigation Systems	Traffic Data Systems	The attacker intercepts and alters the traffic information being sent to the user's vehicle.	2	3	4	3	2	2	2.8
AP39	Navigation Systems	Traffic Data Systems	After sending malicious or altered traffic data, the attacker denies any involvement due to the lack of data verification.	3	4	5	3	3	3	3.8
AP40	Navigation Systems	Traffic Data Systems	The attacker analyzes the received traffic data, extracting user patterns, habits, or frequently visited locations.	2	3	4	2	3	2	2.8
AP41	Navigation Systems	Traffic Data Systems	The attacker sends overwhelming amounts of data to the traffic server, causing service disruptions for users.	3	2	3	4	2	2	2.8
AP42	Navigation Systems	Traffic Data Systems	The attacker uses a lower-level user account to gain unauthorized access to more critical system functions.	2	3	4	2	4	3	3
AP43	Telephony and Messaging Systems	Bluetooth Connectivity Systems	An attacker intercepts the initial pairing process, impersonating a legitimate device and establishing a connection.	2	3	3	2	3	3	2.6
AP44	Telephony and Messaging Systems	Bluetooth Connectivity Systems	After intercepting data, the attacker retransmits the saved data packets, causing unintended actions.	3	3	3	3	3	3	3
AP45	Telephony and Messaging Systems	Bluetooth Connectivity Systems	An attacker, after performing malicious activities, deletes Bluetooth activity logs, erasing any evidence.	4	4	5	4	4	4	4.2
AP46	Telephony and Messaging Systems	Bluetooth Connectivity Systems	The attacker continuously scans for open Bluetooth devices, intercepting any unencrypted data being transmitted.	3	3	4	3	3	3	3.2
AP47	Telephony and Messaging Systems	Bluetooth Connectivity Systems	The attacker sends large or malformed data packets to the system, causing it to crash or become unresponsive.	3	3	3	4	3	3	3.2
AP48	Telephony and Messaging Systems	Bluetooth Connectivity Systems	Attackers exploit known vulnerabilities in outdated Bluetooth protocols to gain unauthorized access or higher privileges.	2	3	3	2	3	2	2.6
AP49	Telephony and Messaging Systems	Voice Command Systems	An attacker captures unencrypted voice commands to infer user habits, preferences, or private information.	3	3	4	3	4	3	3.4
AP50	Telephony and Messaging Systems	Voice Command Systems	The attacker uses a recording or mimics the user's voice to issue unauthorized commands.	2	3	2	2	3	2	2.4
AP51	Telephony and Messaging Systems	Voice Command Systems	The attacker exploits the system's interpretation flaws to execute unintended actions.	3	4	4	3	3	3	3.4
AP52	Telephony and Messaging Systems	Voice Command Systems	The attacker accesses stored voice command data to retrieve sensitive information.	3	3	4	3	2	3	3
AP53	Telephony and Messaging Systems	Voice Command Systems	The attacker uses loud noises or disruptive sounds to inhibit the system's ability to receive or interpret commands.	4	4	3	4	3	3	3.8
AP54	Telephony and Messaging Systems	Voice Command Systems	The attacker bypasses normal command authorization processes to execute privileged actions.	2	4	4	3	3	3	3.2
AP55	Driver Assistance Systems	Visual Systems	The attacker broadcasts fake visual data to confuse the driver or passengers.	2	4	2	2	3	2	2.6
AP56	Driver Assistance Systems	Visual Systems	The attacker inserts a harmful image/video, possibly containing malicious code, into the display system.	2	2	3	1	3	2	2.2
AP57	Driver Assistance Systems	Visual Systems	After accessing the system, the attacker eliminates their interaction records, removing any evidence of tampering.	3	3	2	3	3	3	2.8
AP58	Driver Assistance Systems	Visual Systems	The attacker retrieves personal user preferences, e.g., frequently visited places, by exploiting unsecured data practices.	3	4	4	3	3	3	3.4
AP59	Driver Assistance Systems	Visual Systems	The attacker sends excessive data or commands to the visual system, causing it to freeze or malfunction.	3	2	3	4	3	3	3
AP60	Driver Assistance Systems	Visual Systems	An attacker gains access to visual modes or settings reserved for administrators or technicians.	2	3	4	2	2	2	2.6
AP61	Driver Assistance Systems	Sensor Integration Systems	Attacker jams or floods sensor frequencies causing false readings or non-functionality.	3	4	2	3	3	3	3
AP62	Driver Assistance Systems	Sensor Integration Systems	Attacker intercepts sensor data during transmission,potentially altering it before sending to the main system.	2	3	2	3	2	2	2.4
AP63	Driver Assistance Systems	Sensor Integration Systems	Attacker accesses system and disables logging of sensor data, thus leaving no trace of the data manipulation.	4	4	4	3	4	3	3.8
AP64	Driver Assistance Systems	Sensor Integration Systems	Attacker captures unencrypted sensor data as it's transmitted, gaining unauthorized knowledge.	3	3	3	4	3	3	3.2
AP65	Driver Assistance Systems	Sensor Integration Systems	Attacker continuously sends invalid inputs to the sensors, causing them to malfunction or shutdown.	3	2	3	4	2	2	2.8
AP66	Driver Assistance Systems	Sensor Integration Systems	Attacker gains access to sensor calibration settings, adjusting them to provide inaccurate data.	2	3	3	3	3	3	2.8
AP67	Driver Assistance Systems	Assistance Logic Systems	The attacker sends false data to the system, tricking it into making incorrect decisions or actions.	2	3	3	2	4	2	2.8
AP68	Driver Assistance Systems	Assistance Logic Systems	Attacker inserts malicious firmware updates, potentially altering system behaviors or extracting data.	1	2	3	1	4	2	2.2
AP69	Driver Assistance Systems	Assistance Logic Systems	Attacker, after accessing the system, deletes or changes logs to cover traces of their actions.	3	3	4	3	3	3	3.2
AP70	Driver Assistance Systems	Assistance Logic Systems	The attacker intercepts internal communication between components to gain valuable information.	2	3	3	2	4	2	2.6
AP71	Driver Assistance Systems	Assistance Logic Systems	The attacker sends numerous requests or data to exhaust the system's resources and cause malfunctions.	2	2	3	4	3	2	2.8
AP72	Driver Assistance Systems	Assistance Logic Systems	The attacker finds ways to gain unauthorized access to functionalities restricted to higher-level users.	1	3	3	1	3	2	2.2
AP73	Internet and Wi-Fi Systems	Connectivity Systems	The attacker guesses or brute-forces credentials, impersonating a trusted device or user to connect to the system.	3	3	4	3	4	3	3.4
AP74	Internet and Wi-Fi Systems	Connectivity Systems	The attacker intercepts and alters data packets during transmission, leading to misinformation or undesired actions.	2	2	3	2	3	2	2.4
AP75	Internet and Wi-Fi Systems	Connectivity Systems	An attacker performs malicious actions but later denies having done so due to lack of traceability.	4	4	5	4	3	4	4
AP76	Internet and Wi-Fi Systems	Connectivity Systems	The attacker identifies open ports and captures data packets transmitted, accessing sensitive information.	2	3	2	3	3	2	2.4
AP77	Internet and Wi-Fi Systems	Connectivity Systems	The attacker sends a large number of requests, aiming to overwhelm and crash the system.	3	2	3	4	3	3	3
AP78	Internet and Wi-Fi Systems	Connectivity Systems	The attacker identifies and exploits known vulnerabilities in the connectivity software to gain higher privileges.	2	3	3	2	2	2	2.4
AP79	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Attacker sets up a malicious server, deceiving the vehicle into downloading malicious updates.	2	2	2	2	3	2	2.2
AP80	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Attacker intercepts an OTA update and injects malicious code, which then gets installed in the system.	1	2	3	1	3	2	2
AP81	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Attacker accesses the system post-update and alters or deletes logs to remove traces of their malicious activities.	2	3	4	2	2	2	2.8
AP82	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Attacker intercepts the OTA update transmission to gather confidential information or update details.	2	3	3	3	3	3	2.8
AP83	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Attacker sends numerous fake update requests to the server, causing genuine requests to be delayed or denied.	2	2	3	3	2	2	2.4
AP84	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	Attacker sends an OTA update which, when installed, grants them higher system privileges.	1	2	3	1	2	1	1.8
AP85	Internet and Wi-Fi Systems	Integrated Browser and Apps	The attacker impersonates a trusted organization or individual, successfully deceiving the server or users to access sensitive information.	2	3	4	2	3	2	2.8
AP86	Internet and Wi-Fi Systems	Integrated Browser and Apps	The attacker inputs SQL commands in input fields, attempting to control the database and execute unintended commands.	2	3	4	2	3	2	2.8
AP87	Internet and Wi-Fi Systems	Integrated Browser and Apps	After gaining system access, the attacker deletes or modifies their activity logs, thereby erasing evidence of their malicious actions.	4	3	5	3	3	3	3.8
AP88	Internet and Wi-Fi Systems	Integrated Browser and Apps	The attacker establishes a connection between the user and the server, intercepting and/or modifying information transmitted over this connection.	2	3	3	3	2	2	2.8
AP89	Internet and Wi-Fi Systems	Integrated Browser and Apps	The attacker overwhelms the system by continuously sending a large number of queries or requests, aiming to cause service interruptions.	3	2	3	4	3	3	3
AP90	Internet and Wi-Fi Systems	Integrated Browser and Apps	The attacker explores and exploits known vulnerabilities in the browser or its engine to gain higher privileges than their original access.	2	3	4	2	2	2	2.6

Figure 13. Feasibility Values of Smart Vehicles Infotainment Systems

4.6 Risk Determination

This section will focus on the stage of risk determination. This phase encompasses two steps. Firstly, the creation and definition of a risk matrix are required. Subsequently, these elements correspond to the risk matrix by combining the impact values obtained from section 4.3 and the feasibility values of assets under different attack paths obtained from section 4.5. Ultimately, this stage finalises the risk assessment of vehicles infotainment systems.

4.6.1 Risk Matrix

This subsection will focus on the creation and definition of the risk matrix. To evaluate the risk of smart vehicles infotainment systems, the design of the risk matrix will focus on two main pointers as follows:

- Impact Pointer: This pointer is assigned to the horizontal axis of the risk matrix and is divided into five levels (Negligible, Minor, Moderate, Significant, Severe) based on severity (1-5).
- Feasibility Pointer: This pointer is assigned to the vertical axis of the risk matrix and is categorised into five levels (Very Unlikely, Unlikely, Possible, Likely, Very Likely) based on likelihood (1-5).

Mapping impact pointer and feasibility pointer onto the risk matrix yields five distinct risk levels (Low, Low Med, Medium, Med Hi, High), and it displays different colours based on varying risk levels. The specific risk matrix can be referenced in Figure 14 (Katsumata et al., 2010).

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 14. Risk Matrix of Smart Vehicles Infotainment Systems (Katsumata et al., 2010)

4.6.2 Risk Mapping

This subsection will focus on mapping the previously mentioned impact pointer and feasibility pointer of smart vehicles infotainment systems assets onto the risk matrix to determine their risk values. To establish this risk matrix, the following core elements need to be considered:

- Infotainment Systems Asset List: Confirm the types and characteristics of infotainment systems assets as described in section 4.1.
- Impact Values: Based on section 4.3, confirm the overall impact values derived from assets and impact areas for each asset.
- Feasibility Values: Based on section 4.5, confirm the feasibility values of each asset for different attack paths and calculate their averaged sum.

- Risk Matrix: Refer to subsection 4.6.1 to confirm how the two pointers, Impact pointer and feasibility pointer, are mapped onto the risk matrix and how the resulting risk values are obtained.

From Figure 15, it can be observed that each asset has two values, impact values and feasibility values, both ranging from 1 to 5. These values represent the severity of the impact the asset faces and the feasibility of attacks on that asset under different attack paths. A higher value indicates greater impact and feasibility of attacks. Specific scoring criteria can be referenced from sections 4.3 and 4.5.

Taking the audio and video entertainment systems category as an example, for terrestrial radio systems, the feasibility value is 3.4, corresponding to a feasibility pointer of "Possible". Its impact value is 1.9, corresponding to an impact pointer of "Minor". By mapping these two pointers onto the risk matrix, the resulting risk value for this asset is "Low Med".

Risk Determinations (RD)							
No.	Asset Categorisation (AC)	Asset (A)	Feasibility Value (FV)	Impact Value (IV)	Feasibility Pointer (FP)	Impact Pointer (IP)	Risk Determination (RD)
RD01	Audio and Video Entertainment Systems	Terrestrial Radio Systems	3.4	1.9	Possible	Minor	Low Med
RD02	Audio and Video Entertainment Systems	Satellite Radio Systems	2.9	2.1	Possible	Minor	Low Med
RD03	Audio and Video Entertainment Systems	Media Playback Systems	3.2	2.1	Possible	Minor	Low Med
RD04	Audio and Video Entertainment Systems	Integrated Streaming Platforms	2.7	2.9	Possible	Moderate	Medium
RD05	Navigation Systems	Satellite-based GPS Units	2.8	3.9	Possible	Significant	Med Hi
RD06	Navigation Systems	Mapping and Visualization Systems	2.9	4.0	Possible	Significant	Med Hi
RD07	Navigation Systems	Traffic Data Systems	3.0	3.3	Possible	Moderate	Medium
RD08	Telephony and Messaging Systems	Bluetooth Connectivity Systems	3.1	4.1	Possible	Significant	Med Hi
RD09	Telephony and Messaging Systems	Voice Command Systems	3.2	3.3	Possible	Moderate	Medium
RD10	Driver Assistance Systems	Visual Systems	2.8	3.7	Possible	Significant	Med Hi
RD11	Driver Assistance Systems	Sensor Integration Systems	3.0	4.0	Possible	Significant	Med Hi
RD12	Driver Assistance Systems	Assistance Logic Systems	2.6	4.1	Possible	Significant	Med Hi
RD13	Internet and Wi-Fi Systems	Connectivity Systems	2.9	4.6	Possible	Severe	Med Hi
RD14	Internet and Wi-Fi Systems	Over-the-Air (OTA) Update Systems	2.3	4.6	Unlikely	Severe	Med Hi
RD15	Internet and Wi-Fi Systems	Integrated Browser and Apps	2.9	4.0	Possible	Significant	Med Hi

Figure 15. Risk Mapping and Determination of Smart Vehicles Infotainment Systems

4.7 Risk Treatment Decision

This section will focus on the risk treatment decision phase. The tasks in this phase are divided into two main steps. The first step is to identify and define risk treatment areas. This requires thoroughly considering the risks the assets face and exploring various feasible treatment methods to reduce risk to an acceptable level. Once this step is completed, each asset's most suitable risk treatment decisions will be detailed based on the attack paths described in section 4.4. This approach enables swift and appropriate risk treatment decision-making when the infotainment systems encounter different risks.

4.7.1 Risk Treatment Areas

This subsection will delve into identifying and defining Risk Treatment Areas. Following the guidance from "Managing Information Security Risk" by NIST (2011), comprehensive

consideration is given to handling risks associated with assets. As a result, risk treatment areas are categorised into four major categories: Mitigate, Avoid, Transfer, and Accept.

The defined risk treatment areas and their descriptions are as follows (NIST, 2011):

- Mitigate: Implement technical measures to reduce the risk to assets. For example, for the music streaming functionality of the infotainment systems, if potential security issues are identified, immediate software updates can be conducted to prevent unauthorised data extraction.
- Avoid: Choose not to include or disable features that are susceptible to attacks to avoid risk. For instance, if it is assessed that the video call functionality of the infotainment systems is prone to attacks, the decision might be to disable this feature in the system temporarily.
- Transfer: Offload certain risks to third parties, often through outsourcing or purchasing insurance. For example, for the cloud storage functionality of the infotainment systems, partnering with a professional cloud security provider might be chosen to manage data security.
- Accept: Accept certain low-probability or low-impact risks and continuously monitor them. For instance, the terrestrial radio in the infotainment systems is relatively low-risk and convenient for users after assessment. Accepting the risk is the decision in this case, but its security will still be continuously monitored.

4.7.2 Risk Treatment Evaluation

This subsection will focus on assessing the potential attack paths that the infotainment systems could face and formulating corresponding risk treatment decisions. To effectively formulate these decisions, the following core elements are integrated and considered:

- Infotainment Systems Asset Inventory: Refer to the asset inventory from section 4.1 to identify the specific types and characteristics of assets.
- Attack Paths: Based on the attack paths described in section 4.4, understand the relationships between these attack paths and the asset inventory.

- Risk Treatment Areas: Based on the risk treatment areas identified in subsection 4.7.1 and combining them with the possible attack paths for infotainment systems assets, provide risk treatment decisions for different attack scenarios that assets might face.

From Figure 16, it is evident that a specific asset of the infotainment systems, such as terrestrial radio, could potentially be vulnerable to the AP01 attack path (where an attacker broadcasts a deceptive signal, causing the vehicle wireless radio to connect to this signal and transmit incorrect or malicious information to users). In response to this potential attack path, the recommended risk treatment decision is risk mitigation: implementing strengthened signal verification and allowing connections only to known and trusted channels.

Risk Treatment Decisions (RTD)

No.	Asset Categorisation (AC)	Asset (A)	Attack Path (AP)	Risk Treatment Decision (RTD)
RTD01	Audio and Video Entertainment Systems	Terrestrial Radio	The attacker creates a fake station broadcast,causing the vehicle's radio to connectand deliver misinformation or malicious payloads to listeners.	Mitigate: Implementstrong signal verification and whitelisttrusted station frequencies.
RTD02	Audio and Video Entertainment Systems	Terrestrial Radio	The attacker uses equipmentto interfere with or modify the legitimate radio signal,altering or halting the broadcastfor users.	Transfer: Use encrypted signals for sensitive information or transition to digital radio solutions.
RTD03	Audio and Video Entertainment Systems	Terrestrial Radio	An advertiser or user claims a certain messagewas'nplayed, exploiting the lack ofplayback logs as proof.	Mitigate: Implementa transparentlogging mechanism to track allbroadcasts.
RTD04	Audio and Video Entertainment Systems	Terrestrial Radio	The attacker taps into unsecured or less-known channels to gather potentially sensitive information being shared.	Avoid: Ensure all private channels use encryption and require authentication.
RTD05	Audio and Video Entertainment Systems	Terrestrial Radio	The attacker uses jamming equipmentto interruptor block the radio signal,preventing users fromaccessing the service.	Mitigate: Introduce frequency-hopping or diversification techniques to counteracljamming attempts.
RTD06	Audio and Video Entertainment Systems	Terrestrial Radio	The attacker amplifies a malicious or fake radio signal, causing the system to prioritize itover legitimate signals due to perceived strength.	Accept:Update system logic to consider other factors besides justsignal strength. Monitor for unusual broadcast patterns.
RTD07	Audio and Video Entertainment Systems	Satellite Radio Systems	An attacker transmits counterfeit satellite signals, which the system processes as genuine, potentially providing false information.	Mitigate: Implementsignal authentication measures.Educate users aboutthe potential risks ofunauthenticated signals.
RTD08	Audio and Video Entertainment Systems	Satellite Radio Systems	The attacker intercepts and decrypts weakly encrypted signals, altering the contentbefore itreaches the receiver.	Avoid: Use advanced encryption methods. Ensure periodic key rotations and security patches.
RTD09	Audio and Video Entertainment Systems	Satellite Radio Systems	After accessing or altering data, the attacker denies their actions due to a lack ofproof from the system's side.	Transfer: Implementa robustlogging system.Partner with service providers thatoffer comprehensive transaction records.
RTD10	Audio and Video Entertainment Systems	Satellite Radio Systems	The attacker captures the satellite radio signal,gaining access to potentially sensitive information.	Mitigate: Introduce stronger signal protection and encryption.Limit the transmission of sensitive data over satellite radio.
RTD11	Audio and Video Entertainment Systems	Satellite Radio Systems	An attacker employs a jamming device to interruptthe satellite radio service, causing outages and potential hazards.	Transfer: Investin anti-jamming technologies and diversify signal sources. Prepare contingency plans for potential interruptions.
RTD12	Audio and Video Entertainment Systems	Satellite Radio Systems	The attacker exploits a known vulnerability in the radio system's firmware, gaining unauthorized access or privileges.	Accept:Regularly update firmware. Review and restrictuser and system privileges.
RTD13	Audio and Video Entertainment Systems	Media Playback Systems	Attacker tricks system into playing a malicious media file thatcontains embedded code. Once played, the code executes.	Mitigate: Implementstricter file validation. Train users to identify suspicious files.
RTD14	Audio and Video Entertainment Systems	Media Playback Systems	Attacker alters the contentofmedia files,potentially embedding misinformation or malicious instructions.	Mitigate: Use digital signatures to validate authenticity ofmedia files.
RTD15	Audio and Video Entertainment Systems	Media Playback Systems	After playing malicious or unauthorized content,the attacker denies actions due to lack ofconcrete logs.	Transfer: Implementdetailed playback logging mechanisms.Backup logs regularly.
RTD16	Audio and Video Entertainment Systems	Media Playback Systems	Attacker intercepts the transmission ofmedia files, leading to unauthorized access to potentially sensitive information within the media.	Mitigate: Encryptall media transmissions. Regularly update encryption algorithms.
RTD17	Audio and Video Entertainment Systems	Media Playback Systems	Attacker sends media files designed to exploitbuffer overflow, causing system crashes or unintended behavior.	Avoid: Patch known vulnerabilities. Implementinputvalidation for media files.
RTD18	Audio and Video Entertainment Systems	Media Playback Systems	An attacker with basic access exploits lax privilege settings to control or alter media playback functionalities.	Accept:Regularly review and tighten user permissions related to media controls.
RTD19	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker sets up a counterfeit streaming server, luring users to stream from it,which may lead to malware downloads or data exfiltration.	Mitigate: Implementsecure authorization mechanisms and domain whitelisting.
RTD20	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker injects malicious scripts or manipulates streaming data to compromise user devices or data.	Avoid: Incorporate strictinputvalidation and use a contentsecurity policy.
RTD21	Audio and Video Entertainment Systems	Integrated Streaming Platforms	After performing a malicious action, the attacker refutes itdue to a lack of proper logs thatcan prove their deed.	Transfer: Implementcomprehensive logging and use a log managementservice.
RTD22	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker decrypts the encrypted streaming data due to weak algorithms or keys, gaining access to proprietary or sensitive content.	Mitigate: Employ strong encryption methods and conductperiodic cryptographic reviews.
RTD23	Audio and Video Entertainment Systems	Integrated Streaming Platforms	Attackers overload the platform servers with excessive requests, causing service interruptions for legitimate users.	Transfer: Utilize scalable cloud infrastructure and deploy anti-DDoSsolutions.
RTD24	Audio and Video Entertainment Systems	Integrated Streaming Platforms	The attacker uses known vulnerabilities fromoutdated platformversions to gain unauthorized access or escalated privileges.	Accept:Regularly update the platformand review user permissions.
RTD25	Navigation Systems	Satellite-based GPS Unit	The attacker uses equipmentto broadcasta stronger fake GPSsignal to mislead the GPS receiver into calculating an incorrectlocation.	Mitigate: Implementanti-spoofing algorithms and use multi-frequency receivers.
RTD26	Navigation Systems	Satellite-based GPS Unit	The attacker uses jamming equipmentto block the GPS signals, causing the GPS unitto lose its location accuracy.	Transfer: Use secondary positioning methods (e.g., INS) as a backup.
RTD27	Navigation Systems	Satellite-based GPS Unit	After redirecting the GPS system,the attacker disables or deletes the logs to hide evidence ofmanipulation.	Mitigate: Secure the log storage and backup regularly.
RTD28	Navigation Systems	Satellite-based GPS Unit	An attacker intercepts unencrypted GPS data being transmitted, revealing sensitive details like the vehicle's currentand pastlocations.	Mitigate: Implementstrong end-to-end encryption for GPS data transmission.
RTD29	Navigation Systems	Satellite-based GPS Unit	The attacker uses a jammer to block GPS signals, rendering the GPS unitnon-functional and potentially affecting vehicle operations thatrely on accurate location data.	Mitigate: Use anti-jamming techniques and tools. Regularly update GPS firmware.
RTD30	Navigation Systems	Satellite-based GPS Unit	The attacker finds an outdated or unsecured firmware version and uploads a malicious version, gaining control or manipulating the GPS functionalities.	Accept:Regularly update and secure GPS firmware. Implementstrong access controls.
RTD31	Navigation Systems	Mapping and Visualization	The attacker feeds the system with fake GPS signals, leading to false map updates or misdirection.	Mitigate: ImplementGPS signal authentication and use encrypted data channels.
RTD32	Navigation Systems	Mapping and Visualization	The attacker adds harmful or misleading annotations or pins to the map thatcan deceive the driver.	Avoid: Restrictand monitor user-generated map content. Employ robustvalidation techniques.
RTD33	Navigation Systems	Mapping and Visualization	After modifying map data maliciously, the attacker denies any changes due to the absence of a proper logging mechanism.	Transfer: Implementa comprehensive logging mechanism and regular audits.
RTD34	Navigation Systems	Mapping and Visualization	The attacker accesses stored recentlocations, thereby compromising the privacy ofthe user.	Mitigate: Encryptstored location data and give users an option to clear location history.
RTD35	Navigation Systems	Mapping and Visualization	The attacker sends rapid and numerous route requests, causing the map system to crash or freeze.	Transfer: Optimize the map rendering process and limitthe rate ofincoming route requests.
RTD36	Navigation Systems	Mapping and Visualization	Using known exploits, the attacker accesses privileged map settings and makes unauthorized modifications.	Accept:Review and update user permission settings regularly. Conductfrequentsystem security checks.
RTD37	Navigation Systems	Traffic Data Systems	The attacker sends deceptive traffic information, misleading users aboutreal-time road conditions.	Mitigate: Implementdata source authentication. Use trusted traffic data providers only.
RTD38	Navigation Systems	Traffic Data Systems	The attacker intercepts and alters the traffic information being sentto the user's vehicle.	Mitigate: Use end-to-end encryption for data transmission. Regular monitoring and security audits.
RTD39	Navigation Systems	Traffic Data Systems	After sending malicious or altered traffic data, the attacker denies any involvementdue to the lack ofdata verification.	Transfer: Implementa system to verify the integrity ofreceived data. Use data signing or checksums.
RTD40	Navigation Systems	Traffic Data Systems	The attacker analyzes the received traffic data, extracting user patterns, habits, or frequently visited locations.	Mitigate: Anonymize user data before sharing with traffic systems. Implementstrictuser data policies.
RTD41	Navigation Systems	Traffic Data Systems	The attacker sends overwhelming amounts ofdata to the traffic server, causing service disruptions for users.	Mitigate: Implementrate limiting. Use cloud scalability and anti-DDoStools.
RTD42	Navigation Systems	Traffic Data Systems	The attacker uses a lower-level user accounts gain unauthorized access to more critical system functions.	Mitigate: Regularly review and update user role definitions. Periodic security training for employees.
RTD43	Telephony and Messaging Systems	Bluetooth Connectivity System	An attacker intercepts the initial pairing process, impersonating a legitimate device and establishing a connection.	Mitigate: Use secure pairing modes. Regularly update Bluetooth firmware.
RTD44	Telephony and Messaging Systems	Bluetooth Connectivity System	After intercepting data, the attacker retransmits the saved data packets, causing unintended actions.	Avoid: Implementstrong encryption for data transmission. Frequently change encryption keys.
RTD45	Telephony and Messaging Systems	Bluetooth Connectivity System	An attacker, after performing malicious activities, deletes Bluetooth activity logs, erasing any evidence.	Transfer: Use third-party log management.Ensure logs are backed up and protected.
RTD46	Telephony and Messaging Systems	Bluetooth Connectivity System	The attacker continuously scans for open Bluetooth devices, intercepting any unencrypted data being transmitted.	Mitigate: Setdevices to non-discoverable mode by default.Use end-to-end encryption for data.
RTD47	Telephony and Messaging Systems	Bluetooth Connectivity System	The attacker sends large or malformed data packets to the system,causing it to crash or become unresponsive.	Mitigate: Implementdata packetsize limits. Use monitoring tools to detectsuspicious activity.
RTD48	Telephony and Messaging Systems	Bluetooth Connectivity System	Attackers exploitknown vulnerabilities in outdated Bluetooth protocols to gain unauthorized access or higher privileges.	Accept:Regularly update Bluetooth protocols. Conductperiodic security audits.
RTD49	Telephony and Messaging Systems	Voice Command System	An attacker captures unencrypted voice commands to infer user habits, preferences, or private information.	Mitigate: Implementstrong end-to-end encryption for voice data.
RTD50	Telephony and Messaging Systems	Voice Command System	The attacker uses a recording or mimics the user's voice to issue unauthorized commands.	Avoid: Integrate biometric voice recognition features.
RTD51	Telephony and Messaging Systems	Voice Command System	The attacker exploits the system's interpretation flaws to execute unintended actions.	Mitigate: Update and refine voice recognition algorithms regularly.
RTD52	Telephony and Messaging Systems	Voice Command System	The attacker accesses stored voice command data to retrieve sensitive information.	Transfer: Store voice data in encrypted, segmented databases. Implementstrictaccess controls.
RTD53	Telephony and Messaging Systems	Voice Command System	The attacker uses loud noises or disruptive sounds to inhibitthe system's ability to receive or interpretcommands.	Mitigate: Implementadaptive noise cancellation technologies.
RTD54	Telephony and Messaging Systems	Voice Command System	The attacker bypasses normal command authorization processes to execute privileged actions.	Accept:Implementcommand authorization and regular system audits. Setlimits on system command scopes.
RTD55	Driver Assistance Systems	Visual Systems	The attacker broadcasts fake visual data to confuse the driver or passengers.	Mitigate: Implementstrong display authentication mechanisms. Provide user training to recognize unauthorized changes.
RTD56	Driver Assistance Systems	Visual Systems	The attacker inserts a harmful image/video, possibly containing malicious code, into the display system.	Avoid: Ensure rigorous validation for every image or video displayed. Integrate image sanitization mechanisms.
RTD57	Driver Assistance Systems	Visual Systems	After accessing the system,the attacker eliminates their interaction records, removing any evidence oftampering.	Transfer: Utilize third-party logging systems. Secure and frequently back up logs.
RTD58	Driver Assistance Systems	Visual Systems	The attacker retrieves personal user preferences, e.g, frequently visited places, by exploiting unsecured data practices.	Mitigate: Implementdata encryption.Periodically review and update data handling and storage practices.
RTD59	Driver Assistance Systems	Visual Systems	The attacker sends excessive data or commands to the visual system,causing it to freeze or malfunction.	Transfer: Investin system optimization tools and practices. Regularly review resource management protocols.
RTD60	Driver Assistance Systems	Visual Systems	An attacker gains access to visual modes or settings reserved for administrators or technicians.	Accept:Frequently update and review user permissions. Implementmulti-factor authentication for privileged access.
RTD61	Driver Assistance Systems	Sensor Integration	Attacker jams or floods sensor frequencies causing false readings or non-functionality.	Mitigate: Implementsensor anomaly detection, redundancy ofsensors, and frequentcalibration checks.
RTD62	Driver Assistance Systems	Sensor Integration	Attacker intercepts sensor data during transmission, potentially altering itbefore sending to the main system.	Mitigate: Employ encrypted sensor data transmission, validate data source.
RTD63	Driver Assistance Systems	Sensor Integration	Attacker accesses system and disables logging of sensor data, thus leaving no trace ofthe data manipulation.	Mitigate: Ensure logging is robustand protected fromunauthorized changes.Backup logs externally.
RTD64	Driver Assistance Systems	Sensor Integration	Attacker captures unencrypted sensor data as it's transmitted, gaining unauthorized knowledge.	Mitigate: Implementencryption protocols for all sensor data.
RTD65	Driver Assistance Systems	Sensor Integration	Attacker continuously sends invalid inputs to the sensors, causing them to malfunction or shutdown.	Transfer: Employ sensor inputvalidation, utilize overload protection measures.
RTD66	Driver Assistance Systems	Sensor Integration	Attacker gains access to sensor calibration settings, adjusting them to provide inaccurate data.	Mitigate: Restrictcalibration access, ensure any changes are authenticated and logged.
RTD67	Driver Assistance Systems	Assistance Logic System	The attacker sends false data to the system,tricking it into making incorrectdecisions or actions.	Mitigate: Improve sensor data verification.Add multi-sensor fusion techniques.
RTD68	Driver Assistance Systems	Assistance Logic System	Attacker inserts malicious firmware updates, potentially altering system behaviors or extracting data.	Avoid: Enhance secure OTAupdate methods. Implementa secure bootmechanism.
RTD69	Driver Assistance Systems	Assistance Logic System	Attacker, after accessing the system,deletes or changes logs to cover traces oftheir actions.	Transfer: Implementian external auditing system.Regularly back up logs.
RTD70	Driver Assistance Systems	Assistance Logic System	The attacker intercepts internal communication between components to gain valuable information.	Mitigate: Implementinter-componentencryption. Regular security checks for possible vulnerabilities.
RTD71	Driver Assistance Systems	Assistance Logic System	The attacker sends numerous requests or data to exhaustthe system's resources and cause malfunctions.	Transfer: Optimize system resources. Use cloud services for overload handling.
RTD72	Driver Assistance Systems	Assistance Logic System	The attacker finds ways to gain unauthorized access to functionalities restricted to higher-level users.	Accept:Regularly review user and system privileges. Implementmulti-factor authentication.
RTD73	Internetand Wi-Fi Systems	Connectivity Systems	The attacker guesses or brute-forces credentials,impersonating a trusted device or user to connectto the system.	Mitigate: Implementtwo-factor authentication and periodic password changes.
RTD74	Internetand Wi-Fi Systems	Connectivity Systems	The attacker intercepts and alters data packets during transmission, leading to misinformation or undesired actions.	Avoid: Implementdata integrity checks and end-to-end encryption.
RTD75	Internetand Wi-Fi Systems	Connectivity Systems	An attacker performs malicious actions butlater denies having done so due to lack oftraceability.	Mitigate: Ensure logging is robustand protected fromunauthorized changes.Backup logs externally.
RTD76	Internetand Wi-Fi Systems	Connectivity Systems	The attacker identifies open ports and captures data packets transmitted, accessing sensitive information.	Mitigate: Close unnecessary open ports and implementstrong encryption for data in transit.
RTD77	Internetand Wi-Fi Systems	Connectivity Systems	The attacker sends a large number ofrequests, aiming to overwhelmand crash the system.	Transfer: Use cloud-based solutions to handle excessive traffic and deploy anti-DDoStools.
RTD78	Internetand Wi-Fi Systems	Connectivity Systems	The attacker identifies and exploits known vulnerabilities in the connectivity software to gain higher privileges.	Accept:Regularly update and patch the connectivity software. Periodically review user and device privileges.
RTD79	Internetand Wi-Fi Systems	OTAUpdate System	Attacker sets up a malicious server, deceiving the vehicle into downloading malicious updates.	Mitigate: Implementstrictserver authentication and SSL pinning.
RTD80	Internetand Wi-Fi Systems	OTAUpdate System	Attacker intercepts an OTAupdate and injects malicious code, which then gets installed in the system.	Avoid: Use encrypted and digitally signed updates.
RTD81	Internetand Wi-Fi Systems	OTAUpdate System	Attacker accesses the system post-update and alters or deletes logs to remove traces ofmalicious activities.	Transfer: Use a secure,tamper-proof logging system.
RTD82	Internetand Wi-Fi Systems	OTAUpdate System	Attacker intercepts the OTAupdate transmission to gather confidential information or update details.	Mitigate: Ensure end-to-end encryption for all updates.
RTD83	Internetand Wi-Fi Systems	OTAUpdate System	Attacker sends numerous fake update requests to the server, causing genuine requests to be delayed or denied.	Transfer: Utilize robustcloud infrastructure and DDoSprotection.
RTD84	Internetand Wi-Fi Systems	OTAUpdate System	Attacker sends an OTAupdate which, when installed, grants them higher system privileges.	Accept:Regularly review and limitpermissions ofupdates. Implementuser/admin checks.
RTD85	Internetand Wi-Fi Systems	Integrated Browser and Apps	The attacker impersonates a trusted organization or individual,successfully deceiving the server or users to access sensitive information.	Mitigate: ImplementSSL pinning. Strengthen user security training to enhance identification offorged certificates.
RTD86	Internetand Wi-Fi Systems	Integrated Browser and Apps	The attacker inputs SQL commands in inputfields, attempting to control the database and execute unintended commands.	Avoid: Implementstrictinputvalidation and use parameterized queries. Regular security monitoring and testing.
RTD87	Internetand Wi-Fi Systems	Integrated Browser and Apps	After gaining system access, the attacker deletes or modifies their activity logs, thereby erasing evidence oftheir malicious actions.	Transfer: Use a third-party log managementsystem.Ensure logs are properly backed up and protected.
RTD88	Internetand Wi-Fi Systems	Integrated Browser and Apps	The attacker establishes a connection between the user and the server, intercepting and/or modifying information transmitted over this connection.	Mitigate: Implementend-to-end encryption and regularly update TLS/SSL certificates. Train employees to recognize insecure connections.
RTD89	Internetand Wi-Fi Systems	Integrated Browser and Apps	The attacker overwhelms the system by continuously sending a large number ofqueries or requests, aiming to cause service interruptions.	Transfer: Use cloud infrastructure to distribute traffic. Investin anti-DDoStools and solutions.
RTD90	Internetand Wi-Fi Systems	Integrated Browser and Apps	The attacker explores and exploits known vulnerabilities in the browser or its engine to gain higher privileges than their original access.	Accept:Implementregular browser and plugin updates. Review user permission settings periodically.

Figure 16. Risk Treatment Decisions of Smart Vehicles Infotainment Systems

5. Discussion

This chapter will focus on presenting the discussion of this project. The discussion will be divided into main findings and interpretation, comparison with existing research, and limitations. The following will provide a detailed description of each of these sections.

5.1 Main Findings and Interpretation

This project presents a comprehensive threat analysis and risk assessment of smart vehicles infotainment systems, detailing a series of processes and outcomes in chapter 4. This section will focus on discussing the security risk levels determined for the infotainment systems of smart vehicles in section 4.6 and further analyse the following observations:

Audio and Video Entertainment Systems: Within the audio and video entertainment systems, most subsystems, such as terrestrial radio, satellite radio, and media playback systems, have risk levels predominantly categorised as "Low Med". However, the risk level for the integrated streaming media platforms is elevated to Medium. The reason can be found in the impact value of integrated streaming media platforms, which is relatively higher than other audio and video entertainment systems. This suggests the presence of higher security concerns within the integrated streaming media platform.

Navigation Systems: Within the navigation systems, aside from the medium risk level of the traffic data systems, other components such as satellite-based GPS units and mapping visualisation systems have risk levels reaching "Med Hi". The reason can be found in the impact value of traffic data systems, which is lower than other navigation systems. This indicates that security threats have less influence on traffic data systems.

Telephony and Messaging and Driver Assistance Systems: Within the communication and assistance systems, functionalities like Bluetooth, voice command systems, and driver assistance systems are often considered important in daily usage. Thus, their risk levels extend to "Med Hi". This implies that these systems could serve as main targets that attackers might repeatedly exploit.

Internet and Wi-Fi Systems: It is crucial to closely monitor all the Internet and Wi-Fi systems because the risk levels of all systems are reaching "Med Hi". Especially detailed observing over-the-air (OTA) update systems. Despite having a relatively low feasibility score, its

impact score is remarkably high. This indicates that the consequences could be catastrophic if these systems were compromised.

Overall Risk Distribution: Considering the overall data, most of the infotainment systems of smart vehicles exhibit significant risks across various functionalities, particularly in navigation, communication, driver assistance and network systems.

These findings highlight the importance of a comprehensive analysis of the security risks associated with the infotainment systems of smart vehicles. The varying risk levels across different subsystems and functionalities emphasise the need for targeted risk treatment strategies in 4.7 to ensure the safety and security of smart vehicles and their occupants.

5.2 Comparison with Existing Research

This section will focus on comparing the present project with existing research concerning the infotainment systems of smart vehicles. This project adopts a comprehensive approach by utilising the Threat Analysis and Risk Assessment (TARA) framework based on ISO/SAE 21434 (ISO, 2021) to conduct thorough threat analysis and risk assessment of the infotainment systems in smart vehicles. This strategy significantly differentiates this project from most of the existing research.

Past studies often concentrate on specific subsystems or are conducted within specific environments. For instance, some research delves into the security and privacy issues brought about by Bluetooth connections in vehicles (Renganathan et al., 2022), while others focus on potential vulnerabilities in the Wi-Fi functionality of infotainment systems (Josephlal and Adepu, 2019). Furthermore, in previous studies, there needs to be a more comprehensive threat analysis and risk assessment of the infotainment systems in smart vehicles. For example, some studies solely explain and implement the TARA framework from ISO/SAE 21434 (Dantas et al., 2021) or broadly provide a list of potential threats and vulnerabilities that smart vehicles might face (UNECE, 2021). Furthermore, although methodologies utilising the TARA framework have been proposed in the past, limited research focuses on conducting threat analysis and risk assessment specifically for smart vehicles infotainment systems.

This project not only provides a comprehensive threat analysis and risk assessment for smart vehicles infotainment systems but also incorporates the practical application of the

framework in real-world scenarios and considers the dynamics of cybersecurity. These advantages enable this research to practically implement the TARA framework for smart vehicles infotainment systems, encompassing asset identification, threat scenarios, systems vulnerabilities, attacker paths, and corresponding risk values. Furthermore, a series of risk mitigation strategies are presented, forming a practical and concrete set of application guidelines.

5.3 Limitations

This section will discuss the limitations of the threat analysis and risk assessment of the infotainment systems in smart vehicles. The following will provide a detailed explanation of the limitations faced by this project.

5.3.1 Data Limitations

This project relied on secondary data, including an extensive literature review and data integration, for conducting the infotainment systems threat analysis and risk assessment. Firstly, relying on secondary data implies that the data's quality, scope, and content might influence the conclusions of this project. Furthermore, considering the accelerated growth in technology and cybersecurity, secondary data might not encompass the latest threats and vulnerabilities.

5.3.2 Tool and Technology Limitations

This project used Excel as the primary tool for data integration and analysis of the infotainment systems. However, for vast and complex datasets that require the application of multiple spreadsheets, Excel might not be the most efficient tool. Additionally, Excel might present challenges in producing graphics, such as efficiently generating the risk matrix by textual descriptions.

5.3.3 Limitations of the TARA Framework

This project is based on the threat analysis and risk assessment of the infotainment systems of the TARA framework from ISO/SAE 21434. While TARA is considered a powerful and comprehensive framework, it still has limitations. Firstly, subjectivity is present, for instance, in assessing impact and attack feasibility within the TARA framework (Dantas et al., 2021). This assessment process might lead to different outcomes based on different assessors,

standards, and objectives. Additionally, adaptability is a challenge. Since security threats evolve, regular threat analysis and risk assessment process updates are crucial to avoid outdated results. Lastly, due to the subdivision of assets in the asset identification stage of the TARA framework (Dantas et al., 2021), it might be challenging to identify certain interrelated threats and risks in complex systems environments.

5.3.4 Time Limitations

Due to time constraints and considerations, the depth and breadth of this project might be affected. The infotainment systems involve various technologies and applications, and despite attempting an in-depth exploration and analysis of around 50 sources, there might still be areas of the infotainment systems that need to be more thoroughly considered. For instance, this project did not extensively analyse specific threats to certain hardware or software versions of the infotainment systems.

6. Conclusions

This chapter will focus on presenting the conclusions of this project. The conclusions will be divided into contributions and future work of this project. The following will provide detailed descriptions of each section.

6.1 Contributions

This project is based on the Threat Analysis and Risk Assessment (TARA) framework outlined in ISO/SAE 21434 (ISO, 2021). It presents a comprehensive process, threat analysis results, and risk assessment for smart vehicles infotainment systems. This includes an in-depth exploration of the assets, threat scenarios, systems vulnerabilities, attacker paths, and corresponding risk values of the infotainment systems, along with appropriate risk mitigation strategies. Through this series of analyses and evaluations, the project addresses the core question: "How to conduct a comprehensive threat analysis and risk assessment for smart vehicles infotainment systems to reduce cybersecurity risks and enhance the systems security effectively?"

Furthermore, the research provides a clear and practical guideline for stakeholders regarding smart vehicles infotainment systems threat analysis and risk assessment. This guideline aims to decrease cybersecurity risks, improve the safety of drivers and passengers, and enhance the overall security and resilience of smart vehicles infotainment systems.

6.2 Future Work

This section will discuss future directions for the threat analysis and risk assessment of the infotainment systems in smart vehicles. The following will provide a detailed explanation of several directions for future work in this project.

6.2.1 Refinement of Asset Identification

As mentioned in subsection 5.3.4, due to time constraints, this project could not extensively categorise the highly complex infotainment systems, resulting in the possibility of omitting certain areas or not giving them thorough consideration. In future research, the assets within the infotainment systems could be categorised in greater detail. This approach would enable more precise threat analysis and risk assessment for both main systems and

subsystems. Additionally, risk assessment for interrelated systems could be conducted more accurately through asset-based refinement.

6.2.2 Enhancement of Methodology

While this project conducted the threat analysis and risk assessment based on the TARA framework and used appropriate assessment indicators and methods for scoring, there is still room for further improvement in the scoring process. Taking the impact rating of threat scenarios for the infotainment systems assets described in section 4.3, this project included the threat scenarios as reference options and then performed an impact rating for infotainment systems. However, future research could adopt a more detailed assessment process. Specifically, an additional step could be introduced to perform a comprehensive rating for all threat scenarios of the infotainment systems assets rather than treating them as reference options. This approach would provide more accurate impact values for threat scenarios of the infotainment systems assets.

6.2.3 Attack Path Simulation

This project inferred potential attack paths of smart vehicles infotainment systems based on collected and analysed literature data on potential threats. However, relying solely on literature data for inferring attack paths might have limitations. To gain a deeper understanding of the actual process and impact of real attacks, future research could create practical attack simulation environments and conduct attack testing using programming. This approach would provide a more profound insight into the effects and impact of actual attacks on real assets.

6.2.4 Technological Developments and Emerging Threats

The threat landscape for infotainment systems is dynamic. Technologies such as 6G communication, blockchain, and edge computing could introduce new security challenges. While these technologies offer enhanced functionality and convenience for infotainment systems, they also provide new attack vectors for malicious actors (Algarni and Thayananthan, 2023). Therefore, future research could focus on potential threats introduced by these new technologies and explore ways to establish appropriate protective mechanisms to mitigate threat risks as infotainment systems adapt to these innovations.

References

Abdelkader, G., Elgazzar, K., & Khamis, A. (2021). Connected Vehicles: Technology Review, State of the Art, Challenges and Opportunities. *Sensors*, *21*(22), Article 22. https://doi.org/10.3390/s21227712

Algarni, A. M., & Thayananthan, V. (2023). Autonomous Vehicles With a 6G-Based Intelligent Cybersecurity Model. *IEEE Access*, *11*, 15284–15296. https://doi.org/10.1109/ACCESS.2023.3244883

Anwar, M. N., Nazir, M., & Ansari, A. M. (2020). Modeling Security Threats for Smart Cities: A STRIDE-Based Approach. In S. Ahmed, S. M. Abbas, & H. Zia (Eds.), *Smart Cities—Opportunities and Challenges* (pp. 387–396). Springer. https://doi.org/10.1007/978-981-15-2545-2_33

Bolovinou, A., Atmaca, U.-I., Sheik, A. T., Ur-Rehman, O., Wallraf, G., & Amditis, A. (2019). TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems. *2019 IEEE Intelligent Vehicles Symposium (IV)*, 8–13. https://doi.org/10.1109/IVS.2019.8813999

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 557–562. https://doi.org/10.1109/PERCOMW.2017.7917623

Burnap, P. (2021) 'Risk management & governance knowledge area version', in CyBOK. https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf

Cardenas, A. and Cruz, S. (2021). 'Cyber-physical systems security knowledge area version', in CyBOK. https://www.cybok.org/media/downloads/Cyber_Physical_Systems-v1.0.1.pdf

Costantino, G., La Marra, A., Martinelli, F., & Matteucci, I. (2018). CANDY: A Social Engineering Attack to Leak Information from Infotainment System. *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 1–5. https://doi.org/10.1109/VTCSpring.2018.8417879

FIRST. (2023). *CVSS v4.0 Specification Document*. https://www.first.org/cvss/v4.0/specification-document

Dantas, Y. G., Nigam, V., & Ruess, H. (2021). *Security Engineering for ISO 21434* (arXiv:2012.15080). arXiv. http://arxiv.org/abs/2012.15080

Ebrahimi, M., Striessnig, C., Triginer, J. C., & Schmittner, C. (2022). *Identification and Verification of Attack-Tree Threat Models in Connected Vehicles*. 2022-01–7087. https://doi.org/10.4271/2022-01-7087

El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity Attacks in Vehicular Sensors. *IEEE Sensors Journal*, *20*(22), 13752–13767. https://doi.org/10.1109/JSEN.2020.3004275

ENISA. (2010). *Flying 2.0—Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology*. https://www.enisa.europa.eu/publications/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology

Guerrero, H. (2019). *Excel Data Analysis: Modeling and Simulation*. Springer International Publishing. https://doi.org/10.1007/978-3-030-01279-3

Haas, R. E., & Möller, D. P. F. (2017). Automotive connectivity, cyber attack scenarios and automotive cyber security. *2017 IEEE International Conference on Electro Information Technology (EIT)*, 635–639. https://doi.org/10.1109/EIT.2017.8053441

Hashem Eiza, M., & Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Vehicular Technology Magazine*, *12*(2), 45–51. https://doi.org/10.1109/MVT.2017.2669348

ISO. (2021). *ISO/SAE 21434:2021(en), Road vehicles—Cybersecurity engineering*. https://www.iso.org/obp/ui/en/#iso:std:iso-sae:21434:ed-1:v1:en

Jeong, S., Ryu, M., Kang, H., & Kim, H. K. (2023). Infotainment System Matters: Understanding the Impact and Implications of In-Vehicle Infotainment System Hacking with Automotive Grade Linux. *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, 201–212. https://doi.org/10.1145/3577923.3583650

Josephlal, E. F. M., & Adepu, S. (2019). Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability. *2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)*, 241–246. https://doi.org/10.1109/HASE.2019.00044

Katsumata, P., Hemenway, J., & Gavins, W. (2010). Cybersecurity risk management. *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, 890–895. https://doi.org/10.1109/MILCOM.2010.5680181

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, *6*(1), 111. https://doi.org/10.1186/s40537-019-0268-2

Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected Vehicles: Solutions and Challenges. *IEEE Internet of Things Journal*, *1*(4), 289–299. https://doi.org/10.1109/JIOT.2014.2327587

Luo, F., Jiang, Y., Zhang, Z., Ren, Y., & Hou, S. (2021). Threat Analysis and Risk Assessment for Connected Vehicles: A Survey. *Security and Communication Networks*, *2021*, e1263820. https://doi.org/10.1155/2021/1263820

Macher, G., Schmittner, C., Veledar, O., & Brenner, E. (2020). ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell. In A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch, & P. Ferreira (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops* (pp. 123–135). Springer International Publishing. https://doi.org/10.1007/978-3-030-55583-2_9

Mandal, A. K., Cortesi, A., Ferrara, P., Panarotto, F., & Spoto, F. (2018). Vulnerability analysis of Android auto infotainment apps. *Proceedings of the 15th ACM International Conference on Computing Frontiers*, 183–190. https://doi.org/10.1145/3203217.3203278

Mandal, A. K., Panarotto, F., Cortesi, A., Ferrara, P., & Spoto, F. (2019). Static analysis of Android Auto infotainment and on-board diagnostics II apps. *Software: Practice and Experience*, *49*(7), 1131–1161. https://doi.org/10.1002/spe.2698

Mazloom, S., Rezaeirad, M., Hunter, A., & McCoy, D. (2016). *A Security Analysis of an {In-Vehicle} Infotainment and App Platform*. 10th USENIX Workshop on Offensive Technologies (WOOT 16). https://www.usenix.org/conference/woot16/workshop-program/presentation/mazloom

Meixner, G., Häcker, C., Decker, B., Gerlach, S., Hess, A., Holl, K., Klaus, A., Lüddecke, D., Mauser, D., Orfgen, M., Poguntke, M., Walter, N., & Zhang, R. (2017). Retrospective and Future Automotive Infotainment Systems—100 Years of User Interface Evolution. In G.

Meixner & C. Müller (Eds.), *Automotive User Interfaces: Creating Interactive Experiences in the Car* (pp. 3–53). Springer International Publishing. https://doi.org/10.1007/978-3-319-49448-7_1

NIST. (2011). Managing Information Security Risk Organization, Mission, and Information System View JOINT TASK FORCE TRANSFORMATION INITIATIVE. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

NIST. (2018). Risk Management for Automotive Cybersecurity. https://www.nist.gov/system/files/documents/2018/12/06/risk_management_for_automotive_cybersecurity.pdf

Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber security attacks to modern vehicular systems. *Journal of Information Security and Applications*, *36*, 90–100. https://doi.org/10.1016/j.jisa.2017.08.005

Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors*, *22*(17), Article 17. https://doi.org/10.3390/s22176679

Renganathan, V., Yurtsever, E., Ahmed, Q., & Yener, A. (2022). Valet attack on privacy: A cybersecurity threat in automotive Bluetooth infotainment systems. *Cybersecurity*, *5*(1), 30. https://doi.org/10.1186/s42400-022-00132-x

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Article 4. https://doi.org/10.3390/fi11040089

Scalas, M., & Giacinto, G. (2019). Automotive Cybersecurity: Foundations for Next-Generation Vehicles. *2019 2nd International Conference on New Trends in Computing Sciences (ICTCS)*, 1–6. https://doi.org/10.1109/ICTCS.2019.8923077

Takahashi, J., Iwamura, M., & Tanaka, M. (2020). Security Threat Analysis of Automotive Infotainment Systems. *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, 1–7. https://doi.org/10.1109/VTC2020-Fall49728.2020.9348647

Uhlemann, E. (2015). Introducing Connected Vehicles [Connected Vehicles]. *IEEE Vehicular Technology Magazine*, *10*(1), 23–31. https://doi.org/10.1109/MVT.2015.2390920

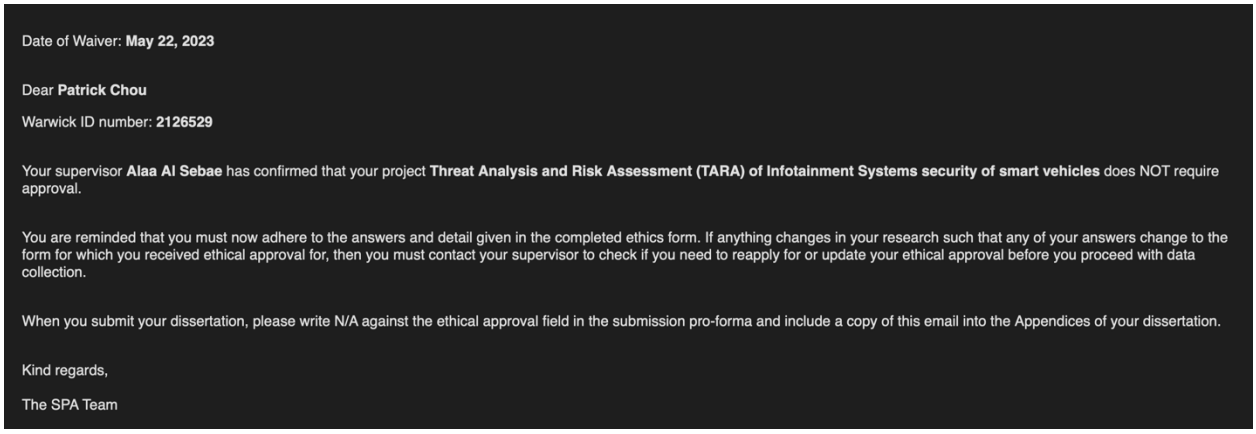
Uhlemann, E. (2016). Connected-Vehicles Applications Are Emerging [Connected Vehicles]. *IEEE Vehicular Technology Magazine*, *11*(1), 25–96. https://doi.org/10.1109/MVT.2015.2508322

UNECE. (2021). *UN Regulation No. 155 - Cyber security and cyber security management system*. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

Yang, D., Jiang, K., Zhao, D., Yu, C., Cao, Z., Xie, S., Xiao, Z., Jiao, X., Wang, S., & Zhang, K. (2018). Intelligent and connected vehicles: Current status and future perspectives. *Science China Technological Sciences*, *61*(10), 1446–1471. https://doi.org/10.1007/s11431-017-9338-1

Appendices

Appendix A. Ethical Approval



Date of Waiver: **May 22, 2023**

Dear **Patrick Chou**

Warwick ID number: **2126529**

Your supervisor **Alaa Al Sebae** has confirmed that your project **Threat Analysis and Risk Assessment (TARA) of Infotainment Systems security of smart vehicles** does NOT require approval.

You are reminded that you must now adhere to the answers and detail given in the completed ethics form. If anything changes in your research such that any of your answers change to the form for which you received ethical approval for, then you must contact your supervisor to check if you need to reapply for or update your ethical approval before you proceed with data collection.

When you submit your dissertation, please write N/A against the ethical approval field in the submission pro-forma and include a copy of this email into the Appendices of your dissertation.

Kind regards,

The SPA Team

Figure 17. Ethical Approval