Cyber Risks Assessment for Connected and Autonomous Vehicles

Asrar Esmaeel Alahmadi

Supervisor: Neetesh Saxena

MCs Cybersecurity

School of computer science and informatic

Cardiff University

October 2022

Cyber Risks Assessment for Connected and Autonomous Vehicles

Asrar Esmaeel Alahmadi

2071018

Dr. Neetesh Saxena

MCs Cybersecurity

School of computer science and informatic

Cardiff University

October 2022

CMT400

Abstract

With the development of autonomous vehicles, the vehicles' sphere of interest has expanded to involve everything related to the vehicle from the infrastructure to the other vehicles that share the road to create what is known as connected and autonomous vehicles (CAVs). As with all technological developments, the threat has also increased. CAVs bring new methods of attack and provide opportunities for attackers who specialise in multiple areas. This work studies and analyses the threats to CAVs by establishing a risk assessment method derived from previous works to match the vital functions of modern technologies and CAVs and thereby develop a tool that helps with the application of the proposed method. It also presents two case studies of CAVs vital functions and their associated risks.

Acknowledgements

First of all, I would like to thank the government of the Kingdom of Saudi Arabia for accepting me into the scholarship program and providing the necessary support.

I would like to express my gratitude to my supervisor, Dr. Neetesh Saxena, who guided me throughout this project. I would like also to extend my special thanks to Cardiff university for providing the support and facilities necessary to complete this program. I am also grateful to my friends who supported me and gave me great advice.

Lastly, my family deserves endless gratitude for their belief in me has kept my spirits and motivation high during this year.

Table of Contents

Table of Figures

Table of Tables

List of Abbreviations

CAV	Connected and autonomous vehicle
AV	Autonomous vehicle
ECU	Electronic control unit
V2V	Vehicle to Vehicle
V2I	Vehicle to infrastructure
V2X	vehicle-to-everything
OTA	Over-the-Air
OEM	original equipment manufacturer
TARA	Threat Analysis and Risk Assessment methods
DoS	Denial of services

Chapter 1. Introduction

In recent years, the concept of intelligent transportation has evolved from the development of self-driving autonomous vehicles (AVs) to autonomous control which includes communications between vehicles and everything that surrounds them – CAVs. Communication increases the vehicles' autonomy and improves safety, but the diversity of components and technologies used has led to an increase in attack surfaces and techniques which have evolved with the vehicles so that the threats have moved from threats to privacy and individual safety to a threat to national security. Analysis and assessment of risk models have become popular topics for AV and CAV design as manufacturers study attacks from different aspects. Due to the diversity of the attack techniques and attack surfaces, the identification of methods and motives may differ from one model to another. In this paper, a risk assessment method is proposed based on previous studies and covers some of the limitations to match the structure and vital functions of CAV, linking them to mitigation methods based on their level of risk.

1.1 Context and scope

AVs could enhance the effectiveness of transportation, the quality of life of its users and reduce the number of traffic accidents. Future intelligent vehicles will communicate with other internet-enabled devices such as other vehicles or infrastructure as they become better connected to the internet and to their surroundings. The most serious security threats are still to reveal themselves. Threats to engine controls, tyre pressure monitoring systems or wireless key fobs are just a few examples of the many new attack vectors and vulnerabilities that have emerged. The attack on autonomous and communication functions would constitute the main part of the risk identification in this thesis, excluding safety risks such as sensor quality, incorrect inputs, and artificial intelligence errors.

1.2 Aim

This research aims to understand the use of CAVs by recognising the critical assets and functions that could be affected by risks and performing a modelling assessment.

1.3 Objectives

1. Analysing the latest risk assessment methods and models to find any gaps.
2. Developing risk assessment methods and tools for CAVs.
3. Performing the methodology in a case study.

1.4 Challenges

A variety of tasks and duties are carried out by CAVs in extremely dynamic settings that frequently modify the threats, weaknesses and technology. Because of this, there has been little research into how to deal effectively with the dynamic dangers that CAVs face. Cyber-risk assessment has the benefit of updating and seeing the dangers from many aspects, thus it might be used to forecast undiscovered threats.

There is a variety of opinions on risk assessment depending on the system levels which can be used to guide the choice of monitoring data and assessment methods. As an illustration of a system level, consider the vehicle which focuses on the evaluation of the safety and security risks posed by the vehicle and other nearby vehicles. The road sign level, by contrast, focuses on regulating the safety and security of a local region, mostly by monitoring the traffic flow and other information sources that provide particular aspects of the situation along the road.

Security analysis of CAVs comes with several challenges:

- CAVs are still under development. Highly- and fully-automated driving systems are still being researched. As a result, CAV systems lack a reference architecture.
- It is difficult to assess every attack and threat. With the diversity of vehicle manufacturers and the varying quality of sensors and other components, the difficulty of threat identification increases with its development.
- This dynamic nature is a major obstacle to risk assessment and the study of the environment and the conditions around the vehicle.

1.5 Effect of the work

Studying cyber security attacks on CAV by classifying them and summarising the corresponding countermeasures could be helpful for the development of CAVs and intelligent transportation systems. This may be useful for policymakers, engineers and researchers in coping with unknown security threats the CAVs in the future where the major effect is related to the safety of the people involved in potential malfunctions. The risk assessment of hazardous events focuses on the harm to each person potentially at risk, such as the driver or the passengers of the vehicle causing the hazardous event. Other people potentially influenced by the considered vehicle malfunction like cyclists, pedestrians or occupants of other vehicles should also be considered. Also, the negative effects on the infrastructure and traffic flow.

1.6 Thesis organisation

Chapter 2 presents the literature review of the topic and compares and analyses existing methods to explain the proposed method. Chapter 3 describes the approach and methodology used and Chapter 4 presents the risk assessment for CAVs derived from previous methods. The results and evaluation of the method and tools are presented in Chapter 5. Finally, Chapter 6 presents the conclusions and future work for this topic.

Chapter 2. Background

2.1 Overview

In this chapter, the background of the CAV will be explored to understand the CAVs and their risk assessment. The second part examines potential risks to CAVs and the existing risk assessment models and methods.

2.2 Background

2.2.1 CAVs

Over the last decade, the idea of an intelligent transportation system has expanded as smart city concepts have been developed, incorporating CAVs, vehicles that drive themselves and complete their duties autonomously, communicating with other entities around it. Sensing the surrounding area, gathering data and maintaining communication with other cars are some of the attributes of the CAV. Cameras, sensors, GPS, radar, lidar and onboard computers are all used by the AVs which are currently under development. The position of the vehicle and everything nearby is mapped using a combination of these technologies. These fully AVs, also known as driverless or self-driving vehicles, are robotic systems based on the 'sense, plan, act' paradigm (Dickmanns et al. 1994; Christensen et al. 2015; Bailey 2018) and defined as Level 5 cars as the top of the SAE (standing for the Society of Automotive Engineers) automated scale (these definitions are explored below). A driverless car can fully see its surroundings, react safely and do all of this without a human sitting in the driver's seat. In fact, it is possible that such vehicles will not even have steering wheels or pedals in the future.

These days, advanced driver assistance systems (ADAS)are standard in the majority of new cars. The technology aids and supports drivers in emergency interventions such as emergency braking and comfort enhancements like cruise control but they do not automatically possess self-driving capabilities just because ADAS technology is installed. An AV differs significantly from an ADAS-equipped vehicle, both philosophically and technically. AVs are conceptualised as a single, fully integrated body that is driven by software, in contrast to ADAS cars. Technically, the application of artificial intelligence (AI) enables the AV to learn from events, make decisions that

may be quite similar to those of humans and even improve their average predicted performance (Di Lillo et al. 2021).

The expansion of the connectivity in smart cars came in conjunction with the expansion of the concept of the Internet of Things. As a result, the communication between vehicles and infrastructure has received a great deal of attention to growing the intelligent transport system. Vehicle-to-everything (V2X)-enabled CAVs can deliver better and new services to society. Connected vehicles equipped with communication devices and within a connected infrastructure environment could collect previously unobtainable traffic data and can also share that information with other connected vehicles and monitoring units.

A CAV may be thought of as a cyber-physical system with driving software backed by several embedded sensors such as GPS, radar, lidar and ultrasonics to perceive the driving surroundings mixed with actuators (Le and Maple 2019). The electronic control units (ECUs) which act as the brain of the vehicle are capable of supporting a number of wireless network protocols including Wi-Fi, Bluetooth and vehicle-to-everything (V2X) communication. V2X is the transmission of data from a vehicle to any entity that may affect the vehicle and vice versa (Meyer et al. 2021). V2V is the link between vehicles, whereas V2I is the connection between a vehicle and the infrastructure used for transportation.

2.2.2 The important components of the CAV

The connected and autonomous vehicle combines information technology with mechanical components to create functions that go beyond the boundaries of autonomous driving and exchange information with the surrounding environment. The components of the connected and autonomous vehicle have been listed in previous studies (Pham and Xiong 2021; Maple et al. 2019; Di Lillo et al. 2021; He et al. 2020; Chow et al. 2021):

- **ECUs** are integrated electronic systems that control the main components and other sub-systems of the vehicle. The ECUs take the external environment information from the inputs of sensors and the vehicle network, then process it and make decisions based on information technologies in addition to sending control signals to the rest of the components such as tyre

pressure monitoring systems, the engine, cabin environment and media control unit.

- **Sensors.** Vehicles have special sensors that are responsible for sensing and understanding the environment around the vehicle. The most significant are:
    - Light Detection And Ranging (LiDAR). The sensor detects obstacles by sending light waves to illuminate the target and analysing the reflected light for measurements. It might help in creating high-resolution 3D maps of the vehicle's surroundings to navigate safely through environments.
    - Radio Detection and Ranging (Radar). The radar is a sensor based on transmitting radio waves to measure distance and speed, in addition to detecting objects. CAVs contain two types of radar. One measures short distances by sending ultrasonic waves to be used, for example, in the parking assistance system, while the other uses millimetre waves to detect objects which makes it limited to short distances which means that detecting high speed movement would be difficult.
    - GNSS (Global Navigation Satellite System). This helps the vehicle to accurately locate and navigate the vehicle. It is a satellite-based navigation system that transmits high-frequency radio signals which are received by smartphones and GPS receivers in CAVs. The most widely used GNSS system is GPS, which is funded and owned by the United States government.
    - Cameras (image sensors). Vehicles mainly rely on cameras placed in many positions to get a 360-degree view around the vehicle to capture images of its surroundings and create a 3D view of the environment in addition to detecting surrounding objects and the position of the vehicle. The camera performs many tasks such as reading road signs and recognising traffic lights and obstacles.

    The cameras, radar and lidar work together to provide various features for autonomous driving.

- **Intra-vehicular links**. ECUs are usually connected through wired and wireless communications between sensors, ECUs, telecommunications units and end-user equipment within a vehicle and are therefore of great

importance. ECUs are usually connected through a wired network such as CAN or FlexRay. CAVs do not include an authentication field or a source identification field when network packets are sent to all nodes in the CAVs network (Thing and Wu 2016).

- Inter-vehicular links. CAVs can connect to everything surrounding the vehicle. V2X allows a vehicle to maintain contact with its surroundings and is one of the main types of vehicle communication. Vehicles can exchange their state and location and sensor access to nearby vehicles via vehicle-to-vehicle (V2V) links. V2I and I2V represent the connection between the vehicle and the infrastructure and vice versa, this feature supports a variety of traffic management services and applications. The vehicle can connect to smartphones (V2P) to share information with pedestrians or cyclists. These communication methods help greatly improve location accuracy and prevent accidents.

2.2.3 Security challenges and difficulties in CAVs

Security in CAVs faces many challenges due to their nature and complexity. These challenges represent an obstacle to the development of security technologies. The following are the most important challenges that are derived from the characteristics of the internet of vehicles (IoV) mentioned by Kim and Shrestha (2020).

- **Complex communications**. There are many communications inside and outside the vehicle. Some of them connect sensors to ECUs and transmit data to various components of the vehicle, in addition to communication between the vehicle and the surrounding objects where the vehicle exchanges information with vehicles, infrastructure and people to create interactions aimed at increasing safety on the roads by sending alerts to other entities. Road scenarios vary from moving at a low or high speed and this affects the density of vehicles, which leads to complex communication networks.
- **Dynamic Structure**. The vehicle has multiple heterogeneous components that interact with each other to complete the vehicle's functions and maintain the safety of the vehicle, inside and outside. Therefore, the speed in changing the network structure is caused by the movement of vehicles at high speed on the roads which makes it difficult for secure communication protocols to transfer packets quickly due to the rapid structure change.

- **High scalability**. The network expands with the density and congestion of road users, vehicles and people which makes it difficult to study attack methods and potential attack surfaces because of the growing range of attack scenarios and the diversity of potential attack targets for each asset associated with CAV components, creating a large-scale environment for attackers.

2.2.4 The SAE standard

The determination of automation levels of the vehicles is determined by the degree to which a human driver or vehicle system participates in the driving decisions, which is closely related to the safety of AVs. These factors include the complexity of the autonomous technology used, the environment's perceptual range and the level of automation.

The SAE Levels of Driving Automation, also known as SAE J3016TM Recommended Practice: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, has been the most widely used reference for driving automation in the market since its release in 2014. For two different remote support tasks, remote help and remote driving, the SAE's J3016 standard offered further definitions and clarification of words (SAE Levels of Driving AutomationTM Refined for Clarity and International Audience 2021).

Wang et al. (2020) discussed six levels of automation that SAE J3016 listed, ranging from zero to five. Level 0 has no automation, meaning all driving duties are carried out by drivers who have complete control over the vehicles. While there is driving assistance at Level 1, the human driver can employ support technologies to aid with steering, acceleration or deceleration but must always be prepared to do any driving duty at any time. These could include features like lane-keeping, cruise control and parking assistance systems. At Level 2 (partial driving automation), combined automated functions are used in the vehicle but the human driver is still responsible for monitoring the environment and controlling the driving process. This is because it is up to the human driver to recognise when to take back control from an active automation system, which regulates both steering and speed.

At Level 3 (conditional driving automation), if the vehicle alerts the human operator, they must be ready to drive the vehicle under specific circumstances. At Level 4 (high driving automation), the automation system is capable of driving autonomously under specific circumstances, thus the human driver is not required to maintain their attention on the road. Activating the automation systems in a secure manner might be left up to the driver. Finally, at Level 5 (full driving automation) the automation system may operate the vehicle autonomously in all circumstances. The only thing that has to be done by a human is to start the system and instruct it where to drive. The following table is derived from the automation levels table in (SAE Levels of Driving AutomationTM Refined for Clarity and International Audience 2021).

Table 2.1 The SAE Automation levels

LEVEL 0	The human driver has full control of the vehicle. The driver support features are limited to providing warning and momentary assistance. Example: automatic emergency braking. Blind spot warning. Lane departure warning.
LEVEL 1	The driver support features are engaged while the human is driving. These features provide steering or speed support to the driver. Example: Lane centring. Adaptive cruise control.
LEVEL 2	The driver support features are engaged while manual driving. These features provide steering and brake/ acceleration support to the driver. Example: Lane centring. Adaptive cruise control at the same time.
LEVEL 3	When the automated driving features request manual driving. These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met. Example: Traffic jam chauffeur.
LEVEL 4	These automated driving features will not require manual driving to take over driving. These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met. Example: Local driverless taxi Pedals/ steering wheel may or may not be installed
LEVEL 5	Manual driving will not be required because of automated driving features. This feature can drive the vehicle under all conditions. Example: Same as level 4, but the feature can drive everywhere in all conditions

2.2.5 Risk assessment

The process of conducting risk assessments involves identifying threats to the system, its vulnerabilities, potential negative effects if an adversary takes advantage of those weaknesses and the chance that those effects would materialise. The CAV system assets which comprise all the CAVs components and communications are subject to systematic threat modelling methodologies (Le and Maple 2019).

The three basic phases of risk assessment are risk identification, risk analysis and risk evaluation. Risk assessment is a component of overall iteratively and methodical risk management and serves as a benchmark for how far a technology has advanced (Lu 2021). In the new area of CAVs, there are several risk assessment approaches such as EVITA and Common Vulnerability Scoring System (CVSS) methods. One might use factors that are directly related to harm to stakeholders to quantify the effect of a threat. In automated risk models, four factors – safety, driver privacy, operational performance and financial losses of a vehicle – are frequently taken into account (Behfarnia and Eslami 2018).

2.3 Related work

2.3.1 Potential cyber risks in CAVs

In this section, possible attacks of CAVs have been listed and categorized from different literature (He et al. 2020) (Chow et al. 2021).

Table 2.2 The potential cyber risks

The assets category	The attack type	Description	Target	Severity level		Impact
				The information leakage	The physical damage	
ECU	Injection	Inject malware or misleading information to control the ECUs remotely or cause a data breach.	ECU	Medium	Medium	Making the vehicle make the wrong decision or lose control of vehicle function.
	Code modification	The attacker aims to modify the firmware in the ECUs that lack security settings.		Medium	Medium	Cause damage to the ECU or other components.
Sensors	Spoofing attack	Fabricating or replaying satellite signals, replaying laser pulses at a specific position or replaying digital radio signals to create an illusion that there is an obstacle or to make the vehicle take the wrong route.	GNSS, lidar, radar, camera	Medium	High	Causing fatal damage as the sensors get the wrong inputs and make the wrong decision. Location information and historic route information could be leakage.
	Jamming attack	The attackers would use noise or strong lights to decrease the quality of the inputs in the sensors.		Medium	Medium	Detection performance might be reduced and the physical damage could be serious.
	Blinding a camera	Disabling the camera.	camera	Low	low	This might not cause serious damage as it is easy to discover.

	Cloaking attack	This attack involves employing materials to absorb the reflected wave to override the reflected signals.	Radar, LiDAR	Low	Low	Failing to recognise the object
Audio entertainment devices	Malware attack	Due to the integration of the vehicle CAN and the entertainment system, an attacker might remotely control the car through the audio/entertainment system.	Audio devices, CAN	High	High	Take control of the vehicle and information leakage.
Intra-vehicular links	Eavesdropping	The attacker listens and collects sensitive information.	ECU, CAN bus	High	Low	Sensitive information leakage.
	Denial of Service (DoS) Attack	Flood the network and control node.		Low	Medium	Causes the target ECU to enter the error active state, which disables data receiving and sending and causes the CAN network to start its error management operations.
Inter-vehicular Links	DoS Attack	Huge amounts of data might be sent by the assailants to prevent the target vehicle's communication connection from receiving outside data.	V2V links	Low	Medium	Physical damage.
	Fake message	Attackers pretending to be a trusted vehicle send a message with fake position coordinates, speed or heading.		Medium	medium	The vehicle would take the wrong decisions.
	Change infrastructure sign	Infrastructure indicators such as road signs are altered.	V2I, sensors	Low	Medium	Severe traffic congestion or even traffic collisions.
	Cloud real-time traffic database	The attackers have access to the dataset and inject false or modified messages through V2X communication.	V2X	Medium	Medium	All the cars in the cloud database would receive inaccurate information.

The types of attacks on assets in AV are mentioned in (Chow et al. 2021) which is part of Autonomous and Connected Vehicles. The attack on each type of asset was studied, starting with ECU, sensors, and ending with internal communications, proposing the solutions taken from the latest recent studies specialized in each asset. On the other hand, (He et al. 2020) gathered numerous prospective cyberattacks on CAV and examined them from the viewpoints of the target assets, dangers, and outcomes A set of criteria were used to analyse the severity of each sort of assault as well as the severity of the attack was discussed then they suggested Mitigation methods. The attacks mentioned in the above table were collected from these two works of literature and it has been taken according to the similarity attribute. As the severity of attacks took from (He et al. 2020). It has been found that remote control by malware Attack, fake vision on cameras by spoofing attack, hidden objects to LiDAR and Radar by Cloaking Attack, and spoofing attack to GNSS are the riskiest and highly vulnerable aspects of CAV cyber security.

2.3.2 The risk assessment methods

Table 2.3 demonstrates the risk assessment methods discussed and compared by Lu (2021), Luo et al. (2021), Shevchenko et al. (2018) and Boudguiga et al. (2015). Different Threat Analysis and Risk Assessment (TARA) methodologies have been classified (Luo et al. 2021) to analyse and compared the current methods. TARA methods are divided into formula-based and model-based methods.

Table 2.3 The risk assessment methods

Method name	Category	Subcategory	Description	How it works	pros	Cons
STRIDE	Model base	Graph base	Used in identifying risk. STRIDE stands for spoofing, tampering, repudiation, information disclosure, DoS and elevation of privileges.	It is classifying the attack into similar categories.	Increases the effectiveness of identifying the threat as it is the best model to present the relationship between threats, assets and security attributes.	
Bayesian Defence Graph			An illustration of an attack and all routes that can lead to a countermeasure. With likelihood estimation, a Bayesian Defence Graph is supplemented further.	Forming a defence graph by defining the vulnerable components and setting defence techniques. Then performing threat identification and risk assessment based on the severity and likelihood of the threats. Bayesian network analysis is a graphical approach to probabilistic interference of relationships between the components and countermeasures. The functional linkages between the countermeasures' causes and effects are networked.	It might be proper to add it to EVITA and CVSS. The advantage of it is the quantitative analysis of threat risk.	
Attack Tree Analysis (ATA)		Tree base	Used in identifying risk. It could be described as tracing	The basis of the tree is the attacker's goal. The tree branches out to determine the attack	It is suitable for presenting the complex attack process.	It needs detailed knowledge of the system architecture; thus, it is not

			the attack path to specific assets.	functions and then finds the attack surfaces and entry points. After that determining the assets with the possible attacks and considering the attackers' capabilities. Only pathways with a likelihood of occurring should be included in the tree.		convenient for concept evaluation. However, it could be a hard task when dealing with massive system architecture and the level of the mistake is high.
CVSS	Formula-based	Vulnerability-based	Stands of Common Vulnerability Scoring System (CVSS). It is part of risk analysis which supports risk estimation and prioritisation.	It is based on access vector to the attack surface, access complexity required to perform the attack, confidentiality, integrity and availability impacts on attack successfulness and collateral damage potential.	The primary characteristics of vulnerabilities are captured by CVSS, which also produces scores—both numerical and textual—representing the severity of the vulnerabilities. It includes vulnerability priorities and an open framework.	
SARA		Attacker-based	SARA is a systematic threat analysis and risk assessment framework that consists of developing a threat model, modern attack methods, assets maps, attackers' trees and the late driving system observation indicators.	Start with a feature definition step which describes the defence boundary of the system. While, the threat specification step describes the SARA threat to security goal map, attack method to asset map and SARA attacker list definition. The last step in risk assessment is to return the risk value of an attack and then perform	It is an effective framework for Automated Driving System ADS and the automotive vehicle from Levels 0-4.	It is focused on safety more than on security. It is not proper with CAV.

				the SARA attack tree to form countermeasures to decrease the calculated risk from an attack tree.		
OCTAVE		Asset-based	Stands of operationally critical threat, asset and vulnerability evaluation.	Firstly, create asset-based threat profiles. Next, determine the vulnerability of the infrastructure. Lastly, create a security strategy and plan.	It is reproducible, adaptable and versatile.	Not made specifically to address CAV cybersecurity issues.
EVITA			Part of a European Commission-funded research project. It is the ideal risk assessment approach for the automotive industry.	Each asset in the system is subject to an attack assessment using the EVITA approach, which also determines the likelihood of an assault and the gravity of the damage it would do to determine threat priority. The network security objectives for the greatest risk threats can then be established.	It is proper for evaluation methods to discuss different aspects: operations, security, privacy and finance.	EVITA does not focus on other stakeholders. identifying all possible attack techniques virtually endless. only provides an evaluation method, not a complete evaluation process.
Threat, vulnerability and risk analysis (TVRA)			Models the likelihood and impact of attacks to determine assets and threats.	TVRA consist of assets inventory to assess the effect of harming an asset. The result would be a quantitative measure of asset risk to form security measures to reduce risk.	providing detailed analysis of threats.	Not describe attacks using trees. Only gives the steps to be performed not how to apply them.

Formula-based methods, which are categorised as asset-based methods, vulnerability-based methods or attacker-based methods, are techniques for TARA of the system that primarily uses tables, text or formulae. Model-based approaches, which are classified into graph-based and tree-based methods, are a type of threat analysis method that employs a range of models, modelling and assessing the threats and hazards of the system using data flow diagrams, graphs and tree models.

Lu (2021) categorised the risk assessment methods according to the safety and security aspects. Table 2.3 shows only the security methods that have been selected. STRIDE was used as part of the risk assessment process as it met the requirements of the automobile industry. Identifying the risk would increase the fidelity of determining the relationships between threats and assets based on security attributes. If the method focuses on the attack, it might use ATA. EVITA and SARA are frameworks that analyse and evaluate risk. SARA is more focused on the attack and attacker profile while EVITA works around assets. Both methods are formula-based which is more understandable and useful than model-based.

2.3.3 The simulating tools

Understanding the attack is key to overcoming the multidimensional danger of this linked technology that is quickly gaining popularity. Attack simulation aids in avoiding potential weaknesses.

Table 2.4 The existing tools

The practical solution	Source	General features	Security feature that it supports
TransModeler traffic simulation software	(Modelling Connected and Automated Vehicles. 2019)	Analyse the multifaceted nature and complexity of CAV. Simulate communication between V2V, V2I and V2X. Include the most advanced driver behaviour algorithms. A flexible and extensible application programming interface (API).	There is a lack of simulation cybersecurity incidents and security practices.
CARLA	(Team 2020)	It is an open-source simulator. It provides open digital assets (urban layouts, street signs, vehicles, buildings). A wide range of environmental conditions (time and weather). Supports setup of sensor suites and provides signals.	The prerequisites for modelling various cyberattacks are not satisfied by the current model. Maps and other essential navigational tools lack clarity. Furthermore, sensors and vehicles cannot be customised.

Simulators can perform certain types of attack, but will not cover all possible types. Most simulation tools focus on studying the mechanics of the vehicle and require simulation of the attack to be created outside the simulator and applied inside by a connection or programming interface. However, it might be difficult to study specific types of attacks on CAVs as they have two main functions – automation and communication – to simulate, which would be difficult as most simulators focus on the components of the vehicle and the environment. An attack on the network could affect the vehicle and would be difficult to simulate but it could be used in network simulators to simulate each node that is connected to the vehicle.

2.4 Summary

This chapter defined CAVs and their components and levels of automation. It compared the methods used in previous works and focused on security methods to study the potential risks and available simulating tools.

Chapter 3. Methodology

3.1 Overview

This chapter explains the methodology and methods used in this research. It first describes the research approach and then the steps taken to develop the method and the requirements and methodology for developing a risk assessment tool for CAV. Finally, it describes the preparation of the case study and validation process for the framework.

3.2 Research approach

The first part of this work focuses on the theoretical aspects and the current state of knowledge of the research, methodologies, standards, best practices and studies on the risk assessment for CAVs, AVs, Cooperative Automated Driving and V2I systems. The paper takes a qualitative approach. Cybersecurity and CAVs cover many fields of science fields including computer science, mechanical engineering, networking and IoT and required an exhaustive literature search to find the risk assessment method that can cover a variety of threats to CAVs. Scopus, ScienceDirect, IEEE Xplore, SpringerLink and Google Scholar were used as search engines.

The papers were selected based on the following criteria which focused on:

- Only Security.
- Relevance to risk assessment in CAVs.
- Related sectors such as AV, IT, connected vehicles and risk in the automotive industry.
- The Publishing date of 2014 to risks in CAV or later.
- No specified Publishing date for risk assessment on CAV and other domains related to it.
- Risk assessment methods and types associated with connected vehicles, CAVs and AVs.
- Papers that discuss the architecture of CAVs by assets and functions, and the risks and threats associated with them.

No comprehensive risk assessment method for CAV functions and their effect was found. There are studies on risk assessment but they focus on AVs or connected

vehicles. Other papers discuss a few attacks and risks on only parts of the CAV system which is closest to a comprehensive overview of risks in CAV. This work combines the strength of risk assessment methods from different domains to develop a risk assessment method that assists in improving the security of CAV's functions.

3.3 Developing the proposed method and tool

The first step in developing the methodology involved researching and selecting the literature using the previously described criteria and extracting the applied methodologies and their classification methods. Some of the applied methodologies follow safety and security standards, while others are limited to safety or security only. Therefore, the selected methodologies were limited to security only. Formula-based methods were selected from the TARA methods to perform the analysis and risk assessment. Two types were taken to develop the proposed method. The strengths of asset-based and attacker-based methods were combined.

The development of the prosed method depended on several criteria.

- Reproducibility of analysis results.
- Easy to understand and use.
- Flexibility in making inputs in terms of telematics and automation functions as CAVs consist of a variety of assets with diverse functions which are connected to other entities both inside and outside the vehicle.
- Diversity of stakeholders. The potential threats will not be limited to the passenger or vehicle owner but may be greater than that such as causing traffic chaos or showing defects of the vehicle or internal equipment to affect the reputation of the fleet owner or original equipment manufacturer (OEM).
- Limit the endless possibilities of threats and attack methods.
- Link security and threat attributes during threat analysis.
- How the factors of the risk assessment would align with CAVs attributes.

3.3.1 The risk assessments method

This project will be based on the risk assessment of critical functions in CAVs. The risk assessment process contains three steps (see Figure 3.1): identification of the threat, analysis of the potentiality and effect of the threat and evaluation of the risk.

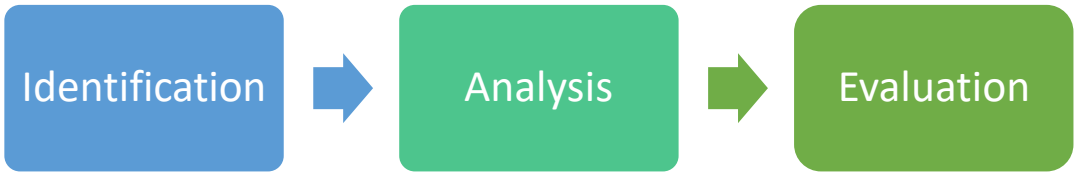

Figure 3.1. Risk assessment processes

This enables the reduction of potentially negative effects by addressing loss exposure and monitoring risk control by putting the basis for the level of acceptance of risk (see Chapter 4).

3.3.2 Developing the risk assessment tool

After the basics of the risk assessment methodology, the design of the tool will be presented using the Moscow methodology (see Section 4.4.1.1) prioritising the requirements, functions and features of the tool which will be a website accessed through a computer or smartphone.

3.4 Case study

After developing the risk assessment method and tool, a case study will show the effectiveness of the method by assessing two critical functions of CAVs which support the main functions: telematics and automation.

3.4.1 The first case

The over-the-air (OTA) software update is the first case to be studied as it may be affected by the telematics function. Here, the method's scalability is checked to assess external threats that may affect the vehicle's components to serve the attacker's goals. This function has been studied in earlier papers, but they did not focus on assessing the threats. Also, to study the outsider threat such as the threat that came from cloud repository.

3.4.2 The second case

The lane-keeping function was selected to verify that the method operates smoothly with threats of automation functionality that may be exclusive to the vehicle's internal components and the threats that occur on the road such as the compromise of lidar by jamming.

3.5 Summary

In this chapter, the methodology, research approach, criteria for choosing papers, the procedure for developing the risk assessment tool and selection of case study were discussed.

Chapter 4. Design and implementation

4.1 Overview

In this chapter, the suggested method will be discussed in detail and compared with previous methods to evaluate the threats to CAVs' functions and components. It will follow the risk assessment processes by identifying, analysing and evaluating the risk then try to find a structure to link the mitigation to the outputs of the assessment. Lastly, it will develop a website that could help experts to implement the method easily and accurately.

4.2 Novelty and the state of the art

This method aims to identify the vital functions of the CAV, the assets associated with each function and the risks arising from potential threats and their effects on each asset. The proposed method was derived by combining the strengths of recent methods that have contributed greatly to the modelling of automotive threats. It uses a variety of criteria extracted from previous methodologies with the addition of some modifications to suit the characteristics of CAV.

Determining the function will indicate how assets interact and the extent to which the use of assets differs from one function to another. Earlier research has relied on assets and threats as the target of the assessment. Defining the physical and logical boundaries of the function helps to identify the assets affected by the attack and distinguish between internal and external threats through the classification of these assets. The idea of classifying assets is taken from the SARA method (Monteuuis et al. 2018) but classification types and use are different. In this method, assets are categorised for use with their threat model and the use of categorising determines whether the threat is inside or outside.

The EVITA method (Henniger et al. 2009) was chosen as the basis for the attack potentiality factors that it shares with the RACE (risk analysis for cooperative engines) and TVRA methods (Boudguiga et al. 2015) of time, experience, knowledge, opportunity and equipment. However, in the proposed method the method of calculating the attack potentiality was derived from SARA which Monteuuis et al. (2018) explained as where the attack potential was calculated by determining the capability of the attacker. This is made up of three factors: knowledge, experience and equipment. Attack potential is calculated by combining

the attacker's capability, the window of opportunity and elapsed time. SARA was used to determine the type and characteristics of a potential attacker and to calculate their capability as a metric to calculate an attack potential. While the values and levels of factors were taken from the EVITA method (Henniger et al. 2009) and linked to the attack likelihood shown in SARA, where a higher probability means a lower likelihood. In this method, the values of the attack likelihood levels were changed from 1 - 5 to 0 - 4 to match the values of the effect levels.

The effects of the attack were taken from Islam et al. (2016) and categorised into four groups: safety, privacy, financial and operational. This is taken from the ISO 26262 standard. This classification follows the severity of the attack described in the RCAE, EVITA and TVRA methods. A control parameter was used to measure the severity of the attack, which shows the extent to which the driver is in control of a vehicle, although not on driverless vehicles. In the SARA method, a new factor was developed: observation. This divides the control into automated driving control and human control to avoid accidents. In this method, the effect of the attack is calculated without addressing the control factor, as the threats associated with the CAVs go beyond attacks on the driving path to attacks on the communications between the objects surrounding the vehicle; for example, the effect of an attack on OTA updates is different from the effect on emergency brakes. Therefore, the evaluation method takes into account the effects on stakeholders, objects (pedestrians, other vehicles and infrastructure) and associated backend systems and not on the driver as in previous risk assessment methods as the connected and autonomous vehicle transcends the function of moving on the road to providing communication and exchanging information with all the elements surrounding the vehicle.

The risk calculation was done from the two factors of likelihood and effect. The risk matrix was quoted from Islam et al. (2016) to match it to the factors used in this method. At the end of the evaluation process, mitigation methods are suggested based on the evaluation results.

4.3 Risk assessment based on CAVs functions

Despite the advantages offered by communications in CAVs and enabling data transfer with other entities associated with the vehicle, the increasing number of

independent and connected functions might make CAVs vulnerable to more cyber security threats that may disable them from performing their duties. Categorising these threats into a single target such as disabling a specific feature of a connected vehicle makes them measurable and restricts the target to one area. In this method, one of the functions of the connected and autonomous vehicle is determined to study the risks to evaluate and link the assets that perform a specific task rather than studying the threats to all assets. Study of the function enables us to raise its effectiveness and determine the security requirements necessary for it to raise the efficiency of the vehicle in general. Prioritising the extent of the interconnectedness of assets makes forecasting threats and damage more accurate, more organised and clearer to the security expert. The method suggested in this project helps security experts to focus on studying the threats to these functions by determining the purpose of the attacks and the damage that follows. The risk assessment focuses on the functions targeted by the attackers, the classification of potential threats in each function in line with the threat model and the types of potential attackers for each threat to raise the efficiency of this function and achieve its security requirements. It includes two paths of functions – communication and automation – each of which covers critical functions in a CAV. Risk assessment is divided into three processes: identification, analysis and evaluation of risk. The first step is to determine which function is under attack and the assets associated with that function and then identifying the threats to the selected function using the STRIDE model. After that, risk analysis is performed to calculate the probability and effect of the attack. Finally, in the risk evaluation process, the risk score is calculated according to the risk matrix and the countermeasures to these risks and mitigation methods determined.

4.3.1 Physical and logical architecture of CAVs

To accurately determine the functions of a CAV, a security expert must be familiar with the vehicle's structure and characteristics. The focus of the architecture in this project will be on aspects of the design necessary to sense the environment and the vehicle's position within it. Each module transforms raw data collected from multiple sensors into information useful to the decision-making software. CAVs are based on modern physical and logical connected components including ECUs, sensors and

actuators and to the vehicle's V2X connection which provides and exchanges information in real-time (see Figure 4-1).

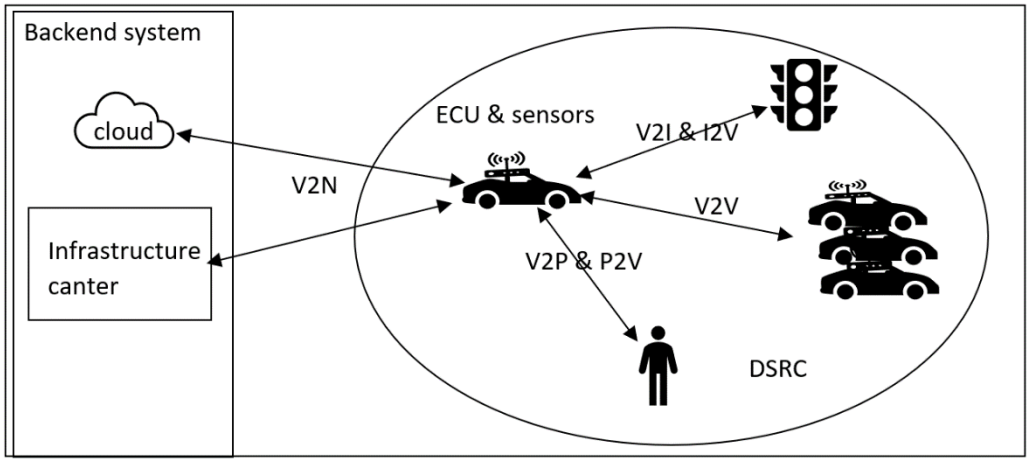

Figure 4.1. CAV Architecture

4.3.2 Risk identification

Before determining the threat to function, the boundaries of that function must first be defined by making a list of critical affected assets based on their roles and how they interact with each other, then identifying a list of possible threats that are relevant to those assets. Each threat will be described in terms of a threat agent, an asset and an attack method (Dominic et al. 2016). The output from this process is used in the risk analysis process once all threats methods have been identified.

4.3.2.1 Asset category

This paper divided CAVs components into six main groups:

- In-vehicle components including sensors, ECUs, actuators and software.
- Intra-vehicular links such as CAN and FlexRay.
- Inter-vehicular communication links such as V2V, V2I and V2P.
- Supporting digital infrastructure such as cloud servers, remote repositories.
- Stakeholders such as the OEM, suppliers and fleet owners.
- Consumers.

Table 4-1 shows examples of critical assets that could affect the risk assessment of CAVs.

Table 4.1 Critical assets and their category

Asset name	Asset category
Electronic control units	In-vehicle component
LiDAR	In-vehicle component
Dedicated short-range communication	Inter-vehicular communication links
CAN buses	Intra-vehicular links
GPS	In-vehicle component
Cameras	In-vehicle component
Radar	In-vehicle component
Flexray	Intra-vehicular links
Bluetooth	Intra-vehicular links
VANET	Inter-vehicular communication links

4.3.2.2 Mapping Assets category to threat classification

Threats can be categorised into internal and external based on how the components of the function are connected to the external environment and how easily the attacker can access them. Classifying the threat as external or internal will not fundamentally affect the risk assessment but will help the expert to understand the threat and better study its effect.

If the data package sent between the vehicle and the software repository contains malicious programmes that have been modified, which is classified as a supporting digital infrastructure, it is an outside threat which will make the expert consider the method of access to the vehicle, physical or remote. If the effect includes the vehicle only, the attacker must have physical access to the vehicle and so the probability of attack is low and the effect is limited to that vehicle and its passengers. To classify the threat, it is necessary to take into account the common and important components affected. For outside threats, the number of vehicles targeted and the interaction of the function with the environment are taken into account. Does the density of vehicles impact the threat to the function, for example, sharing of data.

Some assets may determine the classification, internal or external, but the expert must decide if the threat is inside or outside. Table 4.2 classifies the asset categories based on threat type.

Table 4.2 Classify the assets categories based on threat type

The assets category	Threat classification
In-vehicle component. Intra-vehicular links component Consumers	Inside threat
Inter-vehicular communication links component Supporting digital infrastructure the stakeholders	Outside threat

4.3.2.3 attack method

In the area of vehicle information security, the STRIDE method is recommended by the SAE J3061 regulations (Luo et al. 2021). The acronym indicates the six threat categories used and it is used to categorise and define attacks into classes. Table 4-3 summarises attack methods according to the STRIDE model and shows a static mapping of the threats categories to security attributes.

Table 4.3 Microsoft's STRIDE methodology

Threat	Explanation	Security attributes
Spoofing	A legitimate vehicle is impersonated by the attackers and/or fake information is spread. pretend to be somebody or something different.	Authenticity
Tampering	The attacker modifies data or functions when the messages exchanged between vehicles, sensors data and electronic control unit's firmware are being altered.	Integrity
Repudiation	A repudiation occurred when a vehicle begins to falsely deny having carried out a certain activity or having been a part of a certain incident. Attackers commit acts that cannot be linked to them.	Non-repudiation
Information disclosure	Unauthorised access is gained by an attacker to sensitive information or traded communications, allowing them to obtain confidential data.	Confidentiality/Privacy
DoS	Attackers interrupt a system's legitimate operation, such as the gathering of sensor data or the timely transmission of messages.	Availability
Elevation of privilege	Attackers perform unauthorised actions such as sending the navigation system the wrong orders and gaining unprivileged access to the vital systems of the car.	Authorisation

4.3.3 Risk analysis

After the risk identification step is completed, the next step is measuring these risks and determining the relationship between the probability of an attack and it effect. This is the result of combining the SARA and EVITA methods (Monteuuis et al. 2018; Henniger et al. 2009) with a new visual representation of the risk matrix and other factors.

4.3.3.1 Attack likelihood

The attacker plays an important role in calculating the potentiality of the attack by determining the attacker's knowledge of the target, the level of experience and the equipment required to identify or exploit vulnerabilities. While the other parameters that could contribute to calculating the potential of attack are time elapsed and window of opportunity.

Threat agents

One of the first steps in risk assessment after identifying threats and affected assets is identifying the threat agents and their goals. The attacker’s methods and motivation could also be defined to help calculate the attacker’s potential capabilities. The following types of potential threat agents are related to the CAVs environment some of which have been identified by McCall et al. (2021).

- Security researchers

These are experts who use their technical knowledge to identify vulnerabilities and are recruited through bug bounty programmes to find system vulnerabilities. Many researchers prefer to share discovered vulnerabilities through social media or at large gatherings such as conferences. This threat lies in sharing information freely, which makes cybercriminals look for public information about vulnerabilities that help them to exploit or take advantage of in other attacks.

- Hacktivists

In this category, individuals or groups use their hacking capabilities to present ideas for political or social purposes to disrupt businesses and target individuals to obtain

media coverage and public attention. Hacktivists often engage in fraud, identity theft and DoS activities.

- Thieves

Individuals in this group focus on activities associated with theft for personal financial gain. Thieves usually tend to engage in DoS activities, circumvention and system intrusion.

- Organised crime

This group has a great deal of resourcefulness and sophistication and is financially motivated. Attackers may attempt to use reverse engineering to damage the reputation of their competitors or use parts of it for their products. The attacker aims to open backdoors and grow their botnets in addition to using ransomware attacks or stealing sensitive data and using it to blackmail or sell it in underground markets.

- Terrorists

The attacker in this category aims to arouse widespread fear among the people and cause general disturbance to support personal socio-political causes. They focus on getting wide news coverage by using reverse engineering, data mining techniques and tools to carry out the attack.

- Advanced Persistent Threats (APT)

These groups are supported by governments to carry out espionage and attacks. The national infrastructure of competing countries is targeted by their attacks. This category often uses advanced threat methods such as malware, phishing attacks and zero-day attacks.

- Owners

The owners of CAVs hack their vehicles to remove manufacturer-implemented restrictions to enhance performance, such as increasing engine power.

Attacker capabilities

Determining the attacker's capability (C_a) could enhance the process of discovering their style and character to conduct the attack and achieve its objectives and

influence the likelihood of occurrence. Monteuuis et al. (2018) demonstrate that the calculation of the capability of an attacker depends on multiple standardised factors:

- Knowledge of the target (K_t) refers to the sources that attackers can use to learn more about the target and describes how challenging it is for an attacker to do so. It could be public, restricted, sensitive or critical.
- Expertise (E_x) refers to the level of general knowledge of the fundamental principles necessary to perform an attack. The identified levels are: laymen, proficient, expert or multiple experts.
- Equipment (E_q): refers to the IT hardware, software or other equipment that is needed to identify and exploit the target: standard, specialised, bespoke or multiple bespoke.

Capability is calculated as follows (Monteuuis et al. 2018):

$$C_a = K_t + E_x + E_q$$

The SARA method also bases its attacker capability calculation on common factors which will be used in this project. These factors have four levels with an associated value (Henniger et al. 2009), as shown in Table 4-4.

Table 4.4 Attacker capability values

Factor	Level	Description	Value
Knowledge of target (K_t)	Public	The necessary information is public.	0
	Restricted	The information is shared with partners under non-disclosure agreements.	3
	Sensitive	Constrained access to information between shared members.	7
	Critical	Access to information is tightly controlled on a strict need-to-know basis.	11
Expertise (E_x)	Layman	No particular expertise is required.	0
	Proficient	Basic security knowledge is required.	3
	Expert	Has a strong security background in this field and knows techniques and tools of existing attacks and can create new attacks.	6

	Multiple experts	Security and domain knowledge is required for several distinct domains to launch simultaneous attacks to achieve their attack goal.	8
Equipment (E_q)	Standard	The equipment is readily obtained or available for the attacker.	0
	Specialised	The equipment could be acquired without effort that could be ordered from a specialised shop.	4
	Bespoke	Not easy to purchase and is expensive to create as may need to be specially produced or the equipment's distribution is likely constrained and even limited because it is so specialised.	7
	Multiple bespoke	Equipment where different types of bespoke equipment are required for distinct steps of an attack.	9

Table 4-5 lists examples of a collection of threat agents along with their profiles and capabilities but it could be changed according to the threat event. The goals and skillsets attributed to each attacker might vary depending on the assumptions made. Some threat agent profiles have been taken from Monteuuis et al. (2018) and Dominic et al. (2016).

Table 4.5 The models of threat agents

Threat agent	Motivation	Expertise	Knowledge of the system	Equipment	Capability
Thief	Financial	Layman (0)	Public (0)	Standard (0)	0
Organised Crime	Financial	Proficient (3)	Restricted (3)	Bespoke (7)	13
Mechanic	Financial	Expert (6)	Critical (11)	Specialised (4)	21
Hacktivist	Ideology, Passion	Multiple Experts (8)	Sensitive (7)	Multiple Bespoke (9)	24
Terrorist	Ideology	Proficient (3)	Restricted (3)	Standard (0)	6
APT	Financial, Ideology	Multiple Experts (8)	Restricted (3)	Multiple Bespoke (9)	20

Attack potentiality

The attack potentiality is calculated as a product of the attacker's capabilities, the elapsed time (E_t) and the window of opportunity (W_o) which refers to the access type available to the attacker. The elapsed time is the time taken by the attacker to identify the vulnerability and launch the attack and achieve it successfully considering the attacker's ability. It depends on the skill level of the attacker and the availability of equipment required to launch the attack and their ability to use that equipment. The level of equipment used and attacker expertise may not correlate.

These parameters could change over time as they focus on the attacker and the detection of new vulnerabilities and the development of attack tools change the whole estimation. The worst-case scenario is used to calculate the necessary length of time when taking this element into account. The worst-case scenario is used to calculate the necessary length of time when taking this element into account. Table 4-6 shows the value of the window of opportunity and elapsed time (Henniger et al. 2009).

Table 4.6 Window opportunity and elapsed time values

Factor	level	Description	Value
Window of opportunity (W_o)	Unnecessary/unlimited	Physical and network accessibility are boundless for an infinite amount of time, therefore the attack does not require any kind of opportunity to be carried out.	0
	Easy	Accessibility is high physically and remotely with some time restrictions.	1
	Moderate	Accessibility is restricted physically or remotely to the vehicle interior or exterior without using any special tools and with severe time limitations.	4
	Difficult	Physical access is needed to carry out intricate disassembles of vehicle components to access internals and mount an attack on the asset.	10
Elapsed time (E_t)	≤ 1 day	Less than one day.	0
	≤ 1 week	Between one day and one week.	1
	≤ 1 month	Between one week and one month.	4
	≤ 3 months	Between one and three months.	10
	≤ 6 months	Between three and six months.	17
	> 6 months	More than 6 months.	19

Monteuuis et al. (2018) followed the form below to calculate attack potentiality which will be applied in this method:

$$P_a = C_a + E_t + W_o$$

Finding attack likelihood

According to the SARA method, the likelihood of an attack is related to its potentiality. The lowest potentiality is more likely to occur as shown in Table 4-7 below.

Table 4.7 Mapping attack potentially and attack likelihood

Attack potentiality (P_a)		Attack likelihood (A_l)	
Pa	Description	Description	A_l
0–9	Basic	Highly likely	4
10-13	Enhanced basic	Likely	3
14-19	Moderate	Possible	2
20-24	High	Unlikely	1
≥ 25	Beyond high	Remote	0

4.3.3.2 Attack impact

The new feature suggested in this framework is to add the target factor affected by the attack, whether it is a vehicle, infrastructure, backend system or other assets category. The CAVs risk assessment is not limited to the vehicle component but includes all parties connected to the vehicle that may be affected by the attack. Where the attack on one of the sensors may affect the vehicle, but also other vehicles and connected objects around it. That will be greatest on the surroundings, but will not significantly affect the backend systems.

Determining the risk involves calculating the effect level of a potential attack and includes an estimate of the expected loss for the various stakeholders and objects. Four criteria were identified by Islam et al. (2016): safety, privacy, financial and operational. The four levels set are: none, low, medium and high (see Table 4-8). The SARA method determines the severity of the attack through the level of human control but in this thesis, the focus will be on level 5 automation. So, the automation feature would work instead of human reaction and CAVs have several functions that do not include driving tasks which could be affected by an attack which could by data flooding and communication. As a result, this paper will focus on the effect of the threat without considering the control factor following a formula taken from Islam et al. (2016):

$$I_m = 10\ (S_a + F_i) + O_p + P_r$$

To calculate weightings for each value. Given that the operational and privacy effects are low, Islam et al. argue that the privacy and operational should be weighted at 1, while the safety and financial weights should be 10, due to their effect on the body of the vehicle and objects that surround the vehicle and stakeholders (see Table 4.8).

Table 4.8 Impact parameter values

Impact category	Description		Value
Safety (S_a)	No injuries	None	0
	Light and moderate injuries.	Low	1
	Life-threatening injuries with probable chance of survival.	Medium	10
	Injuries that are fatal or life-threatening with a low chance of survival.	High	100
Operational (O_p)	No discernible effects.	None	0
	Comfort affected, the vehicle can be used with some restrictions. Between 25% and 75% of customers are annoyed by an item's appearance or an audible noise.	Low	1
	An important function is affected, the degradation or loss of a secondary or primary function.	Medium	10
	One or more fundamental functions are affected which make the vehicle use is infeasible and potentially affects safety or legislative aspects.	High	100
Financial (F_i)	No impact or financial damage for the stakeholders and objects.	None	0
	The financial damage remains tolerable for the stakeholders and objects.	Low	1
	Substantial financial damage, but do not threaten the existence of the stakeholders and objects.	Medium	10
	Existence-threatening financial damage of the stakeholders and objects.	High	100
Privacy (P_r)	No unauthorised access to data	None	0
	Anonymous data only (no specific driver of vehicle data).	Low	1
	Identification of vehicle or driver; anonymous data for multiple vehicles.	Medium	10
	Driver or vehicle tracking; identification of driver or vehicle for multiple vehicles.	High	100

Table 4.9 shows the value of the impact calculation and the level of impact.

Table 4.9 Impact Values

Parameter Sum	Impact Level	Value
0	None	0
1-19	Low	1
20-99	Medium	2
100-999	High	3
≥1000	Critical	4

4.3.4 Risk evaluation

Table 4.10 shows the risk matrix derived from Islam et al. (2016). The risk evaluation is derived by integrating this information. Table 4-11 shows the attack likelihood, the effect of the attack and the corresponding classification of risk which is calculated by multiplying the attack likelihood (Section 4.3.3.1) by the result of the attack (Section 4.3.3.2). The risks are categorised as shown in Table 4-12 and sorted into five levels: QM, low, medium, high and critical here QM is Quality Management. The colours represent each category: red for critical risk, orange for high, yellow for medium, green for low and blue for QM.

Table 4.10 Risk matrix

	Attack impact					
Attack likelihood		0	1	2	3	4
	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

Table 4.11 Risk Values

Risk value	Risk level
0	QM
[1-3]	Low
[4-6]	Medium
[8-12]	High
≥16	Critical

Since the level of risk is critical if both the effect and the likelihood are equal to 4, the highest priority is given if it is exploited to reduce it to the minimum. Based on the risk level, the level security requirements are formulated (Islam et al. 2016). QM refers to quality management and is derived from the ISO26262 standard as mentioned in (Islam et al. 2016). Where there is no need for special controls to reduce risks, no security requirements will be formulated and approved quality procedures are satisfied. Using QM instead of none, helps the expert to put the correct classification of the risk because there may be a possibility of attack or some impact that could be medium or low. Therefore, placing it under none makes the evaluation of this type of attack negligent.

While it could be different in the case the value of attack impact or attack likelihood are (0,4) or (4,0), in this case the level of risk will be Low and need to formulate some security requirement. As one of these factors takes the highest value in the classification, while the other has the lowest value, which is zero, so it created an anomaly in the formula for calculating the degree of risk, because of the high value in one of them, which increases the possibility of occurrence or that its impact is high. The formula for the calculation is derived from the TVRA method (Moalla et al. 2012):

$$\text{Risk} = \text{Likelihood } (A_i) \times \text{Impact } (I_m)$$

The cases where one of the factors is zero and the other 4 should, following this equation, result in a risk of zero, prudence suggests that some measures be put in place.

Table 4.12 Description of the level of risk

The level of risk	Description
Critical	The likelihood of the threat occurring is critical due to the availability of capability and opportunities and it is expected that the threat event will have many severe or catastrophic negative effects on the function of the vehicle.
High	The average of likelihood of the threat occurring is major and the threat event might be expected to have severe or catastrophic adverse effects on the vehicle function.
Medium	The average of likelihood of the threat occurring is moderate and the threat event could be expected to have moderate to severe or adverse effects on the vehicle function.
Low	The average of likelihood of the threat occurring is minor and the threat event could be expected to have minor adverse effects on the vehicle function.
QM	The average of likelihood of the threat occurring is far and threat event could be expected to have a minor impact on the vehicle function.

When all potential risks to the function have been assessed, the levels of risk can be represented using a line chart. The purpose is to visually express the levels of risks associated in the function for each threat and represent the data in a consistent and attractive way.

4.3.4.1 The proposed mitigation method

Mitigation methods are proposed based on the results of the risk assessment and depend on the level of risk. They are similar and can be grouped into five categories based on specific CAVs characteristics (He et al. 2020) but updated to link them to

risk level. Table 4-13 defines the mitigation methods and the link to risk level is shown in Table 4-14.

Table 4.13 The description of mitigation methods

The mitigation method	Description
Acceptance	Keeping risks that cause limited negative effects on the function, where the task can be performed without affecting the rest of the tasks in the function, or that the possibility of its occurrence is excluded and does not require countermeasures.
Transference	Sharing the potential with trusted third parties such as insurance companies and others. Since the risk is of medium probability and may result in unacceptable effects that may affect the parties involved in this function, the solution lay in sharing the risk to setting controls.
Contingency	Prepare potential reactions in the event of attacks by preparing a contingency plan in advance to restore functionality and reduce risk.
Reduction	Reducing the attack probability or effects by providing the CAVs with more controls and solutions for the attacks to reduce them to a manageable level; for example, placing redundant sensors to increase the reliability of the data entered by the sensors.
Prevention	The prevention of attacks could be through the use of solutions that prevent the attack methods from negatively affecting the entire functionality such as the use of a secure communication channel and encryption of the messages.

Table 4.14 Mapping the level of risk and the mitigation methods

The level of risk	The mitigation method
QM	Acceptance
Low	Transference
Medium	Contingency
High	Reduction
Critical	Prevention

4.3.4.2 The counter measurements

The last step will be countermeasures which could set some controls according to the level of risks and the mitigation method. A countermeasure would address the whole function and not be limited to a single threat. It would increase the effectiveness and performance of the function and enhance security. This would have two steps: determining the security requirements of the function and then identifying a solution.

4.4 Developing the risk assessment tool

This section proposes a tool that will implement the proposed method described above. It is web-based and can be accessed using a computer or smartphone and is

intended for security experts and CAV researchers. The website would help many stakeholders understand and prepare their plans for operating CAVs on the roads. Moscow method has been used in order to setting the requirements.

4.4.1 The tool requirements

4.4.1.1 Moscow method

Some functional and non-functional requirements are needed to support the features of the website. The functional requirements could be categorised using the Moscow method which was used to set the requirements. Under the method, the tool:

Must

- Implement the risk assessment process.

The tool must implement the risk assessment process on the function through identifying threats, analysing threats and the evaluating the risk that depends on the proposed method.

- Be accurate and repeatable.

The result of risk assessment must be accurate and the calculation must follow the proposed formula. If the user repeats the process, the same result must occur.

Should

- Determine the critical assets.

The tool should determine the critical assets that could be infected by the threat, the attacker types and capability, the potentiality of threat and its effect.

Could

- Present risk level.

The tool could present the risk levels for the threats which could be line chart.

- Be easy to use.

The website is not difficult to understand and it interacts with user input. The site requests data sequentially and logically so that the user can track the data smoothly.

- Return to previous reports.

The user can view the previous reports and works that could help compare the latest threats and previous work. If the function has been updated with new technology, the user can also review the assets of the new and old versions.

- The user can download and print the report.

Won't

- calculate unlimited threats for a single function.

The tool will not have unlimited threat identification for one function. Each function could present approximately 8 threats.

- Determine the sub-function.

The function could have subfunctions which will not be mentioned.

4.4.2 The design of the tool

In designing the website, we used the following:

- PHP, HTML, JavaScript, CSS, MySQL and Vue.js.
- The bootstrap library, Appexchart library and Jquery.
- Xmapp for the Apache HTTP Server and MariaDB database.
- A database.

Figure 4-2 shows the landing page for the user. Here the user can review the older works and could add new work.

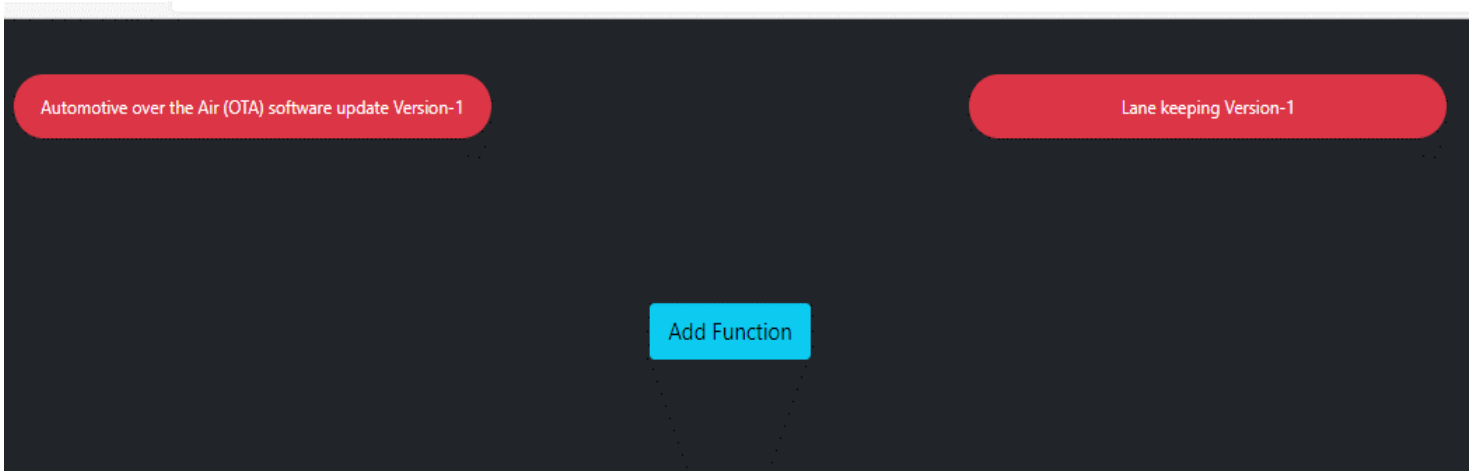

Figure 4.2 The first page of the website

The next page would be the first input for the risk assessment process, as the user will write the name of the function and determine the assets and threat number associated with the function.

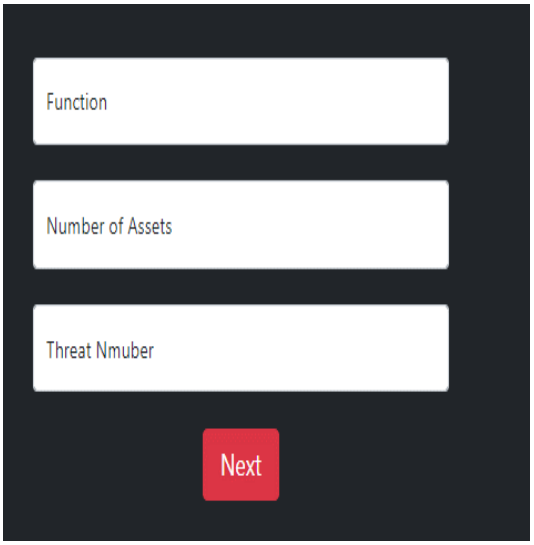

Figure 4.3 The starting new risk assessment page

After that, the user will write the assets and threat name and choose their category.

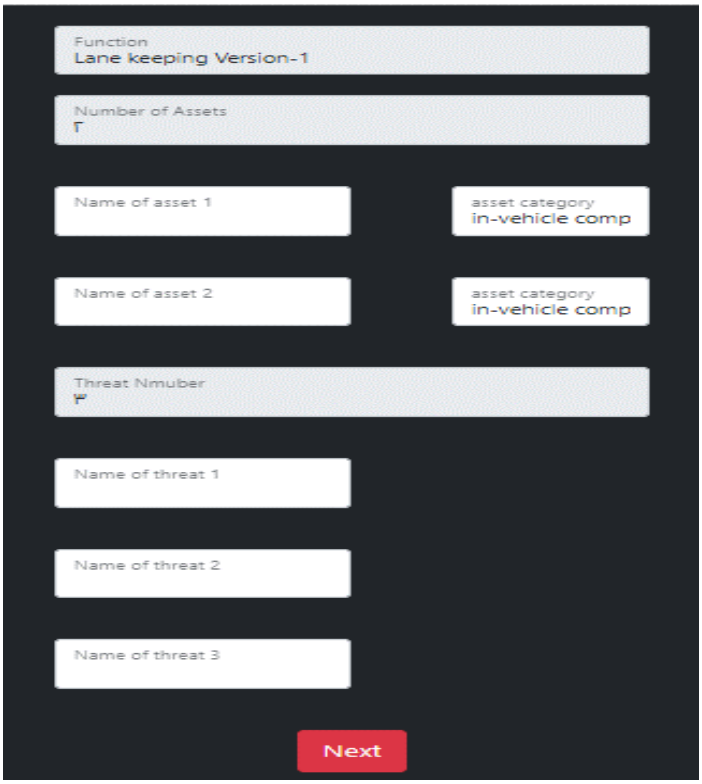

Figure 4.4 The assets and threat identification page

Then the user will input threat data (attack goal, threat agent information, the estimated impacts) for each threat and the tool will calculate attacker capability, attack potentiality, attack likelihood and attack impact.

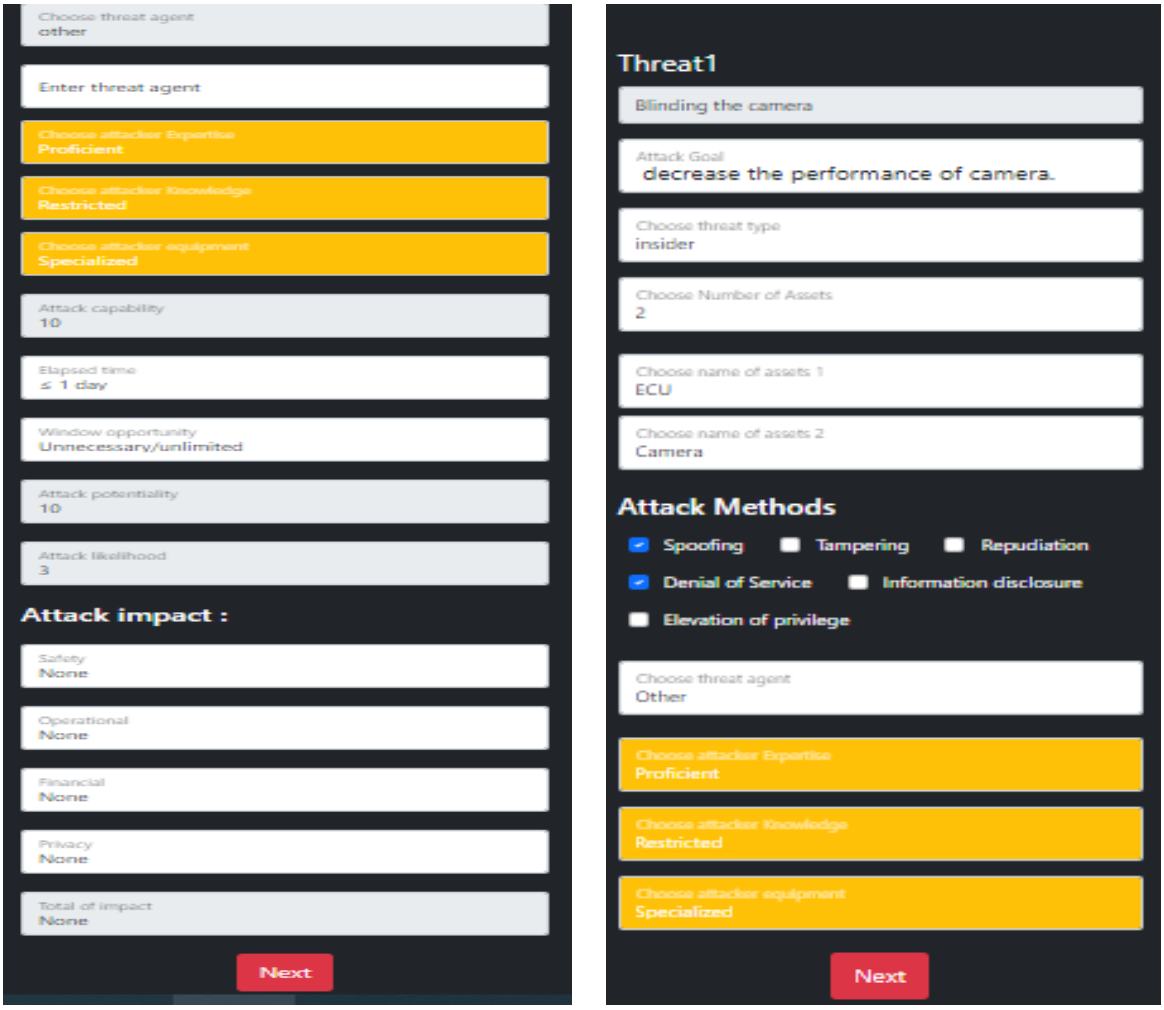

Figure 4.5 Threat analysing pages

The last page presents the full report about the function threat with the information in a table and shows the most affected threat on this function. The level of risk could be present in a line chart for all threats in that function. The user can download this page or print it.

Risk assessment report :

Function name : Lane keeping Version-2

Number of Threat : 3

	Jamming attack	Spoofing attack on sensors	Spoofing attack on V2V
the number of affected assets :	4	3	2
the threat category :	insider	insider	insider
the threat agent :	Researcher, Hacktivism	Researcher, Hacktivism	Hacktivism, Terrorist
the attack goal :	Decreasing the performance of sensors.	False detection leading to corresponding reactions.	Affecting decision making to changing vehicle direction.
Attack method :	denial of service	spoofing tampering denial of service	spoofing tampering information disclosure
Security attributes target :	Availability	Authenticity Integrity Availability	Authenticity Integrity Confidentiality/Privacy
the likelihood:	Highly Likely	Highly Likely	Unlikely
the impact of attack:	High	High	Low
the estimated risk :	High	High	Low
the mitigation method :	Reduction	Reduction	Transference

Table 4.15 The risk assessment output

Table 4.16 The line chart representation

4.5 Summary

This chapter laid the foundation of the proposed methodology that combines the strength of the SARA and EVITA methods to evaluate the functions of CAVs as it is difficult to enumerate all threats and attack methods on CAV assets, and those assets are constantly being developed along with their surrounding technologies. The last part of the chapter displayed the features of the developed website.

Chapter 5. Findings and evaluation

This chapter demonstrates the risk assessment method described in Chapter 4 in two case studies then discusses the effectiveness of the methodology and the tool.

5.1 Risk assessment implementation and evaluation for CAV

The method proposed in Chapter 4 is applied to two vital functions: automotive OTA software updates and lane-keeping. The risk assessment will determine the function boundaries, potential threats, threat agents and likelihood of attack success and evaluate the effect of the attack to conclude the value of the risk and apply the mitigation methods mentioned in Chapter 4.

5.1.1 OTA software updates

The security and safety of CAV are being compromised by the numerous methods that might be targeted the OTA software updates by hackers which could have impact on the on-demand software lifecycle such as repository, distribution, and installation which are often inadequately protected, leading to substantial damage. The remote control of the infotainment system of moving vehicles, engine, steering and braking could happen after the attacker manipulated the software and installs malicious versions of firmware which might cause a fatal effect on objects surrounding the vehicle. The critical assets that could be affected by these attacks include backend servers, remote repositories, wireless networks, ECUs and software packages (Park and Park 2022). ECUs are quite diverse in processing speed, memory capacity and security features. The remote software repository is provided by the OEM which hosts software update files that are produced by both the supplier and the OEM (Karthik et al. 2016). The agents download the latest software to the remote repository in the form of images and metadata and from there to the ECU where the process is done by publishing updates on vehicles via wireless communication or through physical distribution channels, but our focus is on updates via wireless communication. Karthik et al. (2016) assumed that all software in the repository is arranged by image and each contains all the files required to run an application on an ECU. Table 5-1 contains the asset names and categories.

Table 5.1 OTA software updates function assets

Asset name	Assets category
Remote repositories	Backend system
Wireless networks	Inter-vehicular communication links
ECU	In-vehicle component
Software packages	Software Components

After understanding the function and defining its boundaries, threats are the first step in the risk assessment (see Table 5-2). Four targets were identified by Karthik et al. (2016): reading updates, denial of service, denial of functionality and control. Each of these targets has several attacks, some of which are mentioned in this paper. For each threat, the threat agent, the attack goal, the attack surface and the threat method are defined, in addition to a simplified description of the attack. The attack likelihood for each threat is determined by calculating the attack potentiality through the attacker's capability, window of opportunity and elapsed time as described in Chapter 4. The effect of the attack is calculated for each threat by setting the safety, privacy, financial and operational levels. Table 5-2 shows the risk assessment process.

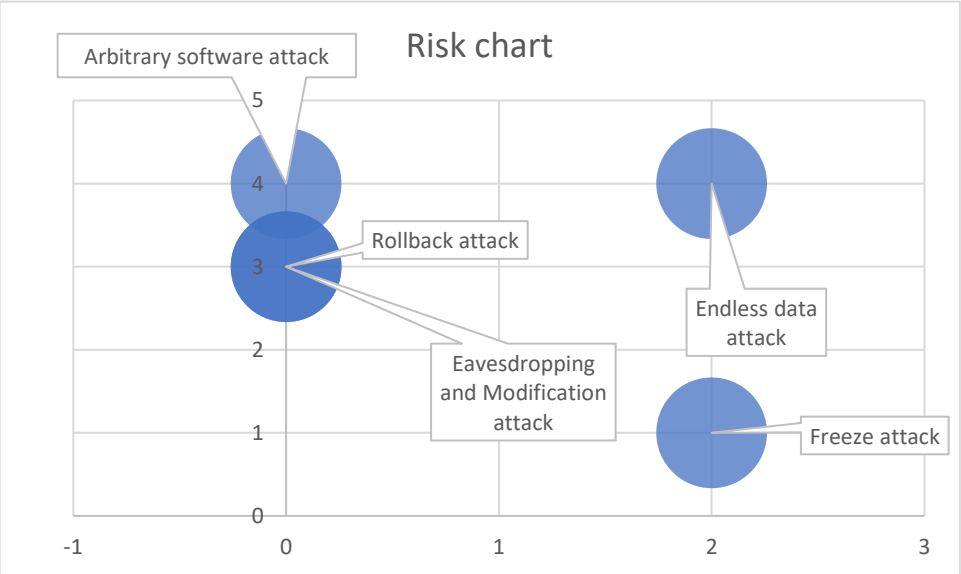

Figure 5.1 OTA software updates risk chart

Table 5.2 Risk assessment for OTA software updates function

The threats	Eavesdropping and Modification attack	Endless data attack	Arbitrary software attack	Freeze attack	Rollback attack
Attack goal	Attackers are interested in the contents of software updates to reverse-engineer ECU firmware.	Attackers would like to cause vehicles to fail.	Attackers can cause an ECU to install software of the attacker's choosing. This means that the attacker can arbitrarily modify the vehicle's performance.	Attackers want to prevent vehicles from fixing software problems by denying access to updates.	Attackers try to stop ECUs from functioning correctly, thus causing the vehicle or a component to fail or behave abnormally, either temporarily or permanently.
Threat type	Outside threat	Outside threat	Outside threat	Outside threat	Outside threat
Threat agent	Hacktivist, organised crime	Terrorist, organised crime	Hacktivist	Organised Crime	Organised Crime
Attack Surface	ECU, software packages, wireless network	The remote repository, ECU	ECU, software package	ECU, software packages, remote repositories	ECU, software packages
Attack Method	Information disclosure, Elevation of privilege, tampering	Tampering, denial of services	Tampering, Information disclosure, Elevation of privilege	Tampering, Information disclosure, denial of services	Tampering, denial of services
Description	Attackers can read unencrypted updates sent from the repository to the vehicles and modify them.	Causes an ECU to crash by sending it an indefinite amount of data, thus making it run out of storage and denying the functionality.	Attackers overwrite the software on an ECU with malicious software.	Indefinitely sends to ECU the last known update, even if there may be newer updates on the repository.	Causes an ECU to install outdated software with known vulnerabilities.
Expertise	Multiple Experts (8)	Experts (6)	Multiple Experts (8)	Experts (6)	Multiple Experts (8)

Knowledge of System	Sensitive (7)	Restricted (3)	Critical (11)	Restricted (3)	Sensitive (7)
Equipment	Multiple Bespoke (9)	Standard (0)	Multiple Bespoke (9)	Specialised (4)	Bespoke (7)
Attacker capability	24	9	28	13	22
Time Elapsed	≤ 3 months (10)	≤ 1 month (4)	> 6 months (19)	≤ 1 month (4)	≤ 6 month (17)
Window of Opportunity	Unnecessary/unlimited (0)	Easy (1)	Moderate (4)	Easy (1)	Moderate (4)
attack potential	Beyond high (34)	Moderate (14)	Beyond high (51)	Moderate (18)	Beyond high (43)
Attack likelihood	Remote (0)	Possible (2)	Remote (0)	Possible (2)	Remote (0)
Financial	Low (1)	High (100)	High (100)	None (0)	None (0)
Privacy	High (100)	None (0)	High (100)	None (0)	Low (1)
Safety	Low (1)	High (100)	High (100)	Low (1)	Medium (10)
Operational	Medium (10)	High (100)	High (100)	Low (1)	Medium (10)
Total impact	130	2100	2200	11	111
Impact level	High (3)	Critical (4)	Critical (4)	Low (1)	High (3)
Risk	QM	High	Low	Low	QM
The mitigation methods	Acceptance	Reduction	Transference	Transference	Acceptance

5.1.1.1 Risk assessments discussion

These threats will be discussed in more detail and linked the data.

Eavesdropping and modification attack

The hacker exploits the communication between the remote repository and the vehicle and reads the unencrypted updates to steal the intellectual property of the vehicle by reverse engineering the firmware of the ECU to reach the target of the attack. Where it is possible, this is by man-in-the-middle attack in which the attacker can not only monitor data packets but receive packets and modify them or insert new packets without knowing either party. This is an outside attack but it can be accomplished from outside or inside the vehicle, and the attacker can control the cellular network that distributes updates or control via physical communications in the car which enables the attacker to spoof messages as coming from any source. Experience and knowledge are required as one of the capabilities of the attacker to do reverse engineering, while the attacker does not need two weeks to track updates, and less than two months do reverse engineering, because some updates usually work periodically every 6 months. Therefore, the likelihood of this attack is remote to achieve the objectives of this attack, due to its high impact on the vehicle. Therefore, the risk is classified as QM according to the risk matrix. This attack may be the first step to the rest of the threats. The mitigation method that could be suitable for this attack is acceptance which mean keeping risks because of would be excluded occurrence it.

Endless data attack

The attacker sends a loop of streaming data to flood the ECU with a large amount of data, which leads to the depletion of storage space or lower battery life which affects the functions of the ECU. Additional contents are appended to a updates image and re-added to the repository as a result of compromising the repository where changes are made to the updates images in the repository or if the attackers have a man-in-the-middle connection to the ECU and insert modifications to the updates. This attack might be classified as an outside threat as it comes from the repository. It is possible to target a large number of vehicles to create traffic disorder or damage the reputation of competitors, so the terrorist and organised crime categories were chosen. The attacker does not need a lot of experience, knowledge or equipment to understand the new update. It may take nearly a month to complete the attack. The

effect of the attack is the failure of an important ECU which leads to the failure of performance according to the task performed by the ECU. Where it materially affects the OEM the company's reputation may be damaged in addition to the physical damage caused by the accident. The safety of the passenger and those around the vehicle is affected if the operational functions of the vehicle are affected. The risk was calculated by finding the likelihood and the effect of the attack, as the percentage is high. As the result, the mitigation might be reduction; solutions to reduce the effect or the probability.

Arbitrary software attack

This is an outside threat in which the attackers aim to modify the performance of the vehicle arbitrarily. The attackers could overwrite a programme on the ECU and replace it with malware. These updates include not only software that is rated relatively low in affecting vehicle functions such as vehicle entertainment systems, but also highly rated software components that perform a critical function. Exposing these sensitive programmes may lead to hazards to the objects surrounding the vehicle and to passengers. Sensitive information may also be leaked during the process of controlling the vehicle. The worst-case scenarios come from controlling the images to be installed on the ECUs resulting in the ECUs could not being able to work together or making the infected vehicle distribute the malware through V2X. In this attack, the attacker needs a high experience and the ability to understand the system. The attack may take at least a year to complete in terms of information gathering and reverse engineering. It also requires physical access. The effect of such an attack is large, but the risk of its occurrence is low due to the costs and effort involved. Mitigation is the transfer of responsibility to the OEM to find a solution or effective control.

Freeze attack

Due to the lack of time recognition, many ECUs are unable to determine the time, this is where the attackers play their role on transmit the same update to ECUs even though there are potentially latest version available on the repository. In this attack, the attacker aims to deny access to updates and prevent vehicles from fixing software problems, making them vulnerable to attack by organised crime where both integrity and reliability are targeted to serve their general goals such as delaying fixing problems to make the vehicle vulnerable to other attacks. The attack requires

almost high capabilities and knowledge to carry out this attack and specialised equipment. To carry out this attack, the attacker needs approximately month and the chance of remote access is high if the attacker performs a man-in-the-middle attack. The effect of this attack is low due to its long term to reach the target which lowering the performance. Therefore, the risk is low. As with the arbitrary software attack, this attack will be sharing the responsibility with the OEM.

Rollback attack

An attacker could introduce an old version of the software with known vulnerabilities which attackers can exploit and create a path that would allow the vehicle to be manipulated or remotely controlled simply. There is no need for special controls and quality management could be enough to control it as the effect of the attack is high but the likelihood is low. The potentiality of the attack is beyond high due to the need of more time to achieve it, high expertise, expensive and specialised equipment with limited access to information.

After completing the risk assessment of the potential threats to the OTA update function, it was found that the endless data attack had the highest attack probability and impact compared to the rest of the threats (see Figure 5-1) as the affected assets in this attack affected the critical functions of the vehicle, both in-vehicle assets such as vehicle components and backend systems. The condition of the vehicle could affect the success of the attack. For example, the battery charge is too low, the temperature in the battery and poor network connection and the time it takes to download updates all affect the success of the attack. Taking into account the scenarios in which the vehicle requests the update, they are updates for safety, performance improvement or to prevent security risks as the vehicle does not update all the time. As a result, exploiting the OTA update functionality entails catching the appropriate time. Threat factors in this function are common to those of the repository and the networks used to deliver updates which makes the function more vulnerable to outside threats.

5.1.1.2 Risk assessment for OTA software updates in tool

Figure 5.2 shows the result of the risk assessment of the function on the tool that has been developed.

	Eavesdropping and modification attack	Endless data attack	Arbitrary software attack	Freeze attack	Rollback attack
the number of affected assets :	3	3	3	3	2
the threat category :	outsider	outsider	outsider	outsider	outsider
the threat agent :	Hacktivist, organized crime	Terrorist, organized crime	Hacktivist	Organized Crime	Organized Crime
the attack goal :	attackers are interested in the contents of software updates in order to reverse-engineer ECU firmware	causes an ECU to crash by sending it an indefinite amount of data, thus making it run out of storage and deny the functionality	attackers can cause an ECU to install software of the attacker's choosing. This means that the attacker can arbitrarily modify the vehicle's performance.	Attackers want to prevent vehicles from fixing software problems by denying access to updates.	Attackers try to stop ECUs from functioning correctly, thus causing the vehicle or a component to fail or behave abnormally, either temporarily or permanently.
Attack method :	tampering information disclosure elevation of privileg	tampering denial of service	tampering information disclosure elevation of privileg	tampering denial of service information disclosure	tampering denial of service
Security attributes target :	Integrity Confidentiality/Privacy Authorisation	Integrity Availability	Integrity Confidentiality/Privacy Authorisation	Integrity Confidentiality/Privacy Availability	Integrity Availability
the likelihood:	Remote	Possible	Remote	Possible	Remote
the impact of attack:	High	Critical	Critical	Low	High
the estimated risk :	QM	High	Low	Low	QM
the mitigation method :	Acceptance	Reduction	Transference	Transference	Acceptance

Figure 5.2 The report of risk assessment for OTA software update on the website

5.1.1.3 Countermeasures

In this section, we discuss the security requirement of OTA updates to perform the mitigation and present some recommended solutions mentioned in other papers. To apply the mitigation methods, security requirements often have to be defined as the first step.

Confidentiality

Data is encrypted using a symmetric encryption key shared between the sender and receiver to prevent the attacker from reading the data and accessing the firmware, as the firmware is considered proprietary data and is not disclosed.

Authentication

Data authentication ensures that the update software package is protected during transmission. The vehicle verifies that the received data packets are indeed from the repository by adding a digital signature to the transmitted data. This prevents the attacker from modifying the data in transit. Ensuring that the version is the newest update prevents an attacker from forcing the vehicle to install an old version of the firmware.

Integrity

It is important to trust that updates haven't been created maliciously when they are sent. Data integrity ensures that data packets are sent to the car via a secure protocol and without alteration, ensuring integrity through data authentication and encryption. This allows the vehicle to confirm that the contents of the packets have not been altered.

5.1.1.4 Solutions

To achieve maximum security, attacks should be controlled so that they do not affect all vehicles that are connected to the remote repository or to the infected vehicle. It is possible to restore the compromised ECU and correct the operation with minimal negative consequences. Many papers have discussed strategies to enhance the security of OTA software updates in CAVs.

A secure OTA software update framework called Uptane was created by Karthik et al. (2016) which adapts the TUF secure software repository framework. TUF works to spread tasks by dividing them into several roles, such as director, root, release, projects and timestamp. To protect against a variety of security attacks, the repository administrator bundles all the updated images and metadata files signed by each of the five administrator roles using five different private keys stored in the cloud. This provides both security and the ability to tailor updates for various vehicles depending on their specific requirements. The image repository, the director repository and the time server are its three parts.

Steger et al. (2017) developed a blockchain-based architecture to overcome security and privacy concerns with OTA software updates for smart cars. The confidentiality, integrity and authenticity of the OTA updates can be successfully guaranteed using blockchain technology. The distributed architecture’s inherent greater complexity could cause issues with costs, time commitment and effort. Furthermore, more research in blockchain architecture is required into more sophisticated update repository-related assaults, such as the endless data attack.

Mayilsamy et al. (2018) have suggested a technique for protecting vehicle OTA software updates that combine advanced encryption and picture stenography techniques. The update data is encrypted using a customised version of the RSA cryptographic algorithm and then placed along the edge of the image using the least

significant bit approach. To detect edges, they employ fuzzy logic. They use the hash algorithm to verify the veracity of the source of the software update. Compared to traditional cryptography methods, the suggested method in (Mayilsamy et al. 2018) demonstrates higher security outcomes. However, the performance of their suggested solution in terms of encryption and decryption time is a significant constraint.

The fact that the assets might be accessible in the public domain presents the biggest vulnerability that attackers can leverage so it is important to combine previous solutions like transmission cyphers to make man-in-the-middle attacks more difficult and code signature verification to prevent tampered programmes from being used by an attacker. It is also possible to integrate using cryptographic signatures, which is a necessary component of securing a software update system. Including additional information in the metadata such as knowing the expected size of the file to be downloaded also makes ECU safe against endless data attacks.

5.1.2 Lane-keeping

The primary technologies needed for CAVs are positioning, perception, judgement and control. To determine the speed, steering and braking commands for steady driving, these vehicles use a variety of sensors to identify their location, the road and the things around them. To regulate the movement of the vehicle, autonomous driving software issues orders to the drive and steering systems. Lane-keeping is one of the critical functions of keeping passengers safe by helping if the vehicle wanders out of its lane. It includes many secondary functions such as the detection of roads, detection of lanes, detection of moving agents, markings recognition and trajectory execution (Georgia et al. 2021). With the aid of various sensors which input readings to the vehicle system, the ECU produces the outputs such the required steering angle. There would be serious concerns over vehicle safety if attackers could tamper with CAVs as they are combining and processing data from various sensors or performing lane-keeping. Table 5-4 shows the critical threats related to lane-keeping. The first step of risk identification is identifying the critical assets which show in the following table.

Table 5.3 Lane-keeping function assets

Assets name	Assets category
ECU	in-vehicle component
lidar sensors	in-vehicle component
Camera	in-vehicle component
Rader	in-vehicle component
V2V	Inter-vehicular communication links

Table 5.4 Risk assessment for Lane-keeping function

The threats	Jamming attack	Spoofing attack on sensors	Spoofing attack on V2V
Attack goal	Decreasing the performance of sensors.	False detection leading to corresponding reactions.	Affecting decision making to changing vehicle direction.
Threat type	Inside threat	Inside threat	Outside threat
Threat agent	Researcher, Hacktivism	Researcher, Hacktivism	Hacktivism, Terrorist
Attack Surface	Camera, lidar, Rader, ECU	ECU, lidar, Rader	ECU, V2V
Attack Method	denial of services	Spoofing, Tampering, denial of services	Spoofing, tampering, information disclosure
Description	Attacker may use strong lights to reflect the original light or noise to degrade the signal of radar or blinding the camera by using high-brightness infrared (IR) lights or lasers on cameras that do not have infrared filters.	The attackers might simulate a fake object by reflecting lights or broadcast fake radar signals to mislead lidar or radar inputs.	Receive inaccurate information to take wrong decision.
Expertise	Layman (0)	Layman (0)	Experts (6)
Knowledge of System	Public (0)	Public (0)	Restricted (3)
Equipment	Standard (0)	Standard (0)	Bespoke (7)
Attacker capability	0	0	16
Time Elapsed	≤ 1 day (0)	≤ 1 day (0)	≤ 1 month (4)
Window of Opportunity	Unnecessary/ unlimited (0)	Unnecessary/ unlimited (0)	Unnecessary/unlimited (0)
attack potential	basic (0)	basic (0)	High (20)
Attack likelihood	Highly Likely (4)	Highly Likely (4)	Unlike (1)
Financial	Medium (10)	Medium (10)	None (0)
Privacy	None (0)	None (0)	Medium (10)

Safety	Medium (10)	Medium (10)	None (0)
Operational	Low (1)	Low (1)	None (0)
Total impact	201	201	10
Impact level	High (3)	High (3)	Low (1)
Risk	High	High	Low
The mitigation methods	Reduction	Reduction	Transference

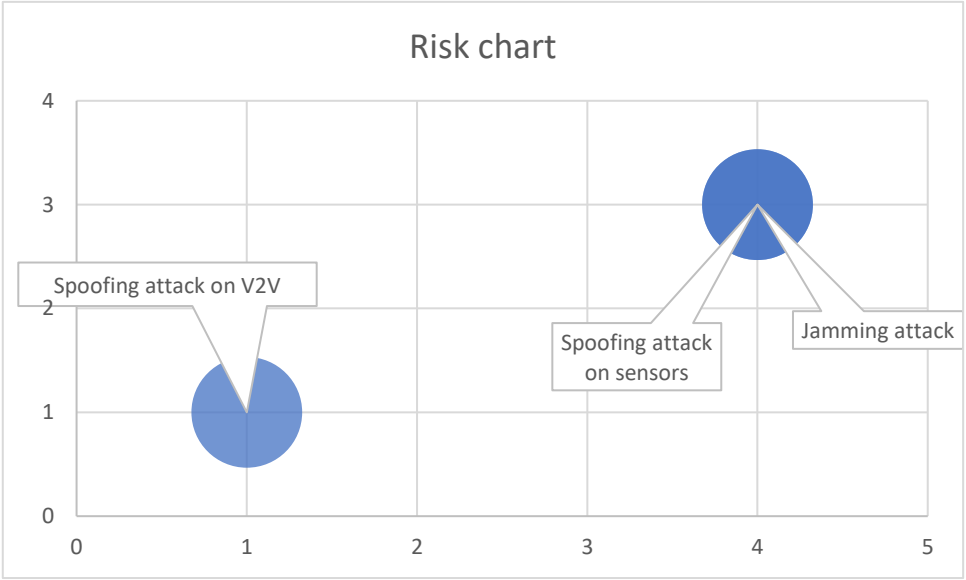

Figure 5.3 Lane-keeping risk chart

5.1.2.1 Risk assessments discussion

The risk assessment method (see Chapter 4) showed its effectiveness in calculating the risk in lane-keeping (see Table 5-4). In this function, the sensors are affected mainly by threats which influence the rest of the vehicle's systems as the wrong inputs support the attacker in confusing the lane-keeping function and making the vehicle take a wrong decision. These threats are discussed below.

Jamming attack

Jamming could be a method for hacktivists who wish to trick sensors and cause fatal damage. The attacker could use noise to degrade the radar signal or strong lights to decrease performance. It is also feasible to carry out this assault by projecting brief optical outputs to temporarily obstruct the camera because it may then only gradually adjust to the changing circumstances. The vehicle will be exposed to things it can't detect for a longer period of time the longer it takes to stabilise. The attacker will need the capability and malicious optical emitters to perform it. Using low-cost devices and with basic knowledge, the attacker can execute this attack which makes the possibility of occurrence highly likely. While it caused physical damage and fatal injuries at a medium rate, the total impact is high and so the risk is high. The mitigation would be reduced by increasing the number of sensors or enhancing their quality.

Spoofing attack on sensors

LiDAR can only see the things that the signal reflects off and if the signal is returned, it means that there is an object on the road (Stottelaar et al. 2015). The attackers could trick the sensor to suggest that there is an obstacle by replaying laser pulses at a specific position which is difficult for the sensor to recognise it as does not require any physical contact with or manipulation of the sensor. These attack types have the potential to deceive the victim sensor into providing what appears to be accurate data but is actually false (Cao et al. 2019). The radar attack includes the broadcast of fake radar signals to force the vehicle to take the corresponding actions. This attack does not need a high attacker capability and the level of effect is high which makes the risk level high. The focus would be on improving the quality of lidar and radar sensors to mitigate the threat.

Spoofing attack on V2V

The main goal of this attack is to send inaccurate information to make the ECU take the wrong action. Either the attacker pretends that the message comes from a trusted vehicle or modifies the message through a man-in-the-middle attack. This may take time to prepare and the probability of it happening would be low as performing the attack while the vehicle is moving is difficult. It puts privacy at risk but does not affect safety, finance or operations because the decision is made after referring to sensor inputs to confirm the information received. As a result, the risk level of this attack is low and the mitigation method is transference by setting some controls over sharing information by V2V.

Threat agents are hacktivists and researchers. The researcher could be interested in the sensor's functionality and testing quality management while the hacktivist might find that these are more effective and could affect single or groups of vehicles at the same time and cause a serious incident that could gain media attention. In this function, the threat comes from the inside from inaccurate inputs and wrong decisions.

5.1.2.2 Risk assessment for lane-keeping in tool

The final report shows the same findings of the assessment is shown in Table 5-4.

	Jamming attack	Spoofing attack on sensors	Spoofing attack on V2V
the number of affected assets :	4	3	2
the threat category :	insider	insider	insider
the threat agent :	Researcher, Hacktivism	Researcher, Hacktivism	Hacktivism, Terrorist
the attack goal :	Decreasing the performance of sensors.	False detection leading to corresponding reactions.	Affecting decision making to changing vehicle direction.
Attack method :	denial of service	spoofing tampering denial of service	spoofing tampering information disclosure
Security attributes target :	Availability	Authenticity Integrity Availability	Authenticity Integrity Confidentiality/Privacy
the likelihood:	Highly Likely	Highly Likely	Unlikely
the impact of attack:	High	High	Low
the estimated risk :	High	High	Low
the mitigation method :	Reduction	Reduction	Transference

Figure 5.4 The report of risk assessment for lane keeping on the website

5.1.2.3 Countermeasures

Availability

The availability of readings means that the sensors are working properly and that there is no other source affecting their work. If the sensors fail unexpectedly, the vehicle will not be able to read the road and surrounding signs, which could cause the vehicle to veer off the lane in the simplest case.

Integrity

Ensure the data of inputs are clear and not modified as the accuracy and completeness of the data affect the sensing of the environment surrounding the vehicle and thus the control of the vehicle. The data which the vehicle receives must be trustworthy over the lifecycle of the function and not modified or forced into misinterpretation.

5.1.2.4 Solutions

Although sensors follow traditional security mechanisms such as data encryption and other post-processing techniques, they are vulnerable to attacks. New defensive strategies against radar spoofing and jamming have been proposed but have not

proven effective on CAV. Shoukry et al. (2015) suggested a physical challenge-response authentication (PyCRA) mechanism to defend active sensing systems against physical assaults occurring in the analogue domain. PyCRA offers safe active sensing by sporadically but purposefully probing the surroundings. The system may verify that the fundamental physics involved are not broken by examining the replies to these probes, offering an authentication technique that not only identifies malicious assaults but also offers resilience against them. Another approach proposed by Dutta et al. (2017) is called challenge-response authentication (CRA) which identifies attacks in active sensor data and calculates secure metrics using a less squared iterative approach. However, the detecting method fails if attackers with enough resources can sample data from the active sensors quickly before being noticed.

The solutions of spoofing and jamming should not take long after detecting the attack. One of the proposed solutions that could be applied to a lidar sensor is to use different wavelengths and reduce the angle of reception of the signal by increasing the devices, but it is expensive according to Parkinson et al. (2017) who also suggested the cooperative exchange of measurements between vehicles but this solution does not exclude that the rest of the vehicles are not vulnerable to attacks and their information might be not accurate or trusted. Sending impulses randomly may not require a high budget, but it may take time to send many unused pulses and receive the response. Matsumura et al. (2018) proposed a solution that includes an authentication fingerprint set into the light wave itself. Using a side-channel trace from an Advanced encryption standard (AES) encryption, the target laser is successfully modulated. Using side-channel data from the laser light, the distance to a target item is also calculated and according to their experimental findings, an assault that decreases in the range below 30 cm cannot be made by the attacker (Matsumura et al. 2018).

In a camera blinding threat, a low-cost solution that operates at varying attack wavelengths would be ideal. Petit et al. (2015) suggested installing multiple cameras with overlapping coverage and using redundancy to capture the image from different angles, making it difficult to attack multiple cameras automatically, which could make attackers spend more effort on a successful attack. A removable infrared filter can

also be built into the front of the camera to filter out near-infrared and other unwanted lights.

Intrusion detection systems can generally be applied to detect spoofing attacks and machine learning techniques can be used to identify potential patterns but will not be useful in the case of a jamming attack. The best solutions for such threats could differ according to quality and cost, but in general, to perform the function different sensors could cover each other to keep the vehicle detecting the road.

5.2 The evaluation of the proposed methodology and the tool

The methodology is applied to two functions that follow different paths of the main functions, which are communication and automation. OTA updates represent the communication between the vehicle and the backend systems, while lane-keeping is under the automation function. The proposed methodology has proven its effectiveness in studying CAV functions which combines AV characteristics with communication. Previous studies focused on one of the two functions or were limited. It is possible to get the same results provided the same steps and the same values are used. However, this is due to the expert's expertise in estimating potential threats and their effects. The same steps were taken when applying the methodology to the two functions, from determining the probability of an attack to studying the potential effects. The risk matrix has proven to be effective in identifying mitigation methods for each threat. Many potential threats can be included but this will affect the quality of the risk chart to show the highest and lowest threat.

The tool showed the same results for the risk assessment process for both functions but there was a limitation to 8 threats so that the chart would not be affected. However, the feature of going back to previous assessments will help experts to compare the new information and new threats. In the event that a new version would be placed and a threat or new asset was added, is this reduce the value of the risks on the function or increase it. The report that appears at the end of the assessment puts all the important factors from the number of assets affected to the number of threats and the function in addition to the risk line chart. The chart was used to depict the level of risk in different dimensions, which will attract the attention of the report reader after the assessment is completed.

5.2.1 Simulation

Attack simulation is one of the most effective ways to study the potential attack's effects and the amount of damage caused, which is calculated by studying the safety, financial and operational effects. Physical damage results in financial loss, such as damage to pedestrians or the vehicle structure due to an accident or making wrong decisions due to wrong entries, which can be simulated to study the physical effects. For safety effects, the simulation can show the condition of the vehicle after the attack and the effect on the passengers and those around the vehicle. For the effects on operational functions, it is possible to simulate them during the attack event and after the attack happened and determine if the vehicle is unable to move after the attack. The study of the three effects through simulation gives a clearer picture of the extent of the damage. The time elapsed since the attack can also be calculated more accurately but in terms of privacy may be very limited. Simulation tools differ from one to the other, but it is difficult to find a tool that studies the two main functions of CAV, communication and automation. If an automation function attack simulator is available, the attack on communication functions is limited or non-existent and vice versa, so the expert may use a different simulator for each function. For communication functions, the expert might use a simulator which focuses on the network nodes to simulate the attack on the network clearly and effectively. The automations functions could use simulators that contain an autonomous vehicle component with several environments.

In the first case study, the highest risk is from the endless data attack and since the mitigation method is reducing the risk, this needs to be simulated to verify the effects by determining the type of threat. It may be appropriate to choose a network simulation tool, but this may affect some criteria for the simulation of financial, operational and safety effects. While the privacy impact will be accurate. To show how the vehicle interacts with V2I and the effect of distributing this infected update to other vehicles. With lane-keeping, jamming and spoofing attacks are the highest risk and require minimization of the risk. They can be studied through simulation tools that show the mechanics of the vehicle such as the Clara simulator, which provides environmental conditions that may affect the attack. It is also possible to measure

the weather and time; if the attack is poor light or low visibility, the quality of the attack, the time taken to attack and financial and safety effects will change.

5.3 Summary

This chapter presented the results of the risk assessment on the OTA update and lane-keeping functions. It found that endless data attack was the highest risk to the OTA function and jamming and spoofing the highest risk in lane-keeping. The results were compared with the output of the tool to the same case scenarios. Lastly, discussed the efficiency of simulating the case scenario for the main functions.

Chapter 6. Conclusion and future work

6.1 Conclusion

This thesis developed a new risk assessment method that derived from the previous methods to make it suitable for CAVs' critical components and functions. The previous literature has focused on the attack tree method or the threat to assets but the inventory of these threats is difficult to produce due to their diversity and the development of the attacker techniques and the diversity of the new attack surfaces because of the constant development of CAV components and technologies. This paper has tried to overcome these challenges by suggesting a new method that focuses on the two critical functions of communication and automation and their subfunctions as the architecture of a case study.

It started by identifying the threat to the critical function and determining the critical assets connected to it. Analysis and evaluation were done to calculate the attacker's ability and thus the likelihood and effect of these threats and define the risk level. Previous studies used human control as one of the factors that might affect the evaluation process but this study looked only at full automation. Not all attacks might cause an accident on the road and so the focus of this method was on involving the objects and stakeholders that could be affected by these threats and connecting the mitigation methods to the level of risk as other methods didn't include them on the assessment processes. Finally, it implemented the method on the OTA software update and lane-keeping functions to test the method on different paths in a CAV. On the OTA software update function which represented the communication function between V2X, it was found that the endless data attack had the highest risk level. In lane-keeping it was threats such as jamming and spoofing attacks on sensors affecting the quality of the function. This method found that these attacks affecting the quality of the function or it might tamper the tasks of the main function. It brought an effective risk assessment method specific to the CAVs' functions and components.

The main limitation was the number of threats that should be identified on a single function which must be no more than 8 to present it accurately and clearly on the risk chart. A second limitation was that the access point for each threat was not

described as the method focused on the attack method on the specific function. There are some limitations of resources as risk assessment for CAVs structures is a new field.

6.2 Future work

Future research might focus on the tasks in the function and create a functions network that includes these tasks and their threats linked with the attacker's profile. Another area is the access point of the attack; communications network, physical plugging or remote performing. A future study could describe each entry point and measure the possibility and effect and the attack profile, and which functions are affected by the threat from these points.

Reflection on learning

soft and hard skills

I learned a lot in this project starting with soft skills, the first of which is patience in the event of a mistake or difficulty. The difficulty of things lies in the initial learning of the thing. Little by little with progress and not give up. Critical and analytical thinking was developed by comparing previous research and linking it to the topic. Organising is one of the most important skills that I have developed, as dedicating hours to writing and researching and dividing them in an orderly manner for achievement prompted me to think about previous times and how a person can allocate part of his time to learning something. In addition, the most important skill related to research, auditing and linking information. As for the hard skills, this project helped me to improve my programming skill and database management review. This thesis provided important information about future vehicles and possible types of attack, which combined the risks to information technologies and AVs and in-depth risk assessment methods and mitigation techniques.

Knowledge

In this project lots of new information that I learned it about CAV. Starting from the difference between CAV and other vehicles. Then, the architecture of CAV and the new technologies on it and the new attacks may occur which will be different from the old vehicle. Finally, the diversity of risk assessment methods that are used to serve the purpose of identifying and analysing the threats on CAV. All of this information expanded my knowledge in this field according to its importance in smart cities as in the near future many of these vehicles will be on the road and all of these threats might be new trends in the crime world.

Reference list

Bailey, D. 2018. Quantitative Cybersecurity Risk Management for Autonomous Vehicle Systems. mediatum.ub.tum.de. Available at: https://mediatum.ub.tum.de/1482036 [Accessed: 30 July 2022].

Behfarnia, A. and Eslami, A. 2018. Risk Assessment of Autonomous Vehicles Using Bayesian Defense Graphs. Available at: https://ieeexplore.ieee.org/abstract/document/8690732 [Accessed: 27 April 2022].

Boudguiga, A., Boulanger, A., Chiron, P., Klaudel, W., Labiod, H. and Seguy, J.-C. 2015. RACE: Risk analysis for cooperative engines. Available at: https://ieeexplore.ieee.org/abstract/document/7266516?casa_token=qD4mincN_kAAAAAA:XILIeitbE1nIfN0jXb-EAX_22hQQwp_Q60a_qZiLFHoswyLpBd5uoRCPUEA1wqkjtxnnxfY [Accessed: 5 October 2022].

Cao, Y. et al. 2019. Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. Available at: https://arxiv.org/pdf/1907.06826.pdf.

Chow, M.C., Ma, M. and Pan, Z. 2021. Attack Models and Countermeasures for Autonomous Vehicles. Internet of Things, pp. 375–401. doi: 10.1007/978-3-030-76493-7_12.

Christensen, A., Cunningham, A., Engelman, J., Green, C., Kawashima, C., Kiger, S., Prokhorov, D., Tellis, L., Wendling, B. and Barickman, F., 2015, March. Key considerations in the development of driving automation systems. In 24th enhanced safety vehicles conference. Gothenburg, Sweden.

Di Lillo, L., Atzei, M. and Avramakis, E. 2021. On the emerging risks of automation: the case for Autonomous Vehicles | Swiss Re. Available at: https://www.swissre.com/institute/research/topics-and-risk-dialogues/digital-business-model-and-cyber-risk/autonomous-mobility-emerging-risks-of-automation.html.

Dickmanns, E.D., Behringer, R., Dickmanns, D., Hildebrandt, T., Maurer, M., Thomanek, F. and Schiehlen, J. 1994. The seeing passenger car “VaMoRs-P.” Proceedings of the Intelligent Vehicles ’94 Symposium . doi: 10.1109/ivs.1994.639472.

Dominic, D., Chhawri, S., Eustice, R.M., Ma, D. and Weimerskirch, A. 2016. Risk Assessment for Cooperative Automated Driving. Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy - CPS-SPC ‘16. doi: 10.1145/2994487.2994499.

Dutta, R.G., Guo, X., Zhang, T., Kwiat, K., Kamhoua, C., Njilla, L. and Jin, Y. 2017. Estimation of Safe Sensor Measurements of Autonomous System Under Attack. Proceedings of the 54th Annual Design Automation Conference 2017. doi: 10.1145/3061639.3062241.

Georgia, D., Ronan, H., Henrik, J., Rossen, N., Apostolos, M. and Ignacio, S.M.J. 2021. Cybersecurity challenges in the uptake of Artificial Intelligence in Autonomous Driving. policycommons.net. Available at:

https://policycommons.net/artifacts/2162455/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/2918011/ [Accessed: 25 September 2022].

He, Q., Meng, X. and Qu, R. 2020. Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles. Journal of Advanced Transportation 2020, pp. 1–15. doi: 10.1155/2020/6873273.

Henniger, O., Apvrille, L., Fuchs, A., Roudier, Y., Ruddle, A. and Weyl, B. 2009. Security requirements for automotive on-board networks. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5399279 [Accessed: 30 August 2022].

Islam, M.Md., Lautenbach, A., Sandberg, C. and Olovsson, T. 2016. A Risk Assessment Framework for Automotive Embedded Systems. Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security. doi: 10.1145/2899015.2899018.

Kim, S. and Shrestha, R. 2020. Internet of Vehicles, Vehicular Social Networks and Cybersecurity. Automotive Cyber Security, pp. 149–181. doi: 10.1007/978-981-15-8053-6_7.

Le, A. and Maple, C. 2019. A simplified approach for dynamic security risk management in connected and autonomous vehicles. Available at: https://ieeexplore.ieee.org/abstract/document/9038004 [Accessed: 30 July 2022].

Lu, W., 2021, Autonomous Vehicle and Risk Assessment. Available at: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9066295&fileOId=9066296.

Luo, F., Jiang, Y., Zhang, Z., Ren, Y. and Hou, S. 2021. Threat Analysis and Risk Assessment for Connected Vehicles: A Survey. Drosatos, G. ed. Security and Communication Networks 2021, pp. 1–19. doi: 10.1155/2021/1263820.

Maple, C., Bradbury, M., Le, A.T. and Ghirardello, K. 2019. A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. Applied Sciences 9(23), p. 5101. Available at: https://www.mdpi.com/2076-3417/9/23/5101/htm [Accessed: 14 February 2021].

Matsumura, R., Sugawara, T. and Sakiyama, K. 2018. A Secure LiDAR with AES-Based Side-Channel Fingerprinting. Available at: https://ieeexplore.ieee.org/abstract/document/8590946?casa_token=KQZI72PVcuUAAAAA:2N5PQpj8Bu2LmLESJZSD35W5XB1CJbGG1ZV6_RSFFSyjfWjXechBz79e0St9Qai9d-1H-Kk [Accessed: 27 September 2022].

Mayilsamy, K., Ramachandran, N. and Sunder Raj, V. 2018. An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air. Computers & Electrical Engineering 71, pp. 578–593. doi: 10.1016/j.compeleceng.2018.08.002.

McCall, S., Yucel, C. and Katos, V. 2021. Education in Cyber-Physical Systems Security: The Case of Connected Autonomous Vehicles. Available at: https://ieeexplore.ieee.org/abstract/document/9454086 [Accessed: 18 September 2022].

Meyer, S.F., Elvik, R. and Johnsson, E. 2021. Risk analysis for forecasting cyberattacks against connected and autonomous vehicles. Journal of Transportation Security 14(3-4), pp. 227–247. doi: 10.1007/s12198-021-00236-4.

Moalla, R., Labiod, H., Lonc, B. and Simoni, N. 2012. Risk analysis study of ITS communication architecture. Available at: https://ieeexplore.ieee.org/abstract/document/6463997?casa_token=D7j5eGNYOCsAAAAA:23a51U8uKLRLAQ4ygG4Zi-6LAatwdoUlI9N8zyE_t7ngcij1ORl1upexfL0wgfcIOZWZGDk [Accessed: 6 October 2022].

Modelling Connected and Automated Vehicles. 2019. Available at: https://www.caliper.com/TransCAD/solutions/modeling-connected-vehicles.htm.

Monteuuis, J.-P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A. and Urien, P. 2018. SARA. Proceedings of the 4th ACM Workshop on Cyber-Physical System Security. doi: 10.1145/3198458.3198465.

Park, S. and Park, H. 2022. PIER: cyber-resilient risk assessment model for connected and autonomous vehicles. Wireless Networks. doi: 10.1007/s11276-022-03084-9.

Parkinson, S., Ward, P., Wilson, K. and Miller, J. 2017. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems 18(11), pp. 2898–2915. doi: 10.1109/tits.2017.2665968.

Petit, J., Stottelaar, B., Feiri, M. and Kargl, F. 2015. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Available at: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf [Accessed: 28 September 2022].

Pham, M. and Xiong, K. 2021. A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles. Computers & Security, p. 102269. doi: 10.1016/j.cose.2021.102269.

SAE Levels of Driving Automation™ Refined for Clarity and International Audience. 2021. Available at: https://www.sae.org/blog/sae-j3016-update#:~:text=With%20a%20taxonomy%20for%20SAE%E2%80%99s%20six%20levels%20of [Accessed: 30 July 2022].

Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T. and Woody, C. 2018. Threat modeling: a summary of available methods. Available at: https://apps.dtic.mil/sti/pdfs/AD1084024.pdf.

Shoukry, Y., Martin, P., Yona, Y., Diggavi, S. and Srivastava, M. 2015. PyCRA. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. doi: 10.1145/2810103.2813679.

Steger, M., Dorri, A., Kanhere, S.S., Römer, K., Jurdak, R. and Karner, M. 2017. Secure Wireless Automotive Software Updates Using Blockchains: A Proof of Concept. Advanced Microsystems for Automotive Applications 2017, pp. 137–149. doi: 10.1007/978-3-319-66972-4_12.

Stottelaar, B., Kargl, F., Raymond, I., Petit, J. and Feiri, Dipl.-I. 2015. Practical cyber-attacks on autonomous vehicles. Available at: http://essay.utwente.nl/66766/1/Stottelaarfinals.pdf.

Team, C. 2020. CARLA. Available at: https://carla.org/.

Thing, V.L.L. and Wu, J. 2016. Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. Available at: https://ieeexplore.ieee.org/document/7917080 [Accessed: 1 April 2021].

Wang, J., Zhang, L., Huang, Y. and Zhao, J. 2020. Safety of Autonomous Vehicles. Available at: https://www.hindawi.com/journals/jat/2020/8867757/.

Karthik, T., Brown, A., Awwad, S., McCoy, D., Bielawski, R., Mott, C., Lauzon, S., Weimerskirch, A. and Cappos, J., 2016, November. Uptane: Securing software updates for automobiles. In International Conference on Embedded Security in Car (pp. 1-11).