UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Innovation and Technology Management Curriculum

Aqel Rizza Ndifuna

On The Road To Security Risk Management in Vehicle Teleoperation Scenarios

Master's Thesis (20 ECTS)

Supervisor(s): Raimundas Matulevičius PhD

Tartu 2025

On The Road To Security Risk Management in Vehicle Teleoperation Scenarios

Abstract:
Autonomous driving is an increasingly growing field in the transportation industry, with the goal to achieve full-on autonomy. However, the transition from normal driving to self-driving vehicles still needs human intervention to ensure proper decision making and safety in situations requiring human judgment, thus leading to the rise of teleoperated vehicles. While this is a solution that ensures improved road safety, teleoperation raises an issue of information security, due to the increased complexity of these systems as well as the large volumes of data transmitted across them. The increased connectivity has led to emergence of new vulnerabilities towards the data transmitted between the vehicles and remote control stations. In this paper, we conduct a systematic literature review to establish the components of teleoperated vehicles and create a general architecture of these vehicles. Then, the architecture is used to define teleoperation scenarios to which Security Risk Management (SRM) is applied following the Information Security System Risk Management (ISSRM) framework and Security Risk Oriented Misuse Cases (SROMUC), to identify possible risks to the defined scenarios and how these risks could be mitigated. Finally, the results are validated through a comparative analysis with already published literature in the field, taking into account the views of both experts and non-experts. Altogether, this thesis provides a baseline for understanding the architecture of teleoperated vehicles, illustrates teleoperation scenarios, identifies risks to defined scenarios and lays a foundation for mitigating these risks.

Keywords:
Teleoperated vehicles, Security Risk management, ISSRM, SROMUC

CERCS: T120 - Systems engineering, computer technology

Teel turvariskide haldamisele sõiduki teleoperatsiooni stsenaariumides

Lühikokkuvõte:
Autonoomne sõitmine on transporditööstuses kiiresti kasvav valdkond, mille eesmärk on saavutada täielik autonoomia. Kuid üleminek tavalisest sõitmisest isejuhtivatele sõidukitele vajab endiselt inimsekkumist, et tagada õige otsustamine ja ohutus olukordades, mis nõuavad inimlikku hinnangut, mis omakorda viib teleoperatsooniga sõidukite tekkeni. Kuigi see on lahendus, mis tagab parema teeturuohutuse, tõstatab teleoperatsioon teabe turvalisuse küsimuse, kuna nende süsteemide keerukus ja suurte andmemahtude edastamine nende kaudu kasvab. Suurenenud ühenduvus on toonud endaga kaasa uusi haavatavusi sõidukite ja kaugjuhtimispultide vahel edastatavate andmete osas. Käesolevas artiklis viime läbi süsteemse kirjanduse ülevaate, et tuvastada teleoperatsooniga sõidukite komponente ja luua nende sõidukite üldine arhitektuur. Seejärel kasutatakse arhitektuuri teleoperatsiooni stsenaariumide määratlemiseks, millele rakendatakse turvariskide haldamise (SRM) raamistikku järgides teabe turvasüsteemi riskide juhtimise (ISSRM) raamistikku ja turvariskikeskseid väärkasutuse juhtumeid (SROMUC), et tuvastada võimalikke riske määratletud stsenaariumide suhtes ja kuidas neid riske saaks leevendada. Lõpuks valideeritakse tulemused võrreldava analüüsi kaudu juba avaldatud kirjandusega valdkonnas, arvestades nii ekspertide kui ka mitteekspertide seisukohti. Kokkuvõttes annab see väitekiri aluse teleoperatsiooniga sõidukite arhitektuuri mõistmiseks, illustreerib teleoperatsiooni stsenaariume, tuvastab riskid määratletud stsenaariumitele ja loob vundamendi nende riskide leevendamiseks.

Võtmesõnad:
Kaugjuhitavad sõidukid, turvariskide juhtimine, ISSRM, SROMUC

CERCS: T120 - Süsteemiinseneeria, arvutitöötlus

Contents

List of Tables

List of Figures

1 Introduction

Devices that humans operate at a distance are surfacing at a rapid pace with greater complexity, moving from simple toys to more important aspects of human life. The light shines on remotely controlled vehicles also known as teleoperated vehicles which are becoming more common in industries such as space exploration, underwater exploration with water vessels, in the military with unmanned air vehicles such as drones and transportation industry with ground vehicles [51]. Teleoperated ground vehicles have come as an acceptable bridging gap between traditional manual vehicles and fully autonomous vehicles as they offer a much-needed fallback, assessment and decision making in situations where autonomous vehicles need human assistance [22]. The increased connectivity and vast amounts of data shared while achieving and maintaining remote operation has raised security and safety concerns from the companies operating these vehicles, passengers of these vehicles as well as other road users. This thesis aims to address some of the security concerns in teleoperated vehicles. In this thesis, we describe teleoperation scenarios to which we apply security risk management.

1.1 Objective of Research

There exist several different architectures for teleoperated vehicles presented by different papers. This research aims to combine and group the components presented in different research articles to provide a general architecture of teleoperated vehicles. There is also a lack of literature showing how different components of teleoperated vehicles interact with each other, this thesis aims to use the described architecture to describe teleoperation scenarios capturing the flow of data between components and use described scenarios for security risk management.

1.2 Scope

Despite the term "Teleoperated vehicles" being used to refer to a variety of remotely controlled objects, this thesis focuses only on ground vehicles. The thesis also focuses on how Security Risk Management can be carried out on real-world scenarios involving teleoperated vehicles hence Security Risk Management is carried out on teleoperation scenarios only leaving out parts of teleoperated vehicles that are not involved in the defined scenarios. The thesis f only explores security risks related to the Network and hence the remote station and vehicle are out of scope for this work. The implementation of security requirements and controls is also not carried out in this work. Privacy and safety aspects relating to teleoperated vehicles are also not taken into account in the thesis.

1.3 Research Questions

In order to meet the objectives of the research, A main reasearch question is proposed as follows;

MRQ: How can data used in teleoperation scenarios be secured?

The main research question is broken down into the following research questions?

- **RQ1: What components make up the architecture of teleoperated vehicles?**
- **RQ2: What are the assets involved in teleoperation scenarios?**
- **RQ3: What are the security risks in teleoperation scenarios and can they be mitigated?**

1.4 Research Methods

We employ a systematic literature review following the steps as proposed by Kitchenham [21] in order to establish the architecture of teleoperated vehicles. The thesis follows the Information System Security Risk Management method (ISSRM) to carry out security risk management for teleoperation vehicles. The thesis also uses Security Risk Oriented Misuse Cases (SROMUC) to capture vulnerabilities and mitigations for risks in teleoperation scenarios.

1.5 Contribution

The work presented in this thesis contributes to existing literature in the following ways;

1. The thesis provides a general architecture of teleoperated vehicles by carrying out a systematic literature review to capture the different components and grouping them to allow representation using a defined standard (UML class diagrams).
2. The thesis provides teleoperation scenarios that capture how components of teleoperated vehicles interact with each other as well as business and system assets involved
3. The thesis applies security risk management to defined teleoperation scenarios and illustrates how vulnerabilities that can be exploited and how risks can be mitigated.

1.6 Thesis Structure

The rest of the thesis is structured as follows: Chapter 2 presents a background, providing information needed to aid in further understanding of the following chapters. Chapter 3 defines the architecture of teleoperated vehicles using a systematic literature review.

The chapter shows the components that make up teleoperated vehicles and presents the architecture using a class diagram. In Chapter 4, we analyse critical scenarios which capture how the components of teleoperated vehicles defined in Chapter 3 interact with each other and the business and system assets involved. We also define security criteria for the business assets. We then carry out risk analysis and assessment in Chapter 5, where we define risks in the different scenarios as well as how the risks can be mitigated. Chapter 6 then presents a validation for the work done and a discussion of results, and finally Chapter 7 presents a conclusion, limitations of the thesis, answers to research questions, and future work to be carried out.

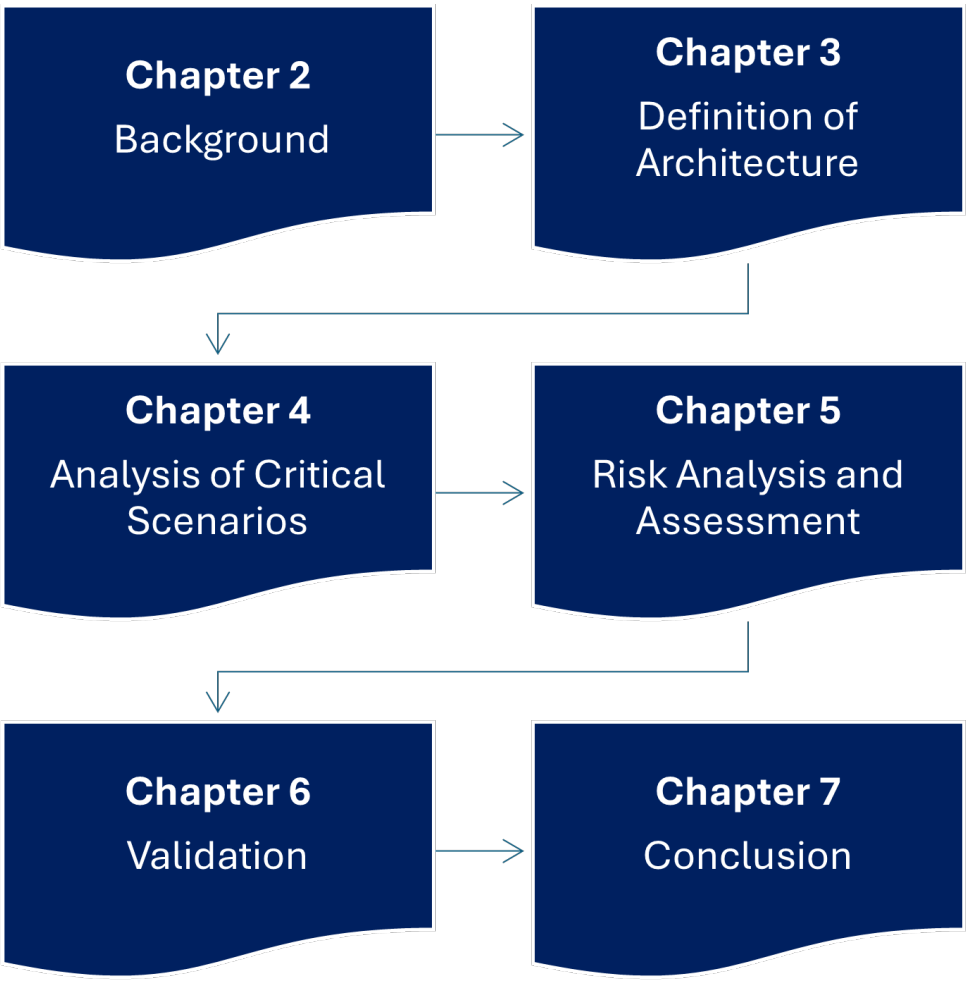


Figure 1. Thesis structure and flow

2 Background

This Chapter provides an introduction to the concepts used throughout the thesis, discussing teleoperation, Security Risk Management and its different approaches, Use and misuse cases and their constructs as well as BPMN diagrams.

2.1 Teleoperation

Teleoperation, also known as remote operation, refers to the operation of a machine from a distance. This has been applied in different industries such as in Space exploration using space rovers, in Underwater exploration using submarines and unmanned surface vehicles (USV), in surgeries, in military using Unmanned Ariel vehicles (UAVs) such as drones as well as in Unmanned Ground vehicles such as cars [51]. In general, a teleoperated system mainly consists of 3 parts and that is an operations interface, a communications link, this can be wired or wireless depending on the type of robot controlled and finally the robot which for the case of this thesis is a ground vehicle as shown in Figure 8.

The operations interface can also be referred to as a teleoperation station/centre, which is mainly to receive data transmitted from the teleoperated object or robot. It also has input devices to enable issuing commands to control the teleoperated object. The communications link or network enables transfer of data between the teleoperated object and the teleoperation centre and need to be full duplex to allow transmission of data both from the teleoperation centre to the teleoperation robot as well as from the teleoperation robot to the teleoperation centre. The third is a teleoperated object which is controlled by the person issuing commands, known as the teleoperator [51].

2.2 Security Risk Management

Risk management is defined as "coordinated activities to direct and control an organisation with regards to risk." A *risk* as defined as a "combination of the probability of an event and its consequence"[54]. Risk Management can address various issues such as risks related to organisation's management, finance, environment and security[54]. However the scope of this thesis is limited to security. *Security Risk Management* (SRM) is defined according to [28] as "an analytical procedure that helps us identify system valuable assets, stakeholders and operations as well as risk levels of undesirable events. It also provides logic and guidance to find and implement appropriate solutions for specific situations and mitigation strategies."

There exist a variety of *Risk Management* standards, however according to [54], the main standards which form the base on which other Risk Management standards are built are ISO/IEC guide [37] which defines vocabulary and guidelines used in ISO standards and the Australian/New-Zealand (AS/NZS 4360) [1] which proposes an overview of the

Risk Management process and terminology. The other standards that exist are categorised into Information Security and Information Technology security standards[54] which include the ISO/IEC 2700x which comprise of information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission and NIST 800 series which are Risk management guides for *information technology* systems standards introduced by the National Institute of Standards and Technology[54].

Information security is defined by ISO ISO/IEC 27002 (2005), as: “the preservations of the confidentiality, integrity and availability of information, for any form (hard copy or soft copy, electronic store, transmitted by email, or any other format)”. as discussed in [4]. However these principles are sometimes expanded to include Authenticity and non-repudiation. To enforce information security, organisations must implement *Information security management systems* (ISMS). A management system is defined as "a framework of processes and procedures used to ensure that an organisation can fulfil all tasks required to achieve its objectives." An *Information Security Management System* (ISMS) as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 is an international standard to provide requirements for establishing, implementing, maintaining and continually improving an information security practices in organizations [17]. An ISMS, just like all management systems, is subject to the Deming wheel, also known as the "Plan-Do-Check-Act" paradigm, which is done iteratively with *Risk Management*.

There are a number of approaches to implement ISO IEC information security standards in organizations [17] and of these, some are frameworks such as Security Requirements Engineering Process (SREP) suggested bt Mellado et al.[31] , Security Management Platform (SMP) proposed by Muller et al. [34] , ISMS-CORAS [7] an extension of the CORAS method and some are models such as Preventive Information Security Management system model (PrISM), Information Systems Security Risk Management (ISSRM) [30], AUtomated Risk and Utility Management (AURUM) [12]. Ganji et al. [17] go on to rank the different approaches based on their fulfilment of the Plan-Do-Check-Act. Of all the frameworks, no single one satisfactory fulfilled all four [17], but some covered atleast three, and of those is the ISSRM which is chosen to be used in this thesis.

The ISSRM [30] is a conceptual model for security risk management and mentions three main concepts to be considered when implementing *security risk management* and which are *asset-related concepts*, *risk-related concepts* and *risk treatment-related concepts*. The model is shown in Figure 2 in the form of a UML diagram. The asset-related concepts describe which of the organisation’s assets are important to protect and to what level of security [28]. An asset refers to anything that is valuable and plays a role in accomplishing the organisation’s objectives, and these are classified into business and system assets. [28]. Business assets refer to information, processes, capabilities and

skills essential to the business at its core and system assets refer to hardware, software or network that support business assets.

The next category is *Risk-related concepts*, which introduce risk and its components. According to ISSRM [30], a *risk* is a combination of a *threat* with one or more *vulnerabilities*, negatively impacting the *assets* , leading to negation of *security criteria*. An *impact* refers to the potential negative consequence of a *risk* that negates *security criteria*. A *vulnerability* refers to a characteristic possessed by one or a group of *IS assets* that exposes a weakness in security and can be exploited by an *attack agent*. A *threat*, on the other hand, is an incident initiated by a *threat agent* using an *attack method* targeting one or many *IS assets*.

The third category, *risk treatment-related concepts*, describes concepts to treat risk[30]. A *risk treatment* refers to the decision to treat an identified risk and is refined by *security requirements*. A security requirement refers to a condition on the environment phenomena we wish to make true by installing an information system in order to mitigate risks. Risk treatment is carried out based on the likelihood and impact of risks, and the aim of risk treatment is to bring the level of risk to an acceptable level for the organisation. According to [28], there are four categories of risk treatment decisions: *risk avoidance*, *risk reduction*, *risk transfer* and *risk retention*. The ISSRM domain model is focused on activities

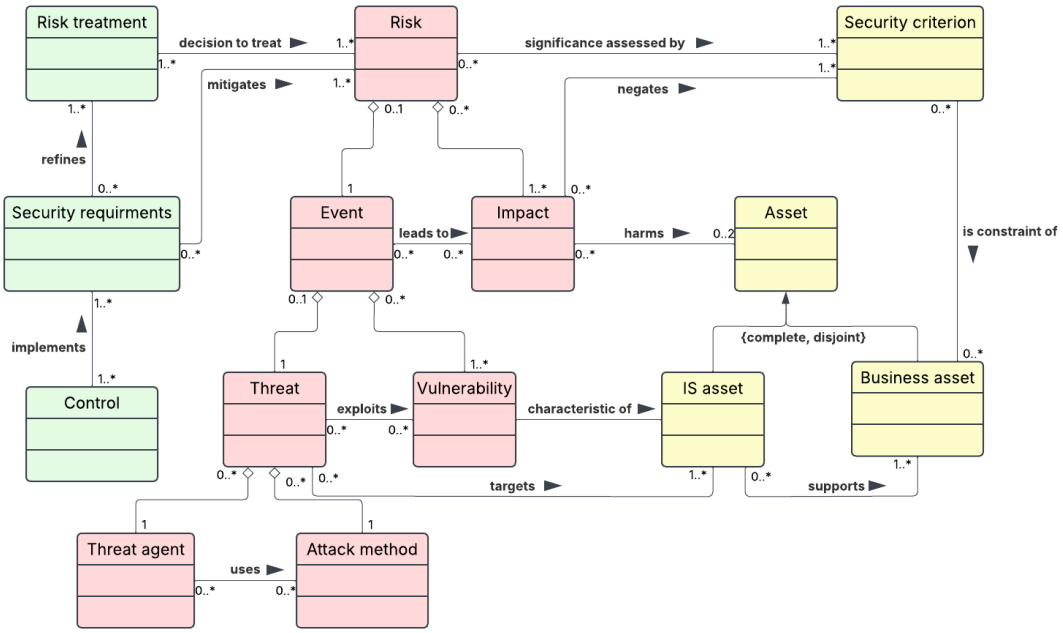


Figure 2. ISSRM domain model adapted from [54, 30]

The ISSRM domain model is focused on a process that describes activities to be

carried out for risk management [30]. The process consists of six steps (See Figure 3) which are: a) context and asset identification, which involves describing the environment in which a given system operates and the assets that make up the system. b) Security objective determination, which involves establishing security objectives following Confidentiality, Integrity and Availability (CIA). c) Risk analysis and assessment, which involves determining risks that harm security objectives and their impact on defined assets. d) Risk treatment, which involves avoiding, reducing, accepting or transferring the risk. e) Security requirements definition, which involves defining requirements that mitigate the defined risks. f) Security selection and implementation, which involves implementing security controls for security requirements

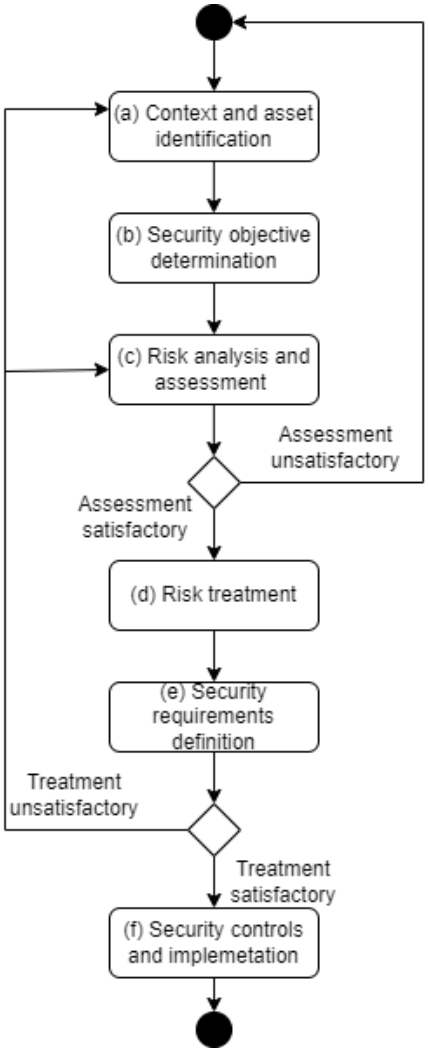


Figure 3. ISSRM process adapted from [30]

2.3 Use And Misuse Cases

A use case is defined as a set of actions performed by a system which yields an observable result that is of value to stakeholders of the system [28]. An actor specifies a role played by user, an include relationship shows that a use case contains behaviour described in another use case and an extends relationship shows extension of behaviour of targeted use case [28]. A misuse case is the inverse of a use case and could be defined as a sequence of actions that result in loss for the organisation or stakeholders [44]. Use and misuse cases can be illustrated using a graphical manner and textual format [44] as shown in Figure 4.

Figure 4. Graphical misuse case constructs adapted from [28]

Misuse cases have a security requirements process involving five steps: identifying critical assets, defining security goals, identifying threats, identifying and analysing risks and finally defining security requirements [13, 44]. A misuser is defined as an actor willing to use the system with unfavourable intentions, a threatens relationship targets a use case intends to harm, and a mitigate relationship shows how a security use case lowers impact of a misuse case [28].

Matulevičius et al. [29] captures how misuse cases can be used for security risk management and how misuse constructs can be used to illustrate ISSRM [54] concepts such as Asset related constructs (See Figure 5), Risk related concepts (See Figure 6) and Risk-treatment related concepts (See Figure 7) to achieve Security Risk Oriented Mis-Use Cases.

Figure 5 shows how the different misuse case constructs are used to represent ISSRM concepts. For example, A human asset is represented by an Actor, system assets are represented using Use Case and System Boundary, and a business asset is also represented using a Use Case. Security criteria are represented using a use case with a security criteria stereotype. Figure 6 shows how risk-related concepts of ISSRM are represented using misuse case constructs such as a risk is represented by a combination of a misuse case connected to a vulnerability by an exploits link, a misuse case connected to an impact by

an impact link, a threatens link connecting the misuse case to a use case and an includes link connecting a use case to vulnerability. Figure 7 shows how the Risk Treatment concepts of ISSRM are represented, such as a security requirement represented using a use case with a security requirement stereotype.

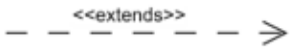
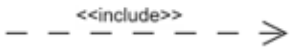
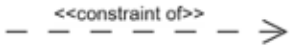
ISSRM	Misuse case constructs	Concrete syntax
Asset	Actor	
System asset	(IS) use case	
	System boundary	
Business asset	(Business) use case	
supports	Explicitly: includes and extends	 
	Implicitly: business asset constructs that are under the system boundary	
Security criterion	Security criterion (use case with stereotype <<security criterion>>)	
Constraint of	Constraint of	

Figure 5. Asset related concepts adapted from [29]

2.4 BPMN Diagrams

BPMN stands for Business Process Management and Notation, which provides a graphical way of specifying business processes in a way that is understandable for all business users while maintaining the complex semantics for technical users. This is captured using BPMN diagrams, which has become a de-facto standard for business process diagrams

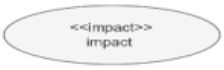
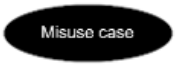
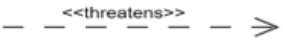
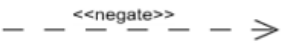
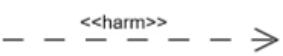
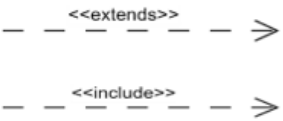
ISSRM	Misuse case constructs	Concrete syntax
Risk	A combination of constructs expressing event and impact	
Impact	Impacts (use case with stereotype <<impact>>)	
Event	A combination of constructs used to express threat and vulnerability	
Attack method	Misuse cases	
Vulnerability	Vulnerability (Use case with stereotype <<vulnerability>>)	
Threat agent	Misuser / Attacker	
Threat	A combination of misuser and misuse case using communication	
Targets	Threaten link	
Exploits	Exploit link	
Negates	Negate link	
Harms	Harm link	
Lead to	Lead to link	
Characteristic of	Include link	
uses	Communication link	

Figure 6. Risk related concepts adapted from [29]

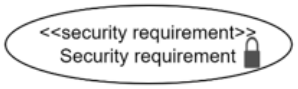
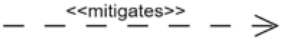
ISSRM	Misuse case constructs	Concrete syntax
Risk treatment	-	-
Security requirement	(Security) use case Use case with stereotype <<security requirement>>	
Control	-	-
refines	-	-
mitigate	Mitigate link	
implement	-	-

Figure 7. Risk-treatment related concepts Adapted from [29]

[36]. A Business Process refers to a set of linked activities that are executed in a defined sequence in order to achieve a given goal within the context of an organisational structure [9]. Business Process Management (BPM) provides governance of Business processes in order to improve agility and performance since collaboration across different enterprises is complex and changing. Business process modelling refers to the representation of business processes so that current processes can be analysed and future (to be) processes captured [9].

BPMN has four categories of graphical elements to build diagrams: *Flow elements* which represent actions happening within business processes and consist of event, activities and gateways. *Connecting objects* provide different ways of connecting various objects to each other, and they include sequence flow, message flow and association. *Swimlanes* are used to group primary modelling components and include lanes and pools. *Aritifacts* are used to provide extra information about the processes without affecting flow and include data objects, group and annotation [9].

2.5 Summary

In this Chapter, we introduced Teloperation, Security Risk Mananagement, particularly Information System Security Risk Management and its three main concepts: Asset related, risk related and risk-treatment related concepts. We also described Use and Misuse cases and their constructs. Finally we discuss Business Process Management and Notation Diagrams. The next Chapter describes the architecture of teleoperated vehicles.

3 Definition of Architecture

The existing literature was studied using a *systematic literature review* following the guidelines presented by Kitchenham et al.[21]. The stages of the review process are defining the research questions, search execution, selection of papers and finally presenting results. The systematic literature review aims to answer **RQ1: What components make up the architecture of teleoperated vehicles?**

3.1 Related Work

Very few studies define the architecture of teleoperated vehicles, and even though the individual components may differ the overall set up is similar for all teleoperated systems comprising a remote station, a network and a teleoperated object as described in section 2.1. Neumeier *et al.* [46] focuses on a way to teleoperated driving, describing how teleoperation has developed through the different stages and how full-on autonomous driving can be achieved. The paper illustrates situations where teleoperation can be useful such as valet parking and car rentals. The paper also describes a general view of teleoperated architecture and architecture of a teleoperated system.

Figure 8. Architecture of teleoperated vehicles adapted from [46]

Kakkavas *et al.* [19] focuses on the design, development and integration of teleoperated service to enable remote control of vehicles and reliability of 5G network in teleoperated support. The paper proposes a design, development and evaluation for Teleoperated Support (TeSo) service over a 5G communications realised through the EU 5G HEALTH (HEalth, AquacultuRe and Transport) project framework. The paper uses an experimental setup for validation trials to leverage Key Performance Indicators(KPI) generated from a previous experiment and valuable insights on the performance of the 5G network and its stability. Both papers provide architectures for teleoperated systems; however, the components of the systems described are both similar and different, as some of the components mentioned in [19] are not present in [46]. This shows that various teleoperated systems may have different components carrying out similar functions, which creates the need for a systematic literature review to provide a baseline architecture for vehicle teleoperated systems.

3.2 Search Strategy

The research question aimed to be answered by the systematic literature review is:
RQ1: What components make up the architecture of teleoperated vehicles?

Literature Sources: The primary sources for the literature were scientific databases, mainly IEEE, Scopus, and Science Direct. These databases were the main ones used based on the tertiary study first carried out as they offered proper arrangement of the content and filters for the different databases. They also returned the most relevant literature in the first fifty results. The chosen databases also clearly show the total number of papers returned at every step. We also included journal articles, book chapters, the internet, and conference proceedings as extra sources to cover work in progress.

Search Query: Different searches were used to find the sources of the available literature. The first search was a tertiary search across various databases and the internet. Four key words were used in this search: "teleoperated, vehicles, architecture, literature review". The search terms were then defined, and synonyms of search queries used across the three main databases were "teleoperated, vehicles, architecture, and unmanned ground vehicles." The terms were separated by "AND" and "OR",depending on the requirements of the database as shown in Table 2 below.

3.3 Selection Process

Inclusion And Exclusion Criteria : To collect papers relevant to the scope of the thesis from the selected databases, the papers were subject to inclusion and exclusion criteria as shown in Table 1.

Table 1. Inclusion and exclusion criteria

Inclusion criteria	**Exclusion criteria**
The paper is related to the research question	The paper is not related to the research question
The paper has no duplicates.	The paper is a duplicate.
The paper is written in English.	The paper is not written in English.
The paper is open access and accessible through the university	The paper is not open access and is not accessible through the university
The paper explicitly mentions components directly related to teleoperated vehicles.	The paper mentions broad aspects related to teleoperated vehicles.

Paper Selection: The initial search across the three main databases returned 690 results. This was before any filtering was applied. After the initial filtering was done using the criteria in Table 1, 262 papers remained. These were downloaded and further

filtered on the basis of the content within the papers. This filtering was performed manually by skimming through the contents of individual papers to identify whether they had information relevant to the study or not. 14 papers were selected to be read and rated as shown in the quality assessment table. For the papers to be selected for information extraction, they had to contain information about any items in the list below.

Table 2. Criteria for selection

Information	**Brief Description**
Vehicle	Mention or description of a specific ground vehicle
Architecture	Mention of component(s) contained in autonomous vehicles or teleoperated systems.
Network	Mention of networks related to teleoperated vehicles

The 14 papers selected for Quality assessment included 6 from IEEE, 1 from Scopus, 6 from Science Direct and 1 from grey literature, as shown in Table 4 below.

Table 3. Paper selection

Database	**IEEE**	**SCOPUS**	**Science Direct**	**Grey Literature**	**Total**
Results	47	80	563	8	698
First filter	23	52	179	8	262
Second filter	6	1	6	1	14
Final	4	-	2	1	7

Quality Assessment: The next phase of the review was a quality assessment of the 14 papers selected. This was done by reading through the papers and ranking them based on how well the content they presented met the quality assessment criteria. The quality assessment criteria comprised four questions:-

- Does the paper mention a specific type of vehicle?
- Is the type of vehicle mentioned a ground vehicle?
- Does the paper mention vehicle architecture and components?
- Does the paper describe a teleoperation system?

The criteria questions were obtained by breaking down the research question into smaller bits, and each question was assigned a scale of 0-5. The papers were then ranked based on how they answered each individual question and the score of each totaled. The papers that scored ten or below were discarded as the low score indicated that they were either not entirely related to the scope of this research or did not provide satisfactory data to answer the research question. The papers were ranked as shown in Table 18.

3.4 Data Extraction

The data was then extracted from the 7 selected research articles to aid in the discovery and interpretation of the components that make up the architecture of a vehicle teleoperated system and how the different components interact with one another. The structure of the teleoperated system was categorised into 3 parts namely the remote station, the network and the teleoperated vehicle as stated by [46] and components were extracted from each category as shown in Tables 16 and 17. The description of the information extracted from the papers is shown in the information extraction form in Table 4.

Table 4. Information extraction form

Information	**Extraction**
Authors	Name of authors
Title	Title of paper or article
DOI	Id of the paper
Vehicle structure	Components of the vehicle
Network	Components related of network used in the vehicles
remote station structure	Components of the remote station

Summary of Selected Articles: Kakkavas *et al.* [19] describes an architecture for the Teleoperated support (TeSo) service vehicle realised within the 5G- HEART context with an end-to-end system architecture comprising of a Remote Operations Centre (ROC) that interfaces with a human operator and receives telemetry data streams, an onboard unit (OBU) that interfaces with sensors, actuators and cameras, remote operations Centre gateway (ROCGW) and a network infrastructure. The vehicle has a local mesh network connecting the ROC and the OBU. The ROC-GW and ROC software agents were hosted on two Dell Optiplex-7070s computers equipped with a u-blox EVK-M8T and EVK-6T GNSS device. Communication between the ROC and ROC-GW was secured by a SOC 2 VPN.

Neumeier *et al.* [46] categorise the components of the teleoperated system into three parts: a Vehicle, Network, and Remote station. The vehicle has a 4/5G modem and a car PC that deals with incoming and outgoing data streams and manages the

physical buses and electric control units (ECU). Additionally, the vehicle contains a set of cameras to provide a 360 view of the vehicle's surroundings, inertial and GPS navigation, odometry sensors and mechanical actuators, a CAN bus, and a Human Machine Interface (HMI). The network comprises an air link between the vehicle and the mobile operator infrastructure, a wired public connection to a Gateway and a remote station. The remote station consists of a teleoperation Server or PC connected to the network, haptic feedback like actuators, control devices - a steering wheel and pedals for basic functionality -and control keys such as blinkers and wipers for added functionality.

Berg *et al.* [49] describe a Jeep Wrangler installed with actuators, sensors including odometry sensors, GPS navigation, ultrasonic sensors, cameras, and two Car PCs connected via an ethernet hub. The remote station described is comprised of a virtual environment using virtual reality and simulation techniques to command and monitor the vehicle. Data transmitted from the vehicle is monitored using a TV.

Lu *et al.* [23] describe a Load haul and Dump vehicle having a front and back car body, Cameras, and a master computer. The remote station consists of a button function module, a handle function module, a pedal function module on the console, a signal acquisition controller, and a host computer. There are two communication channels: The first channel is between the host computer and the signal acquisition controller, which is adapted for serial communication, and the other is the channel between the host computer and the master computer, which uses TCP/IP protocol.

Gadekar *et al.* [16] describe a modular unmanned ground vehicle for surveillance and logistics operations with an onboard computer subsystem, a surveillance unit with LIDAR, a graphics computer (Jetson Nano), A battery, an onboard computer, motor drivers, servo and DC motors, GPS, Inertial Measuring Unit (IMU), an ultrasonic sensor, an FS i6 receiver, and a raspberry camera. The communication is done using a UART communication protocol. The remote station comprises a mobile application and an FS i6 transmitter.

Ellenreider *et al.* [50] describe a four-wheel drive Losi Desert Buggy XL-E having a GNC system, GPS receivers, antennae, GNC battery, a camera, RTK GPS wireless antennae and an emergency Radio frequency (RF) manual controller. The remote station consists of an RTK GPS ground station computer (a laptop), a GPS receiver, and a force-reflexive joystick.

Tang *et al.* [48] describe the system design for a teleoperated vehicle with the vehicle having five industrial GigE (Gigabit Ethernet) cameras mounted. 2 Central Processing Units (CPU), CarPC, actuators, Electric Power steering System (EPS). The communication is done wirelessly using an LTE network using a connectionless UDP-based RTP protocol (Real-time Transport Protocol). The operator workstation has a force-feedback steering wheel, pedals, a driver seat and three 55-inch display monitors.

Component Description: The components of teleoperated vehicles, as extracted from the papers, are described together with the roles they carry out and how they are

connected to each other. The extracted components are categorised based on the three main categories of a teleoperated system which are the remote robot which is in this case the vehicle, the communication interface- the network and finally the operator interface which is the remote station [19] as shown in Figure 8.

The vehicle components are a *Car PC*, a *Human Machine Interface*(HMI), a *Physical Bus* which makes up the CAN, an *Electronic Control Unit* (ECU), *Actuators*, *On Board Unit*, *Antennae* and *Sensors* which include LIDAR, RADAR,Cameras, Inertia Measuring Unit (IMU)and GPS. On Board Unit (OBU). The network consists of an *airlink layer*, *Gateway*, a *Router* and *Modem*. The remote station is comprised of a *server*, a *computer*, *control devices*, *display devices* and an *application*. The architecture is represented using Unified Modelling Language (UML) class diagrams, where each component is represented as a class, as shown in Figure 9. Tables 5 and 6 show the extraction of components from the selected papers, based on the component generalisation for the vehicles architecture, as different papers present system-specific devices for their own architecture for instance laptop, VR, TV are all grouped as display devices.

A Car PC represents a computer installed in the teleoperated vehicle that manages the various components and interfaces of the vehicle [46], issues instructions and is a converging point for data from different components as well as communicating with the remote station over a wireless network [49].The *Electronic Control Unit* (ECU) is the component responsible for moving the vehicle's actuators and controlling the steering directions. It is connected to the car PC via physical buses which make *up the controller area network* (CAN) [46]. Mechanical actuators are used to control the vehicle actuating directly on the vehicle's steering wheel, speed pedals, and brakes [46]. The *On-Board Unit* (OBU) interfaces with *sensors* and actuators to capture operational and ambient data and make it available to other hardware and software components in a standard format[19]. The Onboard Unit also connects to external infrastructure to enable different types of communication such as V2I, V2V, and V2X. This is integrated with both the Car PC and vehicle sensors. The physical buses enable communication and transfer of data between the electronic control Unit and the Car PC . *Sensors* collect data about vehicle environment such as current vehicle speed (IMU), object detection (LIDAR and RADAR), video data (Camera) and vehicle location(GPS).

The Network refers to the different types of networks used in communication in teleoperated systems as well as the different communication protocols used in different vehicles. The network protocols vary as some use *Wireless Area Network* (WAN) [46], UART and SSH protocols [16], LTE and UDP protocols [48]. *Modem* enables the vehicle and remote station to connect to the internet [16] [50]. *Router* is a device that provides WI-FI and is connected to the modem [19]. Sensors refer to devices that detect and respond to some sort of input from the physical environment such as *LIDAR, RADAR, IMU* (Inertia Measuring Units), *Cameras*. These are integrated with the Car PC that allow vehicles to monitor their surroundings and *Airlink layer* allows for the remote

station to share data across the network [46]. *Gateway* allows the airlink layer to connect to the remote station.

The *remote station* where the vehicle is controlled and monitored from includes the components used to issue commands as well as monitor the teleoperated vehicle. These vary in complexity with some having fully developed cockpits and others a mere mobile phone. The station has a *Server* is a device that provides services to other computers connected to the network. A *Computer* connected to the server, and this could be a desktop, a laptop or even a mobile phone. An *Application* runs on a computer on the remote station and on the Car PC. It helps in achieving teleoperation. *Control devices* are used to remotely control the vehicle such as pedals, steering wheels, buttons. *Display devices* are used to show the data being shared from the remote vehicle. An *Antennae* is used to enable transmission of data between vehicles and infrastructure. VPN is used to disguise the exact location of the vehicle.

3.5 Summary

In this chapter we answer **RQ1. What components make up the architecture of teleoperated vehicles?** A systematic literature review as proposed by Kitchenham [21] was used to gather articles and extract components that make up teleoperated vehicles. Data was extracted from 7 papers that met the Quality criteria, and the components extracted were then used to construct a class diagram showing the architecture of teleoperated vehicles (See Figure 9). The described architecture is used to generate and analyse scenarios in Chapter 4.

Table 5. Component description

Component	Car Pc	ECU	Actua--tors	On Board Unit	CAN	Network	Modem	Rou--ter	Airlink	Gate--way
Kakkavas *et al.*[19]	PC	-	Actua--tors	On Board Unit	-	Local Mesh	-	Rou- -ter	-	ROC-GW
Neumeier *et al.* [46]	CarPC	ECU	Actua--tors	-	CAN (Phy--sical Buses)	Cellular WAN	-	-	Airlink Layer	-
Berg *et al.* [49]	Computer	-	Actua--tors	-	-	Remote Link kernal layer	-	-	-	-
Lu *et al.*[23]	Master Computer	Implemen--tation Computer	-	-	-	-	-	-	-	-
Gadekar*et al.* [16]	OnBoard Computer (Rasp-berry PI)	-	-	-	-	SSH client, UART	Modem	-	-	-
Ellenrieder *et al.* [50]	-	-	-	-	-	-	Modem	-	-	-
Tang *et al.* [48]	CarPc	-	-	-	-	LTE UDP RTP	-	-	-	-

Table 6. Component description cont

Component	remote station	Server	computer	Applica--tion	Control Devices	Sensors	Display devices	Antennae	VPN	HMI
Kakkavas *et al.*[19]	ROC	-	-	MATLAB	Keyboard	Sensors IMU LIDAR Cameras	-	Antennae	VPN	-
Neumeier *et al.* [46]	-	-	-	Applica--tion	Control Devices Pedals wheels	Sensor cameras	-	-	-	HMI
Berg *et al.* [49]	-	-	-	-	-	cameras, Sensors, GPS	VR,TV	-	-	-
Lu *et al.*[23]	Host computer	Host computer	-	-	Control Buttons	Camera	-	-	-	-
Gadekar*et al.* [16]	-	-	Mobile Phone	Mobile application	-	Camera, IMU HCSR GPS	-	Antennae	-	-
Ellenrieder *et al.* [50]	-	-	-	-	Laptop, Force reflexive Joystick	Camera	Laptop	antennae	-	-
Tang *et al.* [48]	-	-	-	-	-	Camera	Monitor	-	-	-

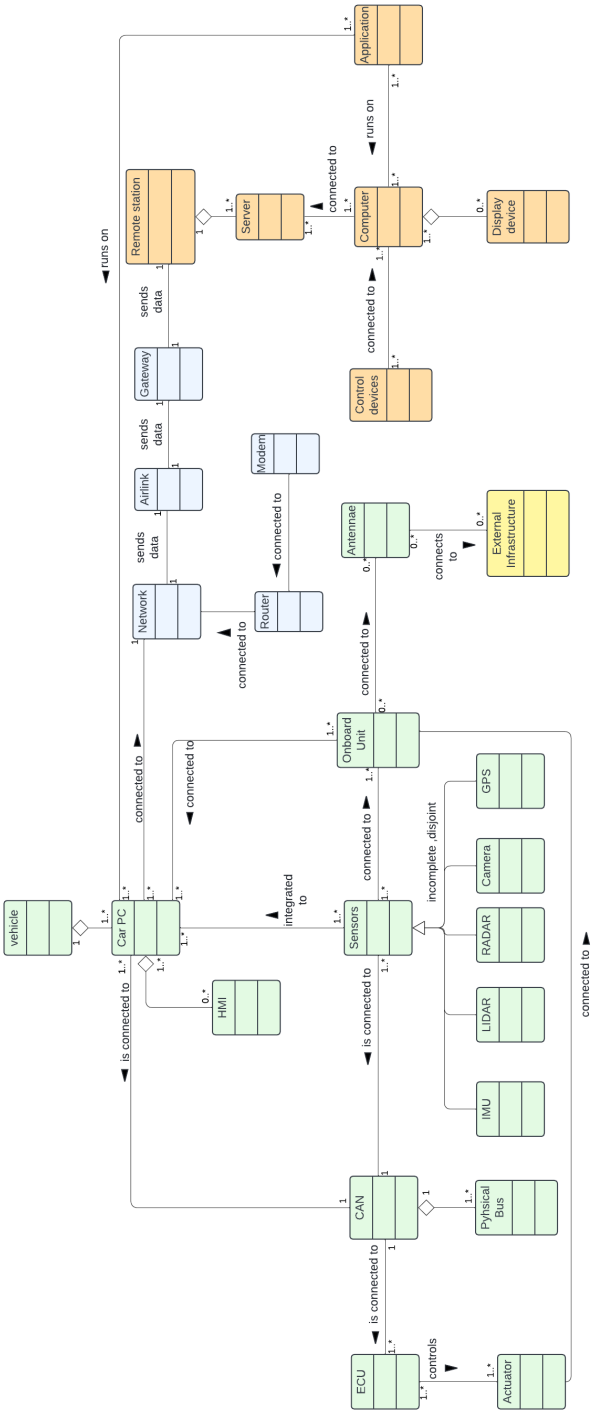


Figure 9. Expanded architecture of teleoperated vehicles

4 Analysis of Critical Scenarios

This Chapter answers the research question **RQ2: What are the assets involved in teleoperation scenarios?** This question is further broken down into;

- **RQ2.1: What are the most critical scenarios that involve vehicle teleoperation?**
- **RQ2.2: What are assets involved in the critical scenarios?**

In order to capture the operation of teleoperated vehicle systems, we use scenarios to show how the different components defined in Figure 9 interact with each other and capture how data flows between the vehicle, the network and the remote station. A scenario as described by Scutlife [47] using a general Oxford dictionary definition, refers "the outline or script of a film, with details of scenes or an imagined sequence of future events". Scenarios can be categorised depending on their use and these could be stories of current use, user designer communication, future/ imagined use [47]. The scenarios generated were to show current and imagined use of teleoperation in real-life incidents, and these are captured and elaborated using use case templates and BPMN diagrams.

4.1 Scenarios Prioritisation

To answer **RQ2.1**, 10 scenarios are brainstormed and eventually prioritised to determine the most critical ones. The 10 scenarios include;

- **S1** Control the vehicle (accelerating, braking and steering) which involves accelerating and steering moving the vehicle from one point to another, reducing vehicle speed and bringing the vehicle to a complete halt.
- **S2** Park the vehicle which includes shifting the vehicle from a drive state to a parked one, usually in designated spaces.
- **S3** Send telemetry data from the vehicle. This includes transmitting data collected by sensors and On Board Unit (OBU) to the remote station.
- **S4** Connect remote station to the vehicle which involves establishing and maintaining a connection between the remote station and the vehicle.
- **S5** Unlock vehicle. This involves remotely unlocking the locks on the vehicle doors.
- **S6** Apply indicators which involves the teleoperator turning on the signals for which direction they intend to move the vehicle.
- **S7** Turn on vehicle headlamps, which includes turning on the lights on the vehicle to a necessary intensity.

- **S8** Engage vehicle horn, which involves the teleoperator engaging the horn of the vehicle.
- **S9** Apply wipers, which involves the teleoperator turning on wipes at the windscreen or the back.
- **S10** Lock the vehicle, which involves remotely unlocking the doors of the vehicle.

The generated scenarios were then prioritised using Analytic Hierarchy Process (AHP) [41] with two criteria, i.e Importance and Impact. Importance for each scenario was gauged by the significance each scenario had in achieving teleoperation, and the impact was determined by picturing the worst possible cases and potential consequences. The AHP process is captured in Tables 22 - 27, and results are shown in Figure 10.

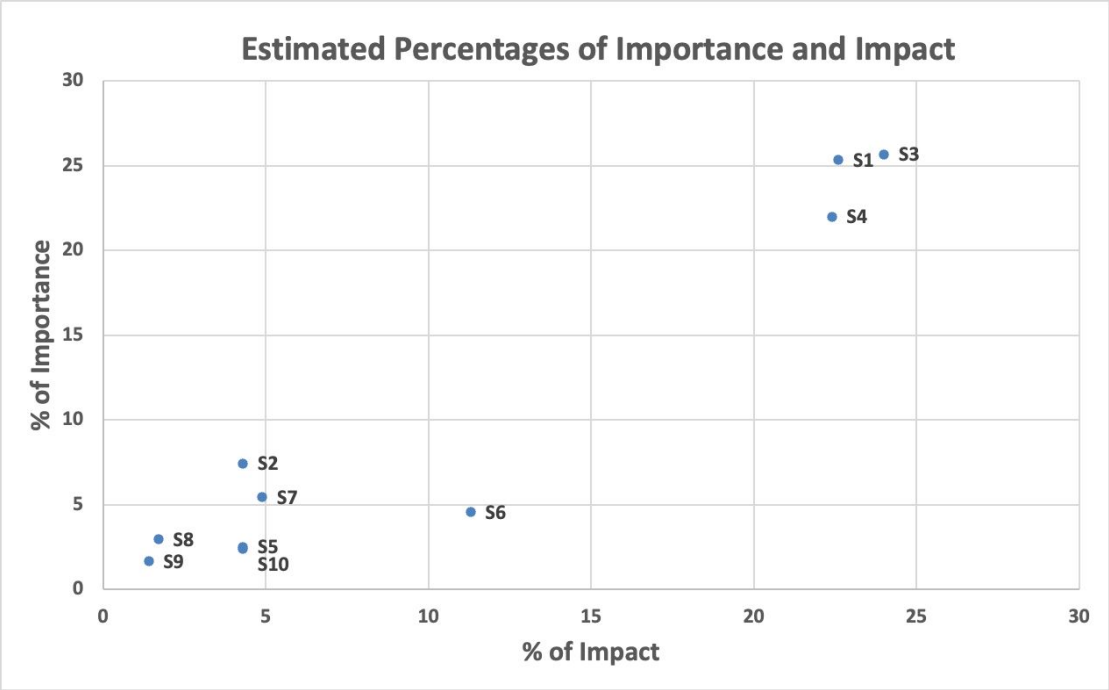


Figure 10. Graph showing the results from AHP process

4.2 Selected Scenarios

The selected scenarios from section 4.1 - are Control vehicle (**S1**), Send telemetry data from the vehicle (**S3**) and Connect remote station to vehicle (**S4**) - are then elaborated using use case diagrams to capture the actors, triggers, pre-conditions, post conditions, normal flow, priority and assumptions of each as shown in subsequent sub-subsections. Each use case is further elaborated using BPMN diagrams to capture the processes and

information shared among the different actors. This is to help fulfil step one of ISSRM as shown in Chapter 2, i.e. context and asset identification. The scenarios are presented in the order of Connect remote station to vehicle (**S4**), Send telemetry data from vehicle (**S3**) and Control vehicle(**S1**).

4.2.1 Scenario 4 (S4) - Connect Remote Station to The Vehicle

The scenario in Figure 11 describes the connect to vehicle scenario, and it begins with the teleoperator. The teleoperator starts the computer and then computer displays *login screen*. the teleoperator inputs *login data* and logs into the system. The teleoperator connects the computer to server. The computer then connects to the server. The server sends *connection request* to the network. The network provides *network configuration details* which include IP address, gateway (router's IP) and DNS. The server then provides *resources* required for the application to run which include computing power, Random access memory (RAM), storage, bandwidth, user access and control interface. The computer runs the application. The network then sends *network configuration details* to the Car PC. Scenario S4 is also illustrated using a use case template in Table 19.

4.2.2 Scenario 3 (S3) - Send Telemetry Data From Vehicle

Scenario 3 shown in Figure 12 illustrates the vehicle sending telemetry data to the remote station, to give the teleoperator a view of the environment. Scenario **S2** begins with the Sensors sending *sensory data* and On Board Unit sending *ambient data* which together make up *telemetry data* to the CAN. The CAN then sends telemetry data to the Car PC. The Car PC sends the *telemetry data* over the network, and the network sends *telemetry data* to the server. The server sends the *telemetry data* to the computer which displays the data to the teleoperator. The scenario is captured using a use case template as shown in Table 20.

4.2.3 Scenario 1 (S1) - Control Vehicle

Scenario 1 depicted in Figure 13 decribes how the teleoperator remotely controls the vehicle by issuing control commands. The scenario begins with the teleoperator analysing telemetry data. The teleoperator uses the control device to issue *drive commands*. The *drive commands* are sent to the server and then over the network. The network sends the *drive commands* to the Car PC. The Car PC sends the *drive commands* to the CAN. The CAN sends the *drive commands* to the ECU. The ECU controls the actuators. Alternatively, the teleoperator can issue *brake commands*, that are sent over the network to the ECU in a similar manner. The details of S1 are also elaborated using a use case template (See Table 21).

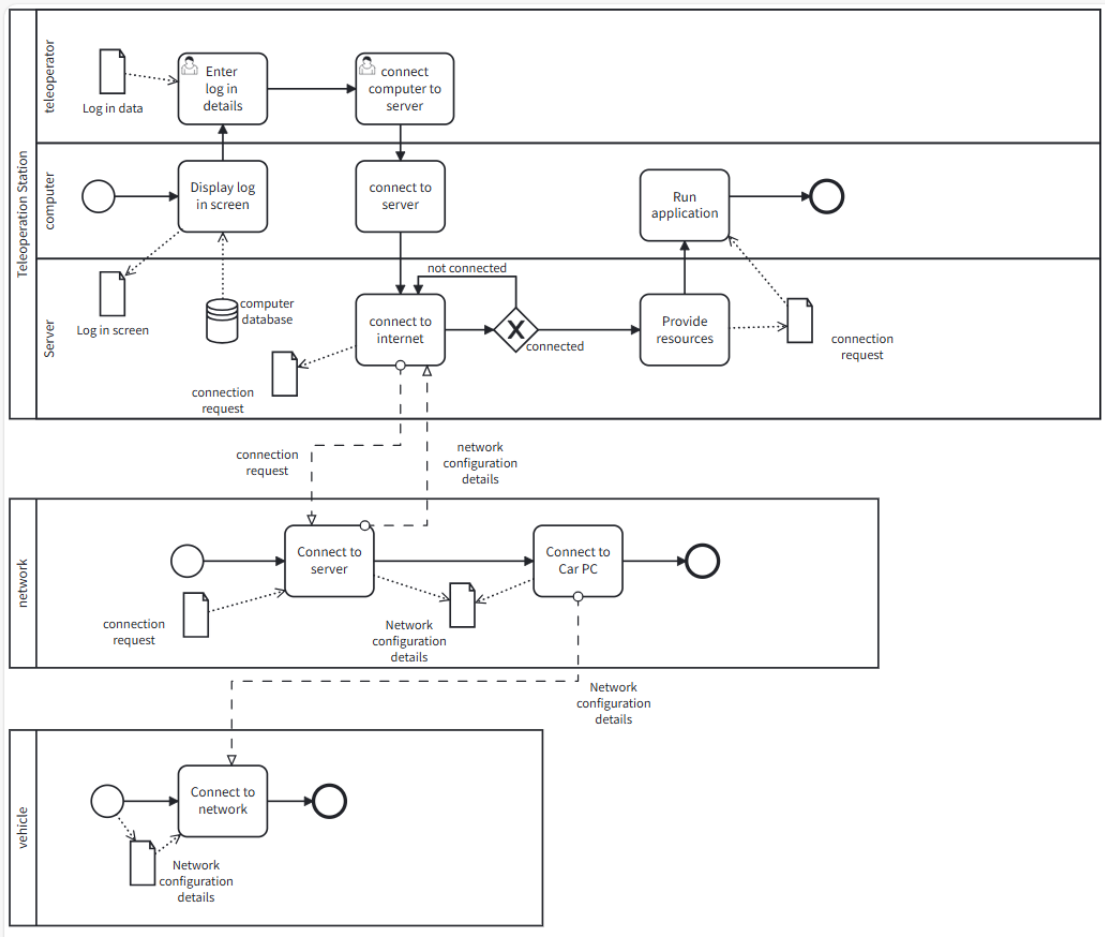


Figure 11. Model of scenario 4 (S4) - connect to vehicle

4.3 Assets in Critical Scenarios

This Section answers the research question **RQ2.2 What are the assets involved in the critical scenarios?** It aims to show the business assets in each of the scenarios in Section 4.2 as well as the system assets that support these assets. The assets are presented following the link proposed by Matulevičius [28] as shown in Table 15 using information processing functions. For each of the business assets for the scenarios, security criteria is defined as shown below.

4.3.1 Asset Identification For S4

The assets in S4 are illustrated in Table 7. The computer displays a login screen, which should be correct in order to ensure the teleoperator inputs login data in the correct slots. The *login data* captured by the computer should be kept confidential and the

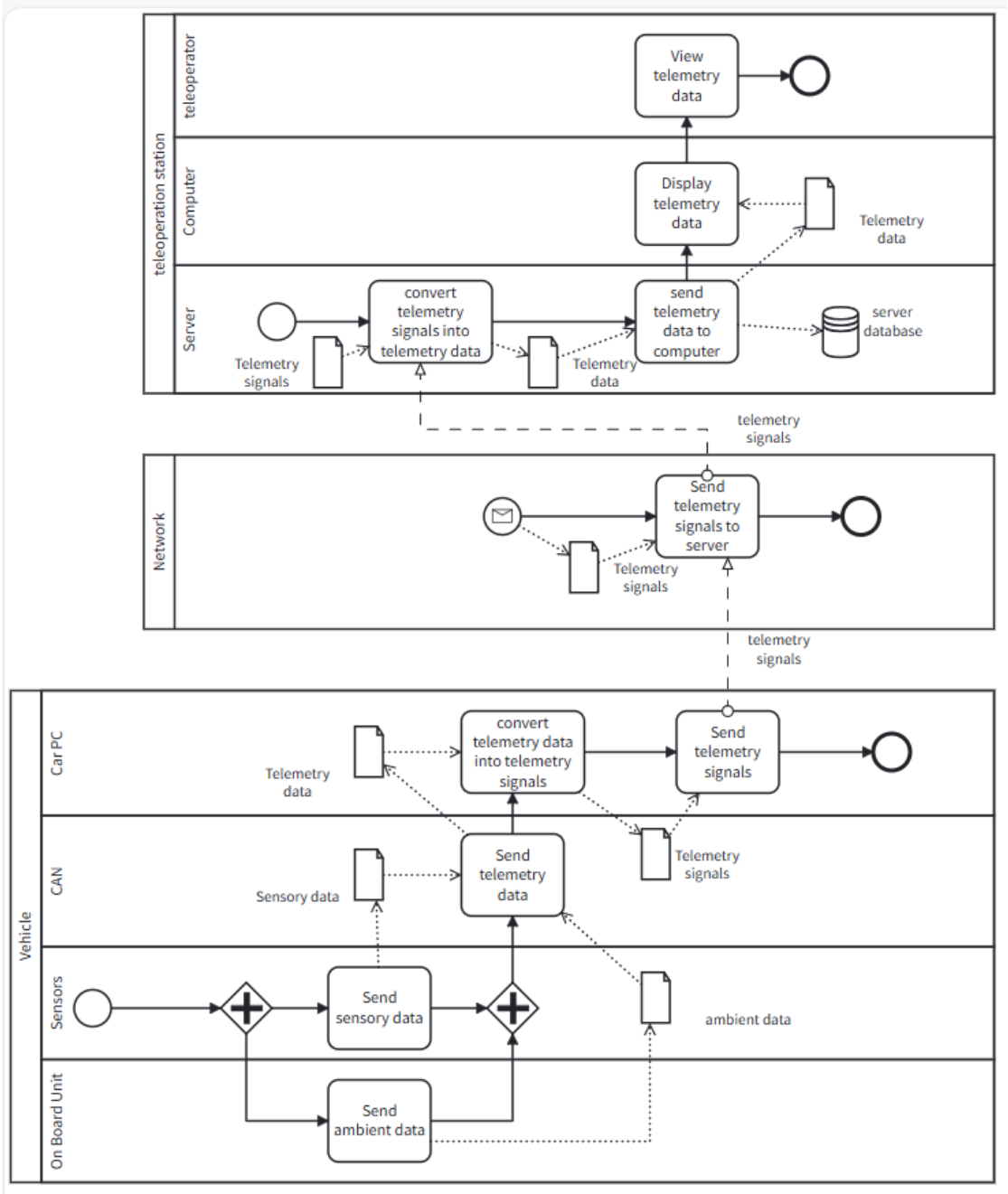


Figure 12. Model of scenario 3 (S3) - send telemetry data

data should be correct before the system is accessed, ensuring the integrity of the *login data*. Storing and retrieving information is done by both computer database and network database. For the computer database, login data is stored and this should not be accessed

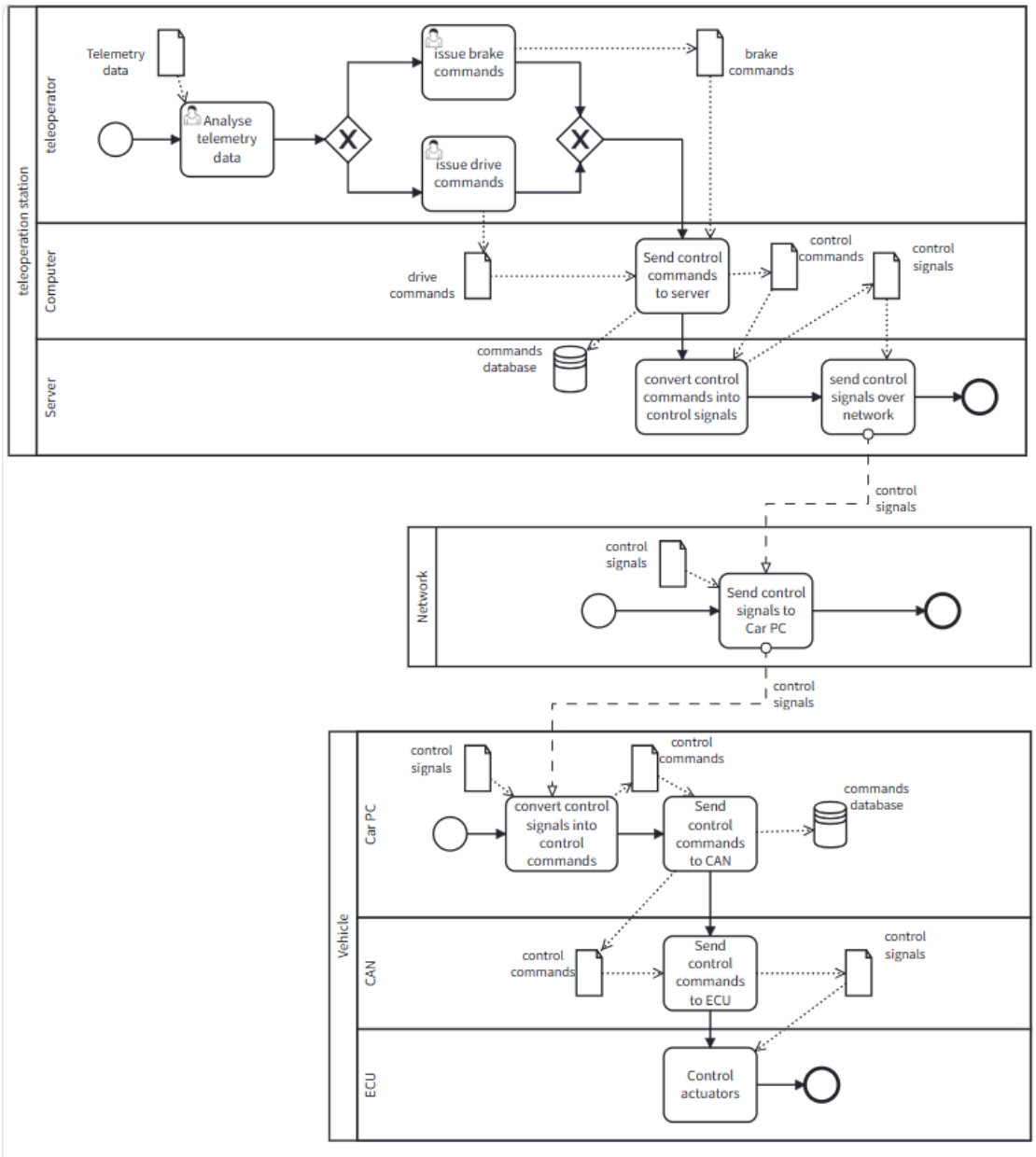


Figure 13. Model of scenario 1 (S1) - control vehicle

by unauthorised parties; the data saved should be correct thus subject to confidentiality and Integrity. The network database stores *Network configuration details* which need to be available to enable both the remote station and vehicle to connect to network. The network configuration details also need to be confidential, to avoid unauthorised connections to the network.

Table 7. Asset identification for connect remote station to vehicle scenario **S4**

Information processing functions	**System assets**	**Business assets**	**Security Criteria**
Display information	Computer	Login screen	Intergrity of login screen
Capturing information	Computer	Login data	Confidentiality of login data Integrity of login data
Storing and retrieving information	Computer database Network database	login data Network configuration details	Confidentiality of login data Integrity of login data Confidentiality of network configuration details Integrity of Network configuration details Availability of network configuration details
Manipulating information	Server	Resources	Availability of resources
Transmitting information	Network	Connection request Network configuration details	Integrity of connection request Confidentiality of network configuration details Availability of network configuration details

Manipulating information is done by a server which provides *Resources* needed to run the application, such as storage space, central processing unit (CPU), bandwidth; the resources need to be available to ensure the application can run. The Network transmits information and this supports a *connection request* from the server. The connection request is subject to integrity to ensure the request to connect is from a trusted source. The network also sends *network configuration details*, and these need to be subject to confidentiality to prevent the wrong party from accessing the network. The network configuration details are also subject to availability as they have to be present for both the remote station and the vehicle. The security criteria for each of the assets in S4 are shown using a use case diagram (See Figure 22).

4.3.2 Asset Identification For S3

The assets in S3 are identified in Table 8. Information is captured by both the On board Unit and the Sensors. The On board unit captures *ambient data* and sensors capture *sensory data*; These are both subject to confidentiality, integrity and availability and this is to ensure the ambient and sensory data is not; accessed by unauthorised parties, altered in any way or unavailable when needed by the teleoperator. Manipulating information is done by both the Car PC and the server, and this involves converting *telemetry data* into *telemetry signals*. The signals are then sent over the CAN and network and are eventually converted back to *telemetry data*. Both the *telemetry data* and *telemetry signals* are subject to confidentiality, integrity and availability in order to make sure; the *telemetry data* and *signals* are available to be transmitted, the telemetry data and signals are correct as well as to ensure they are not accessed by unauthorised parties.

Telemetry data is stored in both the vehicle state and server databases, and the *telemtry data* stored is subject to confidentiality integrity and availability to ensure the data is accessible only by authorised parties, to ensure the data stored is correct, unmodified and available when needed for use. Security criteria for S3 are also captured in use case diagrams (See Figures 23 - 29).

4.3.3 Asset Identification For S1

The assets in S1 are shown in Table 9, capturing information is supported by the computer where the teleoperator inputs *control commands* using control buttons. The control commands are subject to confidentiality, integrity and availability as they need to be accessed by only an authorised entity and be correct and available to ensure the vehicle is controlled efficiently. *Control commands* are converted into *control signals* by the server and Car PC, and eventually converted back to *control commands* to ensure proper transmission over the Network and CAN, respectively. These control commands and control signals are subject to confidentiality, integrity and availability to ensure that they are not accessed by an unauthorised party, the *control commands* and *control signals* are not changed, and they are available when needed. The *control commands* are stored in commands databases available both at the server and the Car PC and these *control commands* are subject to confidentiality, integrity and availability to make sure; unauthorised parties do not access the *control commands*, the *control commands* stored match the control commands issued as well, the control commands are available to be accessed when need arises. The Network and CAN both transmit *control signals*. The *control signals* transmitted are subject to confidentiality, integrity and availability, as the *control signals* should not be accessible without permission; the signals transmitted should be correct and should be available for transmission. Security criteria for S1 is also captured in use case diagrams (See Figures 30 - 33).

Table 8. Asset identification for send telemetry data from vehicle to remote station **S3**

Information processing functions	**System assets**	**Business assets**	**Security Criteria**
Capturing information	On Board Unit	Ambient data	Confidentiality of ambient data Integrity of Ambient data Availability of ambient data
	Sensors	Sensory data	Confidentiality of sensory data Integrity of sensory data Availability of sensory data
Manipulating information	Car PC Server	Telemetry data	Confidentiality of Telemetry data Integrity of telemetry data Availability of telemetry data
Storing and retrieving information	Vehicle state database Server database	Telemetry data	Confidentiality of telemetry data Integrity of telemetry data Availability of telemetry data
Transmitting information	CAN Network	Telemetry signals	Confidentiality of telemetry signals Integrity of telemetry signals Availability of telemetry signals

4.4 Summary

This Section answers **RQ2: What are the assets involved in teleoperation scenarios?** The section presented teleoperation scenarios that show how the components of the architecture defined in Chapter 3 interact with each other. The scenarios are prioritised to determine the most critical ones, which are elaborated further using BPMN diagrams. From the selected scenarios, we define business and the system assets that support them. For the business assets, security criteria are then described in terms of confidentiality, Integrity and Availability. The assets in the scenarios are then used for Risk Analysis and Assessment in Chapter 5.

Table 9. Asset identification for control vehicle scenario **S1**

Information processing functions	**System assets**	**Business assets**	**Security Criteria**
Capturing information	Computer	control commands	Confidentiality of control commands Integrity of control commands Availability of control commands
Manipulating information	Server Car PC	Control commands Control signals	Confidentiality of control commands Integrity of control commands Availability of control commands Confidentiality of control signals Integrity of control signals Availability of control signals
Storing and retrieving information	Commands database	Control commands	Confidentiality of control commands Integrity of control commands Availability of control commands
Transmitting information	Network CAN	Control signals	Confidentiality of control signals Integrity of control signals Availability of control signals

5 Risk Analysis and Assessment

This Chapter executes the third and fourth steps in ISSRM process (See Figure 3) - risk analysis and assessment and risk treatment. The Chapter answers research question **RQ3: What are the security risks in critical teleoperation scenarios and how can they be mitigated? RQ3** is broken down into two parts as follows;

- **RQ3.1 What are the security risks in critical scenarios?**
- **RQ3.2 How can the security risks in critical scenarios be mitigated?**

A risk as defined in Section 2.2 comprises threat and vulnerabilities. Firstly, we find out the threats that could target system assets involved in the critical scenarios shown in Chapter 4. The initial search was for a literature review on attacks in teleoperated vehicles, however there was no literature found addressing this. The next search was then done in a semi-structured way, searching for literature reviews and articles that addressed threats to individual components with a search string like "Attacks" AND "component". This was done for each of the system assets described in Chapter 4 and the results are presented in Tables 28 - 31.

From the attacks, we established that the network and CAN have the highest number of possible threats with 19 and 14 respectively. From the Scenarios shown in Chapter 4, the components that are involved in all three scenarios are Computer, Server, Network and Car PC. Based on the number of threats found, we focus on the threats to the network as it has the highest number of threats and appears in all three scenarios.

The threats to the network include Spoofing, Information disclosure, Dos, Eavesdropping, Man in the middle (MiTM), Flooding, Bidding down attack, 5G replay, IMSI catchers, Radio interference attacks, Wormhole attack, Black hole attack, Selective forwarding, Routing information attacks, Active activation attacks, Spamming, Timing attack, Router stack overflow, bootstrapping attack, and all these are categorised using the OWASP risk framework as used in [11], where threats are categorised based on Impact and likelihood as shown below.

From Figure 14, the threats that have a high impact and high likelihood were categorised as critical and these included Man in the middle(MiTM), Routing information attacks, Router stack Overflow, Bootstrapping, 5G replay, and Denial of service (Dos); a search was then executed in 4 databases in order to provide a rough idea as to the extent to which each threat has been analysed in each of the databases. The search query used involved "Threat name" AND "Network" in order to ensure the results were related to the network. A detailed categorisation of the number of papers in each database is shown in Table 32, however the results are summarised in a graph (See Figure 34).

From the search carried out, three of the least explored threats were chosen for further Risk analysis - Man in the middle (MiTM), Router stack overflow and 5G replay.

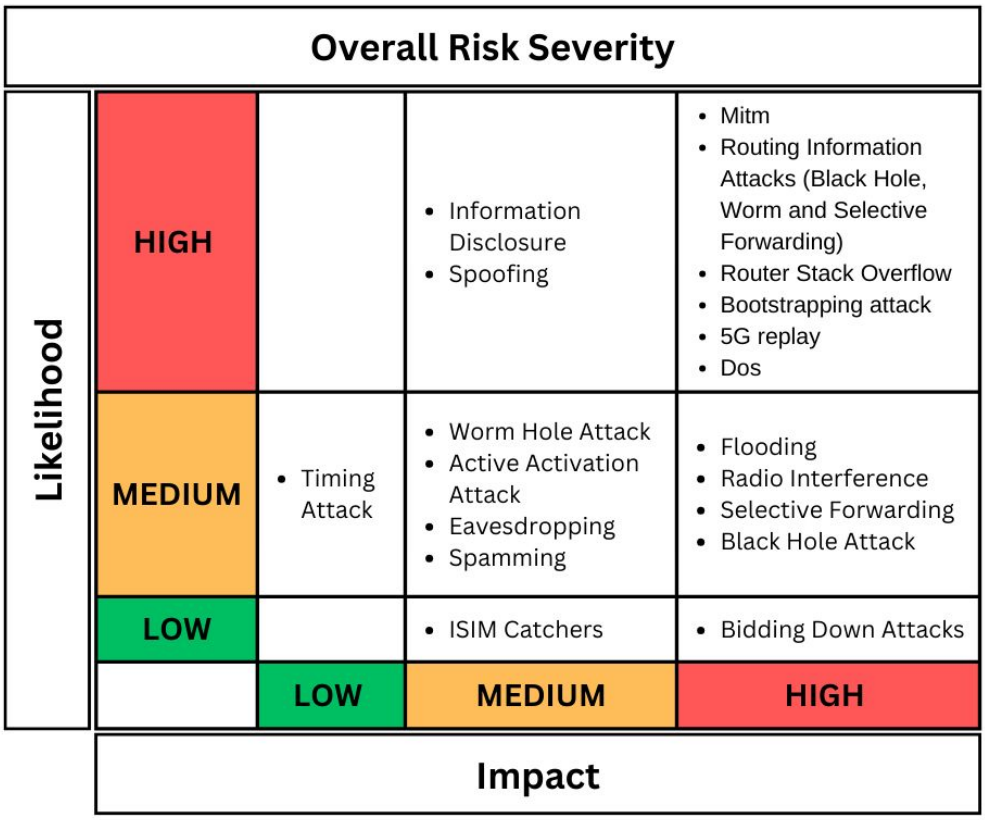


Figure 14. Network threats categorisation

5.1 Risk Analysis for Each Threat

The selected threats are analysed in depth with each risk analysed in detail using one critical scenario, that is, Router stack oveflow is analysed using S4, MiTM using S3 and 5G replay using S1. This is because even though the scenarios have different business assets, the system asset targeted (network) and vulnerabilities exploited are the same.

5.1.1 Router Stack Overflow

Router stack overflow is a type of buffer overflow attack in which the attacker sends oversized packets to the router in order to overwrite the software of the router system [15]. In scenario S4, the attacker scans router for vulnerabilities by exploiting faulty router software. The attacker then overwrites router system software due to weak security protocols of router, something that threatens 'send connection request' use case. The attacker can then issue a *connection request* to network which harms 'send connection request' and negates Integrity of *connection request* as the request sent is not from a legitimate device (See Figure15) .

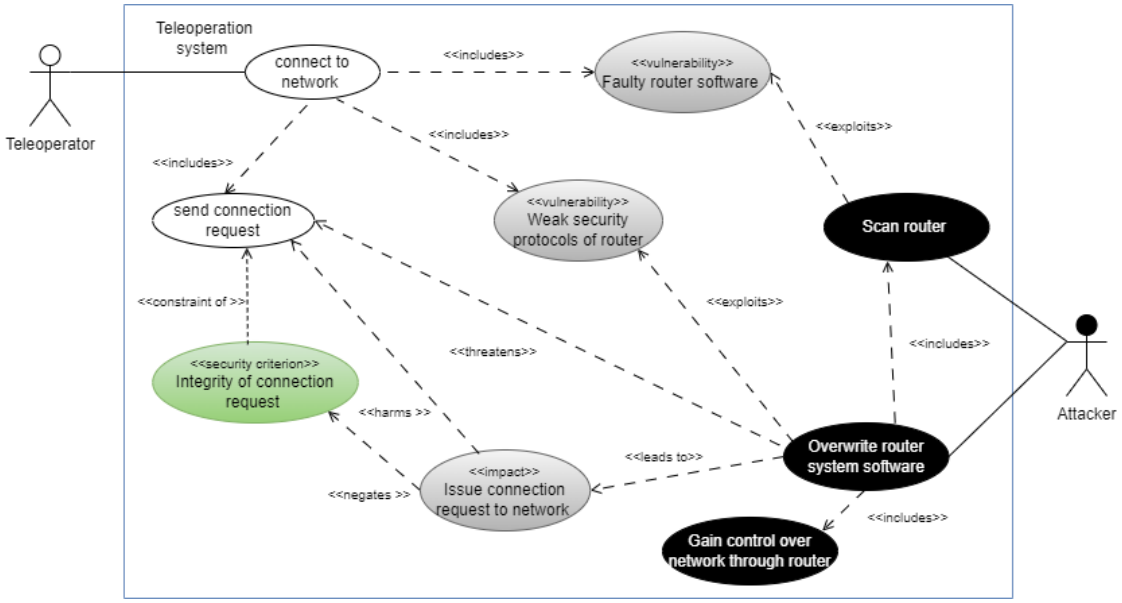


Figure 15. Misuse case showing router stack overflow 1 in scenario S4

Also in S4, the attacker could overwrite router system software by exploiting a lack of router memory protection which leads to the attacker altering *network configuration details* which harms connect to network use case. This misuse case negates; the Integrity of *network configuration details* as the details are changed, availability of *network configuration details* part or whole of them could be deleted and confidentiality of *network configuration details* since the details are accessed by attacker (See Figure 16). The attack in scenario S3 and S1 builds on 'Gain control over network' to harm telemetry and control signals respectively follows the same process as scenario S4 i.e. scan router, overwrite router system software and gain access over network through router (See Figures 35 and 36).

5.1.2 Man In The Middle (MiTM)

Man in the middle also known as manipulator in the middle or adversary in the middle refers to a type of attack in which an attacker establishes himself as a man in between communication networks and eavesdrops and alters messages sent across the network [10]. In scenario S3, an attacker establishes himself as man in the middle, due to weak authentication protocols of network (see Figure 38). There are different types of MiTM attacks, however since Teleoperated vehicles use public networks, IP spoofing-based MiTM attack is most likely which results into an entity controlling flow of communication between two parties. The attacker gains access to *telemetry signals* due to the lack of encryption of *telemetry signals*. The attacker then alters *telemetry signals* and sends them to the remote station. The teleoperator then views incorrect telemetry data, which

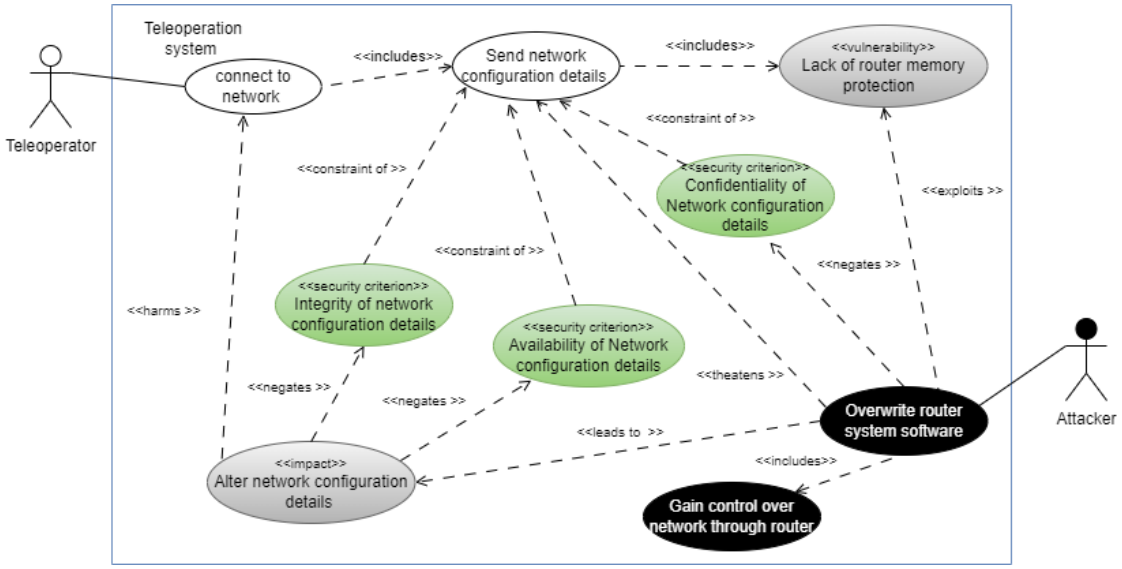


Figure 16. Misuse case showing router stack overflow 2 in scenario S4

harms the view telemetry data use case. The attack also negates the security criteria of *telemetry signals*, that is, Integrity of *telemetry signals* as the signals sent are not the correct ones, Availability of *telemetry signals* because attacker can delay or delete a part of the signals and confidentiality of *telemetry signals* as attacker accesses them (See Figure 17). MiTM for scenario S4 described in Figures 37 and 38 and S1 is shown in Figure 39.

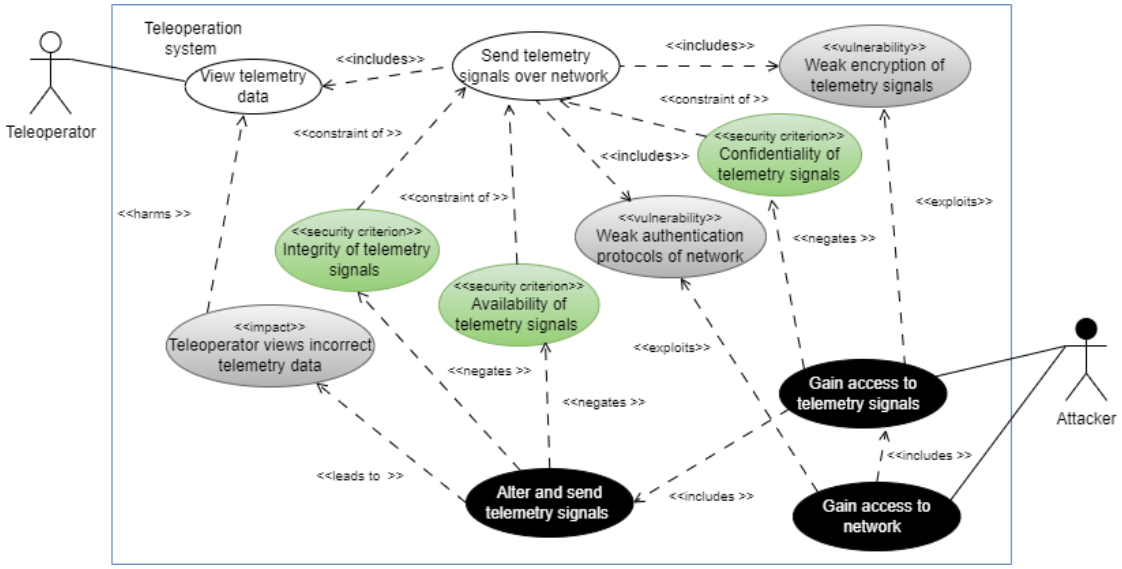


Figure 17. Misuse case showing MiTM in S3

5.1.3 5G Replay

5G replay is a replay attack over 5G where the attacker captures legitimate messages over a network and replays them back at a later time as original messages [43] and a possible replay attack is described using scenario 1. In scenario S1, the attacker accesses and stores *control signals* due to lack of encryption of *control signals*. This negates the confidentiality of *control signals* as an unauthorised party accesses them. The attacker then replays the captured *control signals* due to a lack of session updates and weak authentication in network. This leads to a vehicle executing a command more than once and in turn loss of control of vehicle. This harms issue control commands use case. Replaying old *control signals* also negates Integrity of *control signals* as the signals sent to vehicle are not new commands from the teleoperator as shown in Figure 18. 5G replay has also been illustrated in S4 (See Figure 41, 40) and S3 (See Figure 42).

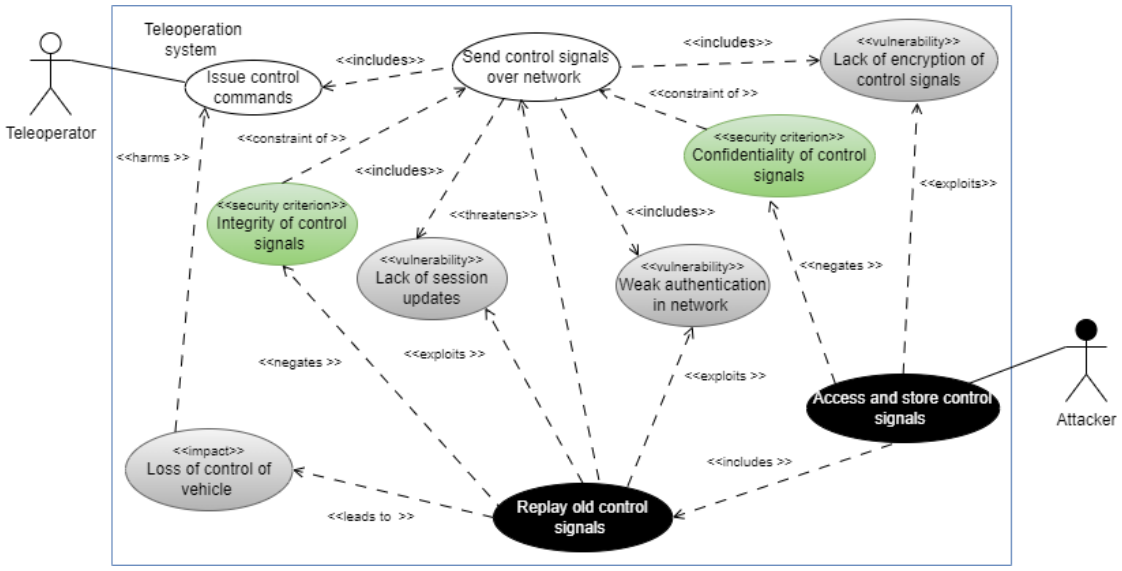


Figure 18. Misuse case showing 5G replay for scenario S1

5.2 Security Requirements and Control

This subsection aims to answer **RQ 3.2 How are the risks in critical scenarios mitigated?** To do this, we generate security requirements. A security requirement refers to a condition of an environment or component that we would like to make true with the aim of mitigating risks [28]. For each of the requirements generated, security controls are also described, which show possible ways to fulfill the security requirement. The security controls are obtained by searching for mitigation to each threat independently and mapping the proposed mitigation to defined requirements.

5.2.1 Router Stack Overflow Risk Treatment

To counter the risks in S4 (see Figure 15 and 16), we define the security requirements as illustrated using a use case diagram in 19 and misuse case template (See Table 35). The security controls for the requirements are shown in Table 12. The security requirements are;

SR1: The network should be regularly tested. Regularly testing the network allows the discovery and early handling of vulnerabilities which minimises the potential of these vulnerabilities being exploited by an attacker. In Scenario **S4**, regularly testing the network would expose vulnerabilities in router software, such as faulty router software. Some of the controls for **SR1** are: **Secure code analysis**, which enables network code to be analysed for weaknesses; **Patching**, which allows the discovered weaknesses to be mitigated.

SR2: The network should validate input. Validating input ensures that the code run is not malicious to the network, and in **S4**, input validation ensures router code is not overwritten. Security controls include: **Structured exception handling overwrite protection** (SEHOP), which prevents attackers' malicious code from being executed [14].

SR3: The memory used in the network should be inaccessible. Making memory inaccessible ensures that the data saved in memory is not accessed by an attacker. Security controls include: **Address space layout randomization (ASLR)**, which prevents an attacker from locating the memory space where executable code is located and hence is unable to overwrite it; **Data execution prevention**, which hinders the malicious code issued by an attacker from running thus preventing overwriting router software [14].

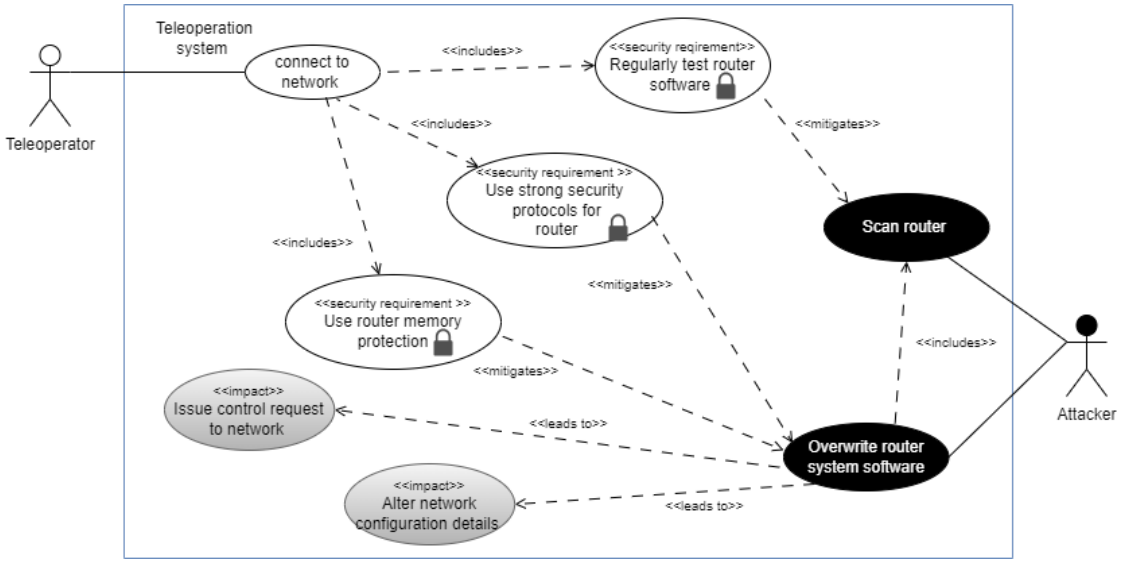


Figure 19. Risk treatment for router stack overflow in S4

Table 10. Table showing controls for security requirements for router stack overflow

Security requirement	Security control
SR1: Network should be regularly tested	Secure code analysis Patching [15]
SR2: Network should use strong security protocols	Structured exception handling overwrite protection (SEHOP) [14]
SR3: The memory used in network should be inaccessible	Address space layout randomization (ASLR) Data execution prevention [14]

5.2.2 MiTM Risk Treatment

The security requirements to mitigate MiTM (See Figure 17) are defined as;

SR4: The network should use strong security mechanisms. Strong security mechanisms alert the teleoperator or service provider about any anomalies in the network and also ensure that the information sent over the network is from a trusted party. In **S3**, strong security mechanisms would prevent an attacker from gaining access to the network. Security controls include: **Enable 2-factor authentication**, which would ensure only trusted parties gain access to the network and guarantee that data shared over network is authenticated and protected [10].

SR5: Data shared over the network should be unreadable. Making data unreadable ensures that data shared over the network cannot be read and altered by an attacker. In **S3**, making telemetry signals unreadable prevents an attacker from accessing and altering the signals. Security controls for **SR5** include: Encrypting communication using cryptography [10].

These are illustrated using a misuse case diagram (See Figure 20) and a misuse case template (See Table 36). The security requirements and controls are shown in Table 11.

Table 11. Table showing controls for security requirements for MiTM

Security requirement	Security control
SR4: Network should use strong security mechanisms	Enable 2 factor authentication (2FA) Implement SSL and TLS certificates[10] Intrusion detection systems (IDS) [10]
SR5: Data shared over network should be unreadable	Encrypt communication using cryptography [10]

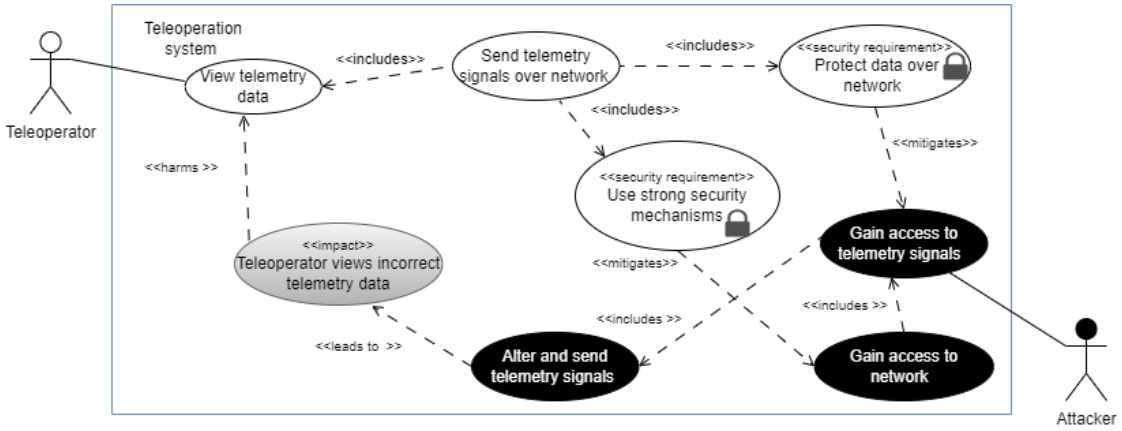


Figure 20. Risk treatment for MiTM in S3

5.2.3 5G Replay Risk Treatment

The security requirements to mitigate replay attack (see Figure 18) are defined as;

SR5: The data shared over the network should be unreadable. In **S1**, making control signals unreadable prevents an attacker from accessing and replaying the signals over the network. Security controls include encrypting communication using cryptography [52].

SR6: The network should use strong authentication mechanisms. Strong authentication mechanisms ensure that the messages shared over the network are authentic and from trusted parties. In **S1**, strong authentication mechanisms ensure that the control signals received by the Car PC are those sent by the teleoperator. One of the controls includes time-binding messages [52], which ensures that the messages that are sent to the vehicle are from the right session and timeframe.

SR7: The teleoperator should regularly update Network sessions. Regularly updating sessions ensures that messages from old sessions are no longer valid. In **S1**, updating sessions ensures that old control signals are not executed by the vehicle in the case that they are replayed. This can be enforced using time-binding messages [52].

The requirements are captured using misuse case diagrams (see Figure 21) and are also further elaborated using a misuse case template in Table 39. Security controls are as summarised in Table 12.

5.3 Summary

In Chapter 5, we answer **RQ3: What are the security risks in critical teleoperation scenarios and how can they be mitigated?** We define threats to different assets in teleoperation scenarios, focusing on the network as it is involved in all three scenarios and has the highest number of threats. Threats to the network are categorised using OWASP, and three are selected: Router stack overflow, Man in the middle and 5G replay.

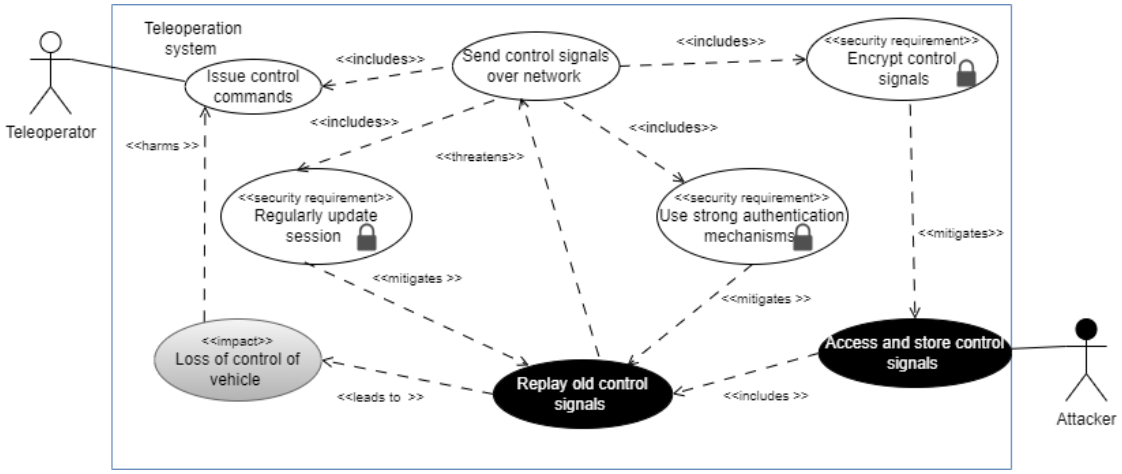


Figure 21. 5G replay in S1 treatment

Table 12. Table showing controls for security requirements for 5G replay

Security requirement	**Security control**
SR5: Data shared over network should be unreadable	Encrypt communication using cryptography [52, 10]
SR6: Network should use strong authentication mechanisms	Time-binding messages[52]
SR7: The teleoperator should regularly update network sessions	Time-binding messages[52]

Each of the threats is described using one scenario and elaborated using Misuse case diagrams after which We then use misuse cases to elicit requirements and controls to treat the defined risks.

6 Validation

In this Chapter, we validate the results of the thesis to determine the correctness, completeness and comprehensiveness of the work. We validate the work done in the thesis by comparing it with already existing published literature. The validation was split into two parts: The first was for the architecture of teleoperated vehicles, and the second for security in teleoperated vehicles.

6.1 Architecture Validation

In this section, we propose the validation research question **VRQ 1: How does the architecture presented in the thesis compare with published architecture of teleoperated vehicles in terms of completeness, comprehensiveness and intuitiveness?**

Design: The *objective* of the validation for the architecture presented is: To determine whether the presented architecture of teleoperated vehicles is *complete*, that is, if the architecture captures components for the three main parts of a teleoperated system (See Figure 8); To establish *comprehensiveness* of the presented architecture, that is, to determine whether the architecture has a high number of components, which would reflect a broader range of teleoperated vehicles. To determine *intuitiveness* of presented architecture, that is, how easy the presented architecture is to understand. To achieve the mentioned objectives, we compared the architectural diagram in the thesis (See Figure 9) with a peer-reviewed article [42] that also presents an architecture relating to teleoperated vehicles. This comparison was done by extracting components from both papers into a table. The components were extracted following the general architecture of the teleoperated vehicles (see Figure 8), and the components of each part were listed. The method to collect used for comparison is a questionnaire approach executed using Google Forms which is structured as follows:
An introduction to the survey describing the linear scale used in ranking (1-5) as;

- Rating < 3 showing preference of Architecture 1 (A1) to Architecture 2 (A2)
- Rating > 3 showing preference of Architecture 2 (A2) to Architecture 1 (A1)
- Rating of 3 showing a similarity between the two architectures.

Respondents are then asked to rate their knowledge about teleoperated vehicles on a scale of 1-10, after which they are presented with 5 questions to fill out. The design for the questionnaire is captured in Figures 50 - 54.

Execution : The link to the questionnaire was sent out to Innovation Technology Management and Quantitative Economics master's students, Computer Science PhD students, and researchers in the Autonomous Driving Lab of the University of Tartu. The respondents were asked to rate their knowledge about teleoperated vehicles on a

scale of 1-10, with 1 being "very limited" and 10 being "expert level" (See Figure 55). A total of 11 responses were received, of which 4 respondents rated their knowledge as between 7-10, another 4 respondents as between 4-6, 2 respondents as between 1-3, and 1 respondent did not rate themselves.

Analysis: The results for each question were grouped based on the criteria each question represented, with Qn 1 and Qn 2 investigating completeness, Qn 3 aimed at comprehensiveness and Qn 4 aimed at intuitiveness. The responses from the participants were grouped based on the level of knowledge by each of the participants as shown in Table 42. For each group, each individual response is added and used to calculate the average of each group's response to each question. The average values for each group for each question are then summed up and used to get a final average for each criterion, as shown in Table 13.

Table 13. Summary of results comparing architecture

Criteria	**Question**	**7-10**	**4-6**	**1-3**	**Average**
Completeness	Qn 1	4	5	5	5
Completeness	Qn 2	4	4	4	4
Comprehensiveness	Qn 3	5	5	5	5
Intuitiveness	Qn 4	2	2	1	2

The average values are interpreted using the initial scale proposed in the survey with values > 3 preferring Architecture 1 (A1) to Architecture 2 (A2), values < 3 preferring Architecture 2 (A2) to Architecture 1 and 3 showing a neutral preference. Architecture 1 (A1) represents the architecture presented in [42] while Architecture 2 (A2) represents the architecture shown in the thesis (see Figure 9).

From Table 13, the results show that for:

- Completeness - The averages of Qn 1 and Qn 2 are > 3, indicating Architecture 2 (A2) is preferred to Architecture 1 (A1).
- Comprehensiveness - average of Qn 3 is > 3, indicating Architecture 2 (A2) is preferred to Architecture 1 (A1).
- Intuitiveness - The average of Qn 4 is < 3, indicating Architecture 1 (A1), is preferred to Architecture 2 (A2).

Threats to validity: The number of people who participated in the survey was minimal, making it hard to draw solid conclusions based on a limited sample. The questions presented in the questionnaire were made as concise as possible to make it easy to do for all levels of expertise, leaving out important information which could

have enabled participants to make more detailed choices. The validation criteria are also limited to certain aspects, leaving out important criteria such as functionality, to compare the applicability of the presented architecture.

6.2 Security Risk Management Validation

For security risk management, we propose the validation research question **VRQ 2: How does the security risk management approach used in the thesis compare with published literature on security in teleoperated vehicles in terms of descriptiveness, specificity and uniqueness?**

Design: The *objective* for validation in this section was to compare the approach of defining and mitigating risks in teleoperation scenarios to determine the *descriptiveness* of Security Oriented Misuse Cases (SROMUC) used in the thesis, that is, the level of detail presented for illustrating a given risk as well as procedure for risk mitigation; to determine the *specificity* of the Security Oriented Misuse Cases (SROMUC) i.e. whether the description and mitigation of the risks are specific to one given risk in detail, to determine *uniqueness* of SROMUC, that is, whether the approach stands out from other ways of managing security risks. To meet the set objectives, we compare the thesis with published literature on risk management in teleoperated vehicles. The paper chosen is a white paper addressing privacy and cybersecurity challenges in vehicle teleoperation and mitigation strategies [2]. The paper is produced by QA Consultants, which is an independent software quality engineering services firm in North America. The paper is produced together with The Automotive Parts Manufacturers' Association (APMA) of Canada and is supported by APMA's V2X cybersecurity committee, which is made up of 11 members who are well-versed with Automotive cybersecurity [2]. The method used for comparison is also a questionnaire approach executed using Google Forms, which is structured as follows: Security risk management approach for the thesis is presented as Option A, and the approach in the white paper is presented as Option B.
An introduction to the survey describes the linear scale used in ranking (1-5) with:

- Rating < 3 showing a preference for Option A over Option B
- Rating > 3 showing a preference for Option B over Option A
- Rating of 3 showing a similarity between the two options.

Respondents were then asked to rate their knowledge about teleoperated vehicles on a scale of 1-10 after which respondents are presented with 5 questions to fill in. The design for the questionnaire is captured in Figures 50 - 54.

Execution : The link to the questionnaire was also sent out to Innovation Technology Management and Quantitative Economics master's students, Computer Science PhD students, and researchers in the Autonomous Driving Lab of the University of Tartu. The

respondents were asked to rate their knowledge about security risk management on a scale of 1-10, with 1 being "very limited" and 10 being "expert level" (See Figure 67). A total of 12 responses, and they rated their understanding of security risk management as follows: 6 respondents rated themselves as 7-10, 5 respondents rated themselves as 4-6, and 1 respondent rated themselves as 1-3.

Analysis: The results for the risk management questionnaire were also grouped based on criteria with Qn 1, Qn 2, Qn 5 and Qn 6 aimed at descriptiveness, Qn 3 aimed at specificity and Qn 4 aimed at Uniqueness. The responses are grouped into 3 categories based on the way participants rated their understanding of security risk management, as shown in Table 43. An average for each group is then calculated using the sum of the responses, and the average values for each group are used to calculate the average for each question as shown in Table 14.

Table 14. Summary of results comparing risk management approaches

Criteria	**Question**	**7-10**	**4-6**	**1-3**	**Average**
Descriptiveness	Qn 1	2	3	2	2
Descriptiveness	Qn 2	2	2	1	2
Descriptiveness	Qn 5	2	2	-	2
Descriptiveness	Qn 6	2	3	1	2
Specificity	Qn 3	2	3	1	2
Uniqueness	Qn 4	3	2	2	2

The averages are interpreted using the linear scale proposed in the survey, however, Uniqueness is measured on a scale of 1-5, with 5 showing a high similarity between the two Options.

From Table 14, the results show that for:

- Descriptiveness - The averages of Qn 1, Qn 2, Qn 5 and Qn 6 are < 3, indicating that Option A is preferred to Option B.
- Specificity - The average of Qn 3 is < 3 indicating that Option A is preferred to Option B.
- Uniqueness - The value is 2, which shows there is little similarity between the two Options.

Threats to validity: The small size of the participants makes it difficult to draw substantial conclusions. The questionnaire only presented snippets of each approach, which makes it difficult to properly judge the two options, as security risk management is a whole process. The ratings of knowledge are also based on the participants, and in order to maintain privacy, no personal details were gathered, which makes it hard to back up the knowledge ratings of participants.

6.3 Discussion

In the architecture validation, the comparison paper was presented as Architecture 1 (A1), and the thesis architecture was Architecture 2 (A2). We asked the respondents to choose which overall architecture they preferred, and while 36 percent of the respondents chose Architecture 1 (A1), 64 percent of the respondents chose Architecture 2 (A2). Of the respondents who chose architecture 1 (A1), they preferred A1 because of its ease of understanding, fewer components that were easier to read and the fact that it was specific to one teleoperated vehicle. The respondents who chose Architecture 2, stated it was more detailed and covered more components for teleoperated vehicles. They also preferred Architecture 2 as it was presented using a well-defined standard, that is, UML class diagrams. For the experts (those who rated their knowledge 7-10), 75 percent preferred architecture 2, 25 percent preferred architecture 1 as it was more concrete and specific to one system but stated that architecture 2 is better to use for security risk management as it covers a bigger range of components.

For the validation of security risk management, the security risk management approach in this thesis was presented as Option A and risk management as described by Ahasanun *et al.* [2] was presented as Option B. The participants were asked to choose between the mitigation options presented, and a staggering 91 percent of the respondents preferred Option A and 9 percent preferred Option B. The responses for questions 5 and 6 were out of 11, as one person did not provide a response. Of the respondents, the participants who chose Option A gave their reasons as: it was more detailed, used a specific method to define risks and mitigation, discussed requirements for security risk management and is more precise. The validation provides strong evidence that security risk oriented misuse cases (SROMUC) provide a detailed approach towards security risk management. The participants were also asked to rate similarity in the definition of risks in the two options and the average was < 3 (See Table 14) which meant that there was little similarity between the approaches despite both approaches describing the same attack, that is, both options mentioned Man in the middle attack.

6.4 Summary

In this Chapter, we validate the architecture and the security risk management approach presented in this thesis by comparing the thesis work with already published literature in the field. The validation is done using a questionnaire approach and is executed using Google Forms. The Chapter describes the design of the questionnaires, the groups of people who participated and their level of expertise. The Chapter then discusses the results from the questionnaires and their implications.

7 Conclusion

In this thesis, we carry out security risk management in teleoperated vehicles using teleoperaion scenarios while following the ISSRM risk mitigation process. To achieve this, we define an architecture for teleoperated vehicles using a systematic literature review, after which we define scenarios using BPMN diagrams to show the data shared among the different components. Then, we determine both system and business assets in the scenarios and define security criteria for the business assets. Next, we narrow down the thesis scope and focus on the network in teleoperated vehicles and carry out a risk assessment to determine risks that negate security criteria to network assets and propose ways to mitigate the captured risks using Security Risk Oriented Misuse Case (SROMUC) diagrams.

7.1 Limitations of Work

The broad scope of this work and its required workload leave room for limitations. First, despite the paper applying a systematic literature review to create an all-encompassing architecture of teleoperated vehicles, only three databases were considered thus some components could have been omitted. The paper also does not consider articles from vehicle websites, and this is because, although numerous companies are actively testing and implementing teleoperation, details of their vehicle architecture and operational procedures are undisclosed; thus we present only publicly available information and do not include components that may be recent developments or trade secrets.

Also in this work, the search for the threats to each individual component was not exhaustive, and hence, a number of risks were left out of the thesis. Furthermore, the selected risks are illustrated using Misuse case diagrams, which offer a certain level of abstraction, something that limits the thesis' ability to illustrate risks in depth. The thesis also investigates only 3 risks and does not consider other potential attacks to the network as well as risks to the vehicle and remote station.

7.2 Answer to Research Questions

In this section we answer our main research question **MRQ: How can data used in teleoperation scenarios be secured?**. This is done by providing answers to the broken-down research questions:

RQ1: What components make up the architecture of teleoperated vehicles? To define the components that make up teleoperated vehicle architecture, we carry out a SLR as shown in Chapter 3 and identify three main parts:

- Vehicle which comprises Car PC, Human Machine Interface (HMI), Physical Bus which makes up the CAN, an Electronic Control Unit (ECU), Actuators, On Board

Unit, Antennae and Sensors which include LIDAR, RADAR,Cameras, Inertia Measuring Unit (IMU)and GPS. On Board Unit (OBU),

- Network consists of an airlink layer, a Gateway, a Router and a Modem
- Remote station which comprises a server, a computer, control devices, display devices and an application.

RQ2: What are the assets involved in teleoperation scenarios? Scenarios were defined in Chapter 4, and three of the defined scenarios were selected. The assets involved in the chosen scenarios are classified into business and system assets. For scenario S4, the assets system assets include: Computer, computer database, Network database, Server and network. The business assets include login screen, login data, Network configuration details, resources, connection request, network configuration details. For scenario S3, the system assets include, On Board Unit, sensors which include LIDAR, RADAR,Cameras, Inertia Measuring Unit (IMU)and GPS, Car PC, server, vehicle state database, server database, CAN, network. The business assets for scenario S3 include ambient data, sensory data, telemetry data and telemetry signals. For scenario S1, the system assets include computer, server, Car PC, commands database, network, Control Area Network (CAN). The business assets in scenario S1 include control commands and control signals. Some of the business assets are similar for the different scenarios, however data supported in each scenario varies. For each of the business assets in the scenarios, we define security criteria in terms of Confidentiality, Integrity and Availability.

RQ3: What are the security risks in teleoperation scenarios and can they be mitigated? To answer this, we conducted risk analysis and assessment shown in Chapter 5. We search for risks to each defined system asset, which would negate security criteria. We discovered that the network and CAN are the system assets used in all three selected scenarios, and that the network had a higher number of threats. We rank the network threats using OWASP and select the three least explored threats in the high likelihood and high impact category. The threats selected are Router stack overflow, Man in The Middle attack and 5G replay. Since the method of execution of each specific attack is the same in all three scenarios, each specific threat is illustrated in one scenario using Security Risk Oriented Misuse Cases (SROMUC) to show vulnerabilities exploited for each attack and its impact. Security requirements are then elicited from misuse cases to mitigate presented risks.

The answers to the research questions for validation of architecture and security risk management are:

VRQ 1: How does the architecture presented in the thesis compare with published architecture of teleoperated vehicles in terms of completeness, comprehensiveness and intuitiveness? To answer this research question, we compared the architecture presented in the thesis with a peer reviewed article presenting an architecture of teleoperated vehicles using google forms. In the survey, the architecture in the thesis was

presented as Architecture 2 and the architecture in the peer-reviewed article was presented as Architecture 1. In terms of completeness and comprehensiveness, Architecture 2 is preferred to the architecture 1. However, in terms of intuitiveness, architecture 1 is preferred to architecture 2.

VRQ 2: How does the security risk management approach used in the thesis compare with published literature on security in teleoperated vehicles in terms of descriptiveness, specificity and uniqueness? To answer this research question, we use a questionnaire executed using google forms to compare the security risk approach presented in the thesis to a white paper addressing security risk management in teleoperated vehicles. The approach used in the thesis is presented as Option 1 and that in the white paper is presented as Option 2. In terms of descriptiveness and specificity, Option 1 is preferred to Option 2. For uniqueness, there was little similarity between the two options.

7.3 Future Work

In the future, the architecture of teleoperated vehicles needs to be expanded to take into account the current make-up of teleoperated vehicles used by car manufacturing companies. The thesis also only carries out security risk management for one of the three main components of teleoperated vehicles, that is, the network; hence, security risk management for the remote station and vehicle needs to be carried out. Further risks to the network and mitigation methods also need to be explored while taking into account the role played by advancing technology, such as artificial intelligence.

List of References

[1] AS/NZS 4360. Risk management guidelines: companion to as/nzs 4360:2004. *Standards Australia International Ltd Standards New Zealand*, 2004:1–131, 2004.

[2] Nessa Ahasanun. Privacy and cybersecurity challenges in vehicle teleoperation and mitigation approaches supported by apma v2x cybersecurity committee. 2022.

[3] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 88:10–28, 6 2017.

[4] Fatimah Alkhudhayr, Shouq Alfarraj, Buthina Aljameeli, and Salim Elkhidiri. *Information Security: A review of information security issues and techniques*. IEEE, 2019.

[5] M. M. Anwar, M. F. Zafar, and Z. Ahmed. A proposed preventive information security system. *The International Conference on Electrical Engineering*, 2007.

[6] Matteo Bassani and Sikha Bagui. A review of database attacks. *Transactions on Engineering and Computing Sciences*, 12:124–148, 6 2024.

[7] Kristian Beckers, Maritta Heisel, Bjornar Solhaug, and Ketil Stolen. Isms-coras: A structured method for establishing an iso 27001 compliant information security management system. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8431:315–344, 2014.

[8] Shuangqiang Chen, Yan Guang, and Qi Han. A review of backdoor control techniques for embedded devices. *ITCC 2024 - 2024 6th International Conference on Information Technology and Computer Communications, ITCC 2024*, pages 1–7, 1 2025.

[9] Michele Chinosi and Alberto Trombetta. Bpmn: An introduction to the standard. *Computer Standards Interfaces*, 34:124–134, 1 2012.

[10] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE Communications Surveys and Tutorials*, 18:2027–2051, 7 2016.

[11] Samantha Thomas Cruz. Information security risk assessment. *Information Security Management Handbook, Sixth Edition*, pages 243–250, 1 2007.

[12] Andreas Ekelhart, Stefan Fenz, and Thomas Neubauer. Aurum: A framework for information security risk management. *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*, 2009.

[13] Donald Firesmith. A reuse-based approach to determining security requirements. *Proceedings of the 9th international workshop on requirements engineering: foundation for software quality (REFSQ'03), Klagenfurt, Austria*, 6 2003.

[14] Fortinet. What is buffer overflow? attacks, types vulnerabilities | fortinet.

[15] The OWASP® Foundation. Buffer overflow | owasp foundation.

[16] Abhijit Gadekar, Sakshi Fulsundar, Prathamesh Deshmukh, Jaideep Aher, Kaajal Kataria, Dr Vibha Patel, and Dr Shivprakash Barve. Rakshak: A modular unmanned ground vehicle for surveillance and logistics operations. *Cognitive Robotics*, 3:23–33, 1 2023.

[17] Daniel Ganji, Haris Moutatidis, Christos Kalloniatis, and Saeed Malekshahi Gheytassi. Approaches to develop and implement iso/iec 27001 standard - information security management systems: A systematic literature review. *International Journal on Advances in Software vol 12 no 3 4*, 2019.

[18] Frank J. Jiang, Yulong Gao, Lihua Xie, and Karl H. Johansson. Human-Centered Design for Safe Teleoperation of Connected Vehicles. *IFAC-PapersOnLine*, 53(5):224–231, 1 2020.

[19] Grigorios Kakkavas, Kwame Nseboah Nyarko, Charbel Lahoud, David Kuhnert, Peter Kuffner, Matthias Gabriel, Shahab Ehsanfar, Maria Diamanti, Vasileios Karyotis, Klaus Mobner, and Symeon Papavassiliou. Teleoperated Support for Remote Driving over 5G Mobile Communications. *2022 IEEE International Mediterranean Conference on Communications and Networking, MeditCom 2022*, pages 280–285, 2022.

[20] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers Security*, 103:102150, 4 2021.

[21] Barbara Kitchenham. Kitchenham, b.: Guidelines for performing systematic literature reviews in software engineering. ebse technical report, 01, 2007.

[22] Pengyuan Lu, Kaustubh Sridhar, Oleg Sokolsky, Lin Zhang, Mengyu Liu, Fanxin Kong, Insup 2024 Lee, P Lu, L Zhang, K Sridhar, O Sokolsky, I Lee, ; M Liu, and F Kong. Recovery from adversarial attacks in cyber-physical systems: Shallow, deep, and exploratory works. *ACM Comput. Surv*, 56:31, 2024.

[23] Yuepin Lu, Tianxu Jin, Li Liu, and Chao Yang. Over-the-horizon teleoperation system for underground unmanned LHD. *2011 IEEE International Conference on Mechatronics and Automation, ICMA 2011*, pages 1804–1809, 2011.

[24] Sumbal Malik, Manzoor Ahmed Khan, and Hesham El-Sayed. CARLA: Car Learning to Act — An Inside Out. *Procedia Computer Science*, 198:742–749, 1 2022.

[25] Uday Mandhata, John Wagner, Fred Switzer, Darren Dawson, and Joshua Summers. A Customizable Steer-By-Wire Interface for Ground Vehicles. *IFAC Proceedings Volumes*, 43(7):656–661, 7 2010.

[26] Liviu Florin Manta, Dorin Popescu, Ovidiu Unguritu, Horatiu Roibu, Marius Marian, and Marian Abagiu. Software Architecture for a Mobile Robot designed for Rescue Missions Support in Hazardous Environments. *Proceedings of the 2020 21st International Carpathian Control Conference, ICCC 2020*, 10 2020.

[27] Johann M. Marquez-Barja, Seilendria Hadiwardoyo, Bart Lannoo, Wim Vandenberghe, Eric Kenis, Lauren Deckers, Maria Chiara Campodonico, Klaudia Dos Santos, Rakshith Kusumakar, Matthijs Klepper, and Joost Vandenbossche. Enhanced teleoperated transport and logistics: A 5G cross-border use case. *2021 Joint European Conference on Networks and Communications and 6G Summit, EuCNC/6G Summit 2021*, pages 229–234, 6 2021.

[28] Raimundas Matulevičius. Fundamentals of secure system modelling. *Fundamentals of Secure System Modelling*, pages 1–218, 8 2017.

[29] Raimundas Matulevičius, Nicolas Mayer, and Patrick Heymans. Alignment of misuse cases with security risk management. *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*, pages 1397–1404, 2008.

[30] Nicolas Mayer. Model-based management of information system security risk. 2009.

[31] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards Interfaces*, 29:244–253, 2 2007.

[32] Rodolfo Meneguette, Robson De Grande, J O Ueyama, Geraldo P Rocha Filho, Edmundo Madeira, Jo Ueyama, Geraldo P Rocha Filho, and ; G P Rocha Filho. Vehicular edge computing: Architecture, resource management, security, and challenges. *ACM Computing Surveys*, 55, 2021.

[33] James Mullins, Ben Horan, Mick Fielding, and Saeid Nahavandi. A haptically enabled low-cost reconnaissance platform for law enforcement. *SSRR2007 - IEEE International Workshop on Safety, Security and Rescue Robotics Proceedings*, 2007.

[34] Ingo Müller, Jun Han, Jean Guy Schneider, and Steven Versteeg. Idea: A reference platform for systematic information security management tool support. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6542 LNCS:256–263, 2011.

[35] Diego Narciandi-Rodriguez, Jose Aveleira-Mata, María Teresa García-Ordás, Javier Alfonso-Cendón, Carmen Benavides, and Héctor Alaiz-Moretón. A cybersecurity review in iot 5g networks. *Internet of Things*, 30:101478, 3 2025.

[36] The Object Management Group® (OMG®). Business process model notation™ (bpmn™) | object management group.

[37] International Standard Organisation. Iso 31000:2018 - risk management — guidelines.

[38] Minh Pham and Kaiqi Xiong. A survey on security attacks and defense techniques for connected and autonomous vehicles. *Computers Security*, 109:102269, 10 2021.

[39] James Pickford, Ireland Lee Harrison, Rasadhi Attale, Siraj Shaikh, Hoang Nga Nguyen, Lee Harrison, and Siemens Disw. Systematic risk characterisation of hardware threats to automotive systems. *ACM J. Auton. Transport. Syst. 1, 4, Article*, 18:36, 2024.

[40] Sampath Rajapaksha, Harsha Kalutarage, M Omar Al-Kadri, Garikayi Madzudzo, Madeline Cheah, M Omar Al-Kadri, and Andrei Petrovski. Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Comput. Surv*, 55, 2023.

[41] R. W. Saaty. The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling*, 9:161–176, 1 1987.

[42] Smit Saparia, Andreas Schimpe, and Laura Ferranti. Active safety system for semi-autonomous teleoperated vehicles. *IEEE*, 6 2021.

[43] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *Journal of Network and Computer Applications*, 149:102481, 1 2020.

[44] Guttorm Sindre and Andreas Opdahl. Templates for misuse case description. *Springer*, 12 2003.

[45] Florian Sommer, Mona Gierl, F Sommer, M Gierl, R Kriesten, Reiner Kriesten, and Frank Kargl. Article 16. sax. 2024. combining cyber security intelligence to refine automotive cyber threats. *Journal of the ACM*, 27, 2024.

[46] Stefan Neumeier, Nicolas Gay, Clemens Dannheim, and Christian Facchi. On the Way to Autonomous Vehicles Teleoperated Driving | VDE Conference Publication | IEEE Xplore, 2018.

[47] A. Sutcliffe. Scenario-based requirements engineering. *Proceedings of the IEEE International Conference on Requirements Engineering*, 2003-January:320–329, 2003.

[48] Tito Tang, Frederic Chucholowski, and Markus Lienkamp. Teleoperated driving basics and system design. *ATZ worldwide 2014 116:2*, 116(2):16–19, 1 2014.

[49] T. W. Van Den Berg, W. Huiskamp, and J. C. Van Den Heuvel. Unmanned vehicle control using simulation and virtual reality techniques. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, pages 895–900, 2001.

[50] Karl D. von Ellenrieder, Stephen C. Licht, Roberto Belotti, and Helen C. Henninger. Shared human–robot path following control of an unmanned ground vehicle. *Mechatronics*, 83:102750, 5 2022.

[51] Alan F T Winfield. Future directions in tele-operated robotics, 2009.

[52] Chuan Yu, Shuhui Chen, Qianqian Xing, and Ziling Wei. Protecting unauthenticated messages in lte/5g mobile networks: A two-level hierarchical identity-based signature (hibs) solution. *Computer Networks*, 254:110814, 12 2024.

[53] Yingshi Zheng, Mark J. Brudnak, Paramsothy Jayakumar, Jeffrey L. Stein, and Tulga Ersal. An Experimental Evaluation of a Model-Free Predictor Framework in Teleoperated Vehicles. *IFAC-PapersOnLine*, 49(10):157–164, 1 2016.

[54] Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. *A systematic approach to define the domain of information system security risk management*, pages 289–306. Springer Berlin Heidelberg, 2010.

Appendix

I. Glossary

AHP	Analytic Hierarchy Process
ASLR	Address Space Layout Randomization
BPMN	Business Process Model Notation
CAN	Controller Area Network
CIA	Confidentiality, Integrity, Availability
DNS	Domain Name Server
Dos	Denial of Service
ECU	Electronic Control Unit
GPS	Global Positioning System
IMSI	International Mobile Subscriber Identity
IMU	Inertia Measuring Unit
IP	Internet Protocol
ISSRM	Information System Security Risk Management
LIDAR	Light Detection And Ranging
LTE	Long Term Evolution
MiTM	Man in The Middle
MRQ	Main Research Question
OBU	On Board Unit
OWASP	Open Web Application Security Project
RADAR	Radio Detection And Ranging
RQ	Research Question
RTP	Real Time Transport Protocol
SEHOP	Structured Exception Handling Protection
SR	Security Requirement
SRM	Security Risk Management
SROMUC	Security Risk Oriented Misuse Cases
SSH	Secure Shell
UART	Universal Asynchronous Receiver Transmitter
UAV	Unmanned Ariel Vehicles
UDP	User Datagram Protocol
UGV	Unmanned Ground Vehicles
UML	Unified Modelling Language
VPN	Virtual Private Network
VR	Virtual Reality
WAN	Wide Area Network

II. Background

This section shows relationship between functional layers and information processing functions.

Table 15. A link between functional layers and information processing functions adapted from [28]

Functionality decomposition layers	**Information processing functions**
User interaction	Capturing information through input ports Displaying information through output ports
Data / storage management	Storing information using data structures, database systems, file systems Retrieving information using database systems, file systems
Resource management	Manipulating information using needed and allocated resources, avoiding deadlocks, having correct data configurations
Distribution management	Manipulating information through defined interfaces between different components at different levels of abstraction
Communication	Transmitting information using messages, protocols, and network infrastructures
Addressing	Manipulating information through identifiable and reachable components

III. Architecture

This section presents tables showing extraction of data from papers selected from the systematic literature review and quality assessment results used for paper selection. The data is extracted basing on the three different components of teleoperated vehicles: The vehicle, the network and the remote station.

Table 16. Information extraction table

Paper	Vehicle components	Network components	remote station components
Kakkavas *et al.* [19]	Camera Antennae On Board Unit AEK- Gnss device Remote operations Centre Gateway Router Sensors LIDAR RADAR IMU MATLAB Application	Local mesh network	Remote Operations Centre Monitor Keyboard Gps Antennae VPN
Neumeier *et al.* [46]	Modem Car PC ECU Physical Buses HMI Cellular network technology Camera Sensors Actuators Application Physical Bus Drivers	WAN Video stream processing Data Conditioning and streaming Communication link layer System monitoring	Teleoperation server Control devices (steering wheel, pedals, Microphone) Cameras
Berg *et al.* [49]	Sensors GPS Remote link Computer Interface Actuators	Real Time control system Actuator control vehicle status data acquisition, vehicle localization path tracking	Virtual reality and simulation TV

Table 17. Information extraction table cont

Lu *et al.* [23]	Positioning and Communication system Master Computer Implementation computer Executive devices Cameras	Signal acquisition controller Button function module. Handle fuction module Pedal function module	Buttons Handle Host Computer Pedals
Gadekar *et al.* [16]	GPS Antennae Onboard Unit Cameras LIDAR Sensors IMU Raspbian OS	UART communication protocol I2C communication protocol. SSH client Jetson Nano	Mobile application
Ellenreider *et al.* [50]	GPS GNC Wireless modem Cameras	-	Laptop Handheld remote control Force reflexive joystick
Tang *et al.* [48]	Cameras PC EPS	LTE – network UDP- based protocol	Steering wheel Pedals Monitor

Table 18. Quality assessment table

Criteria	Mentions particular vehicle	Type of vehicle is a ground vehicle	Describes architecture and vehicle components	Describes teleoperation system	Total
Kakkavas *et al.* [19]	4	5	5	4	19
Marquez *et al.* [27]	0	0	1	0	1
Neumeier *et al.* [46]	5	5	5	5	20
Berg *et al.* [49]	4	4	3	0	11
Manta *et al.* [26]	2	2	2	1	7
Lu *et al.* [23]	4	4	3	4	15
Mullins *et al.* [33]	2	2	1	2	7
Mandhata *et al.* [25]	0	5	2	2	9
Gadekar *et al.* [16]	4	5	5	3	17
Malik *et al.* [24]	0	1	2	1	4
Zheng *et al.*[53]	0	2	2	4	8
Ellenrieder *et al.* [50]	4	2	4	1	11
Jiang *et al.* [18]	2	4	0	2	8
Tang *et al.* [48]	4	4	4	4	16

IV. Scenarios

This section shows the selected scenarios presented using use case templates.

Table 19. Usecase for S4 connect remote station to vehicle

Use Case ID:	S4		
Use Case name:	Connect remote station to vehicle		
Created By:	Aqel Rizza	Last Updated by	Aqel Rizza
Date Created:	21/02/2025	Date Updated	13/03/2025

Actors:	Teleoperator, Application, Server, N/W, Car PC
Description:	The teleoperator initiates this function when there is need to establish a connection to the vehicle
Trigger:	The need to operate the vehicle remotely
Preconditions:	Teleoperator is registered in the system
Post Conditions:	The vehicle transmits current state data back to the to the remote station
Normal Flow:	1. The teleoperator starts computer 2. The computer displays login screen 3. The teleoperator inputs login data and logs into system 4. The teleoperator connects computer to server 5. The server initiates internet connection using router or modem 6. The network provides network configuration details (IP address, gateway (router's IP), and DNS) to server and establishes internet connection. 7. The server provides resources(Real time data processing, Computing power, RAM, storage, bandwidth, user access, remote control interface) to computer to run application 8. The computer runs application 9. The network sends network configuration details to Car PC
Alternative flow:	-
Exceptions:	-
Priority :	High
Frequency of use:	Whenever need arises
Assumptions:	The vehicle is already connected to the internet Connection to the server initates the sending of network configuration details to the vehicle.

Table 20. Send telemetry data from vehicle use case

Use Case ID:	S3		
Use Case name:	Send Telemetry data from vehicle		
Created By:	Aqel Rizza	Last Updated by	Aqel Rizza
Date Created:	24/02/2025	Date Updated	13/03/2025

Actors:	On Board Unit, Sensors, Car PC, Network, Server, Computer
Description:	The vehicle initiates this function to display vehicle environment to the teleoperator.
Trigger:	Turning on of Car PC
Preconditions:	The Sensors and On Board Unit collect data
Post Conditions:	The computer displays telemetry data
Normal Flow:	1. The On Board Unit and sensors transmit ambient and sensory data respectively to the CAN. 2. The CAN sends the telemetry data to the Car PC (encoded and packaged) 3. The Car PC converts the telemetry data into telemetry signals and sends telemetry signals over the network to the server. 4. The server converts telemetry signals into sends telemetry data which is sent to the computer 5. The computer displays telemetry data. 6. The teleoperator views telemetry data
Alternative flow:	-
Exceptions:	-
Priority :	High
Frequency of use:	Whenever need arises
Assumptions:	The sensory and ambient data is transmitted together as telemetry data.

Table 21. Use case for S1

Use Case ID:	S1		
Use Case name:	Control vehicle		
Created By:	Aqel Rizza	Last Updated by	Aqel Rizza
Date Created:	24/02/2025	Date Updated	13/02/2025

Actors:	Teleoperator, Control devices, Server, N/W, Car PC, ECU, actuator
Description:	The teleoperator initiates this function when there is need to control the vehicle.
Trigger:	The need to take control of vehicle
Preconditions:	The teleoperator analyses telemetry data
Post Conditions:	The vehicle speed increases and vehicle moves or the vehicle speed reduces and vehicle stops
Normal Flow:	1. The teleoperator analyses telemetry data 2. The teleoperator uses control buttons to issue drive commands (acceleration and steering). 3. The acceleration and steering commands are sent to the server. 4. The server converts commands into control signals that can be transmitted over the network 6. The server sends control signals(control commands) over network to Car PC 7. The Car PC decodes the control signals and sends control commands to ECU 8. The ECU controls acceleration actuators
Alternative flow:	2. the teleoperator uses control buttons to issue brake command
Exceptions:	-
Priority :	High
Frequency of use:	Whenever need arises
Assumptions:	Both the drive and brake command include a steering command whenever necessary

V. Security Criteria

This section shows the definition of security criteria for the business assets in the selected scenarios presented using Use case diagrams.

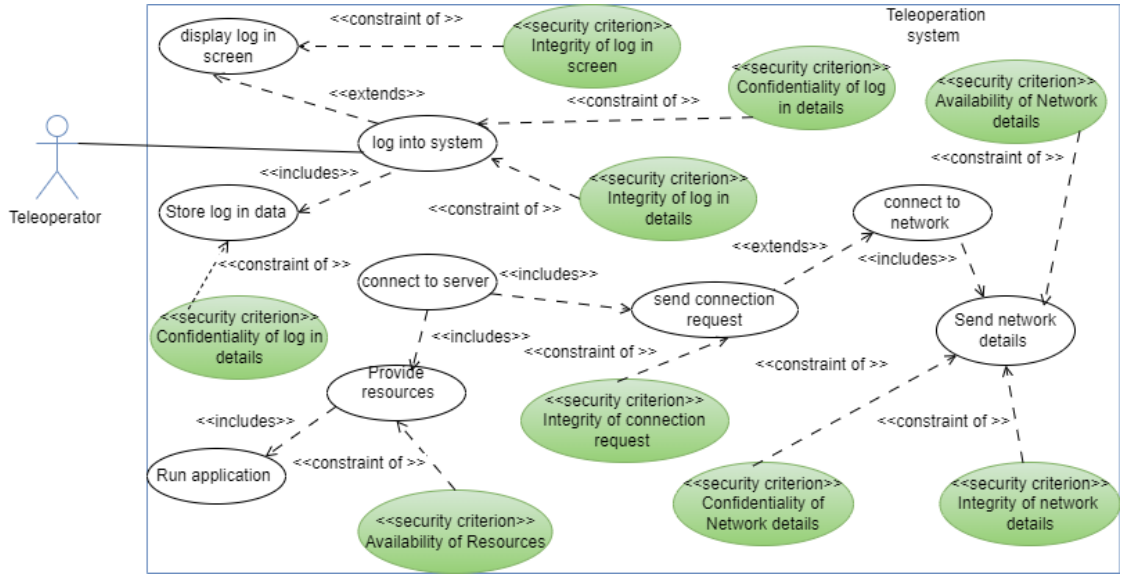


Figure 22. Security criteria for connect to vehicle **S4**

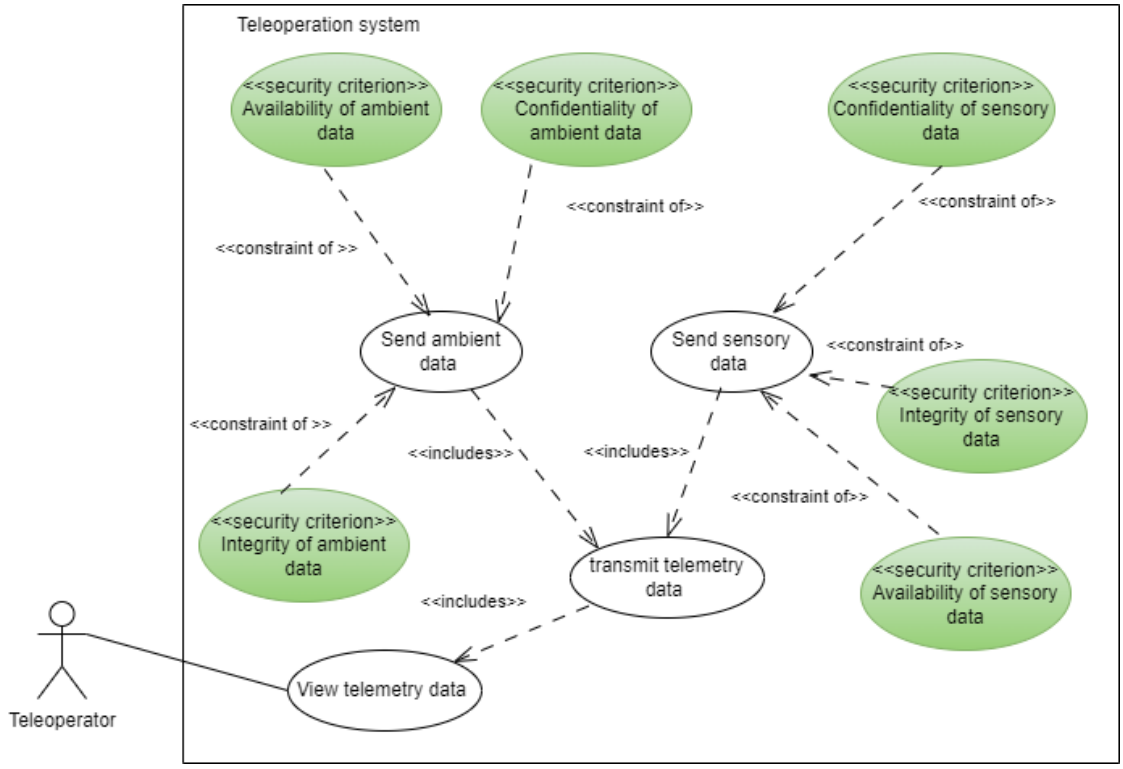


Figure 23. Security criteria for ambient and sensory data in **S3**

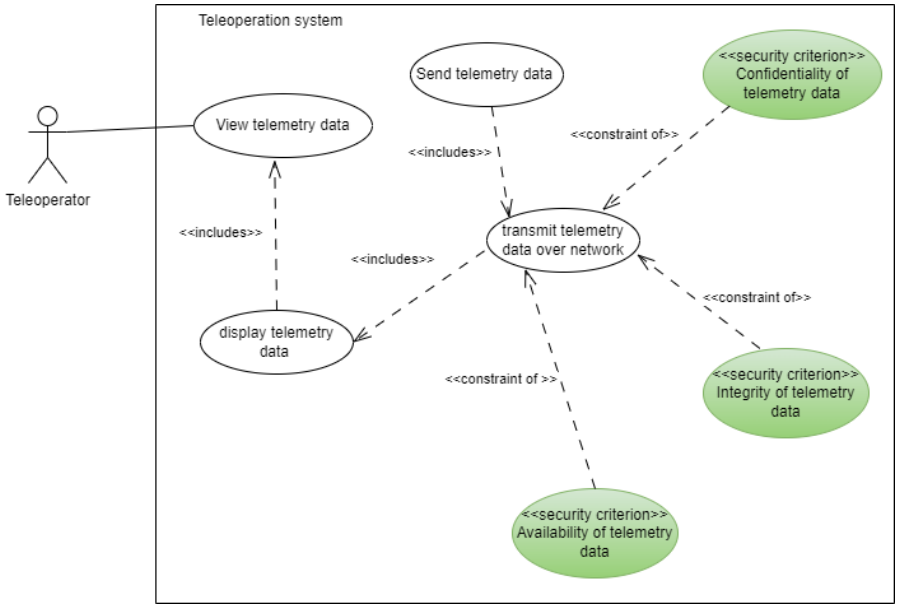


Figure 24. Security criteria for transmit telemetry data in **S3**

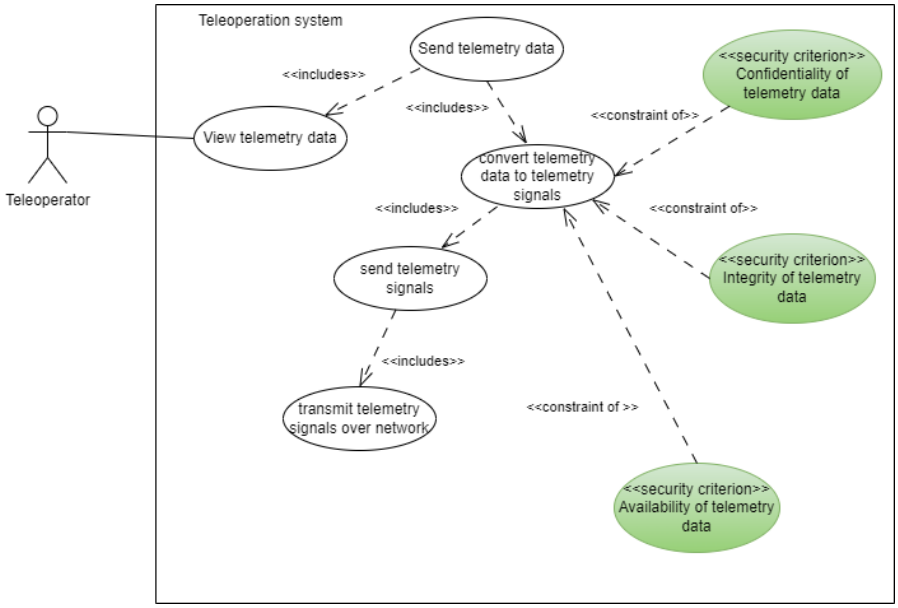


Figure 25. Security criteria for convert telemetry data to telemetry signals in **S3**

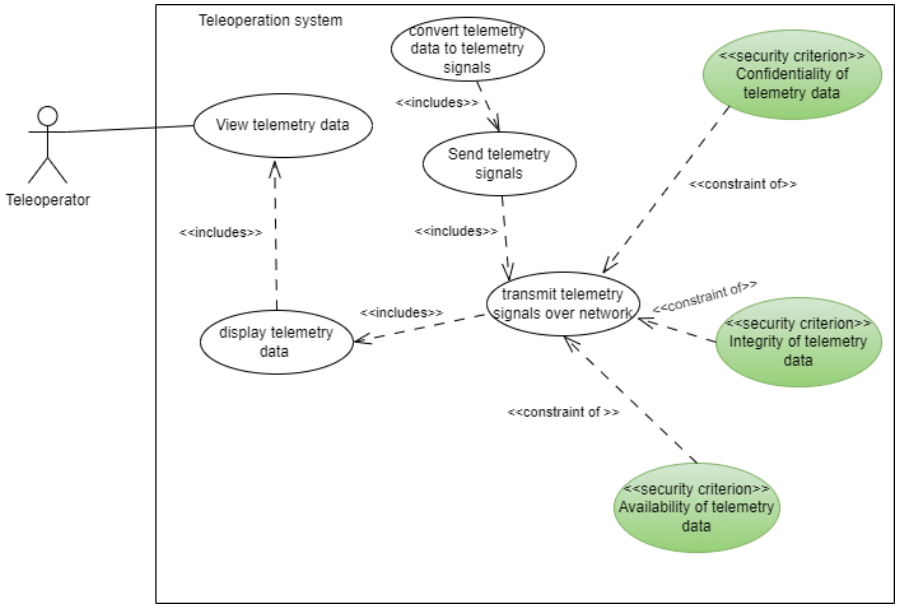


Figure 26. Security criteria for transmit telemetry signals in **S3**

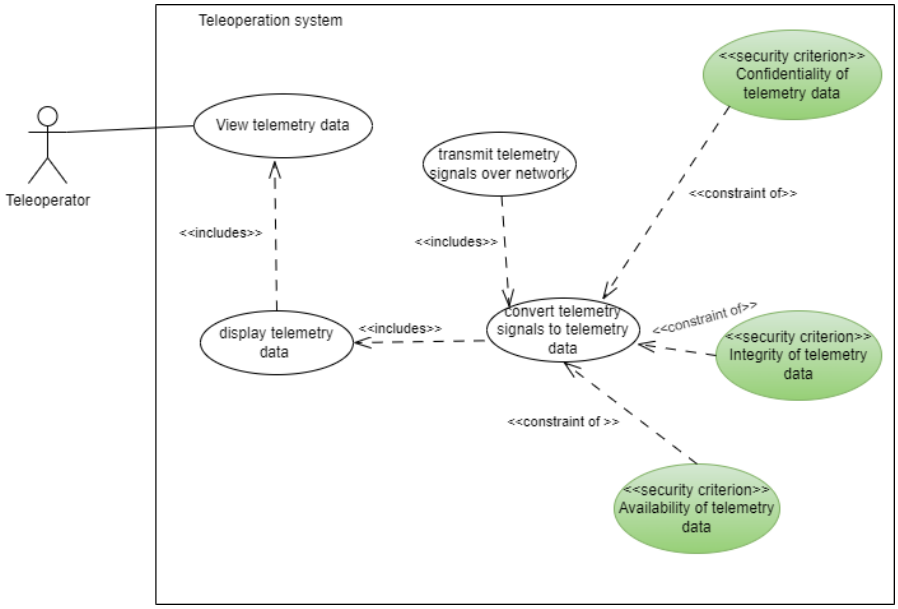


Figure 27. Security criteria for convert telemetry signals to telemetry data in **S3**

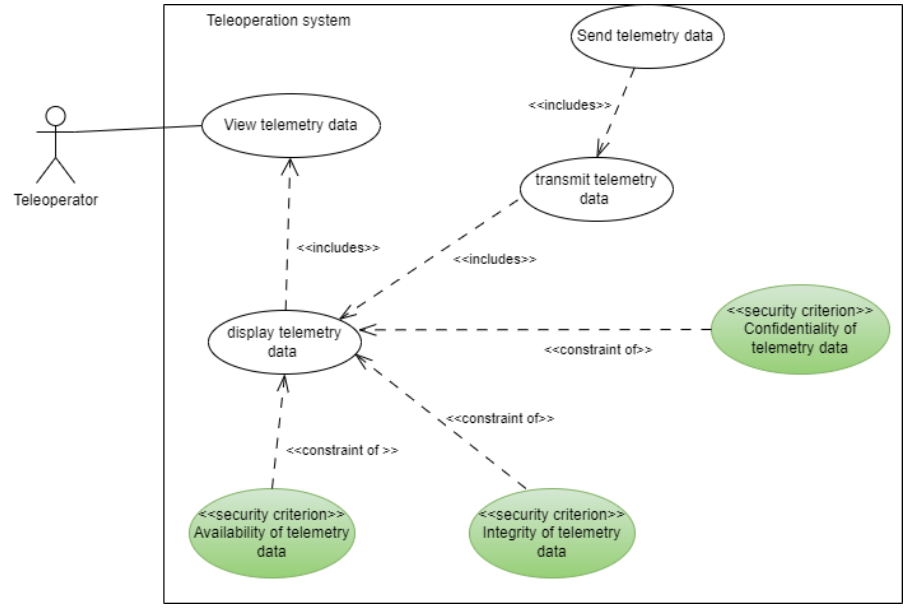


Figure 28. Security criteria for display telemetry data in **S3**

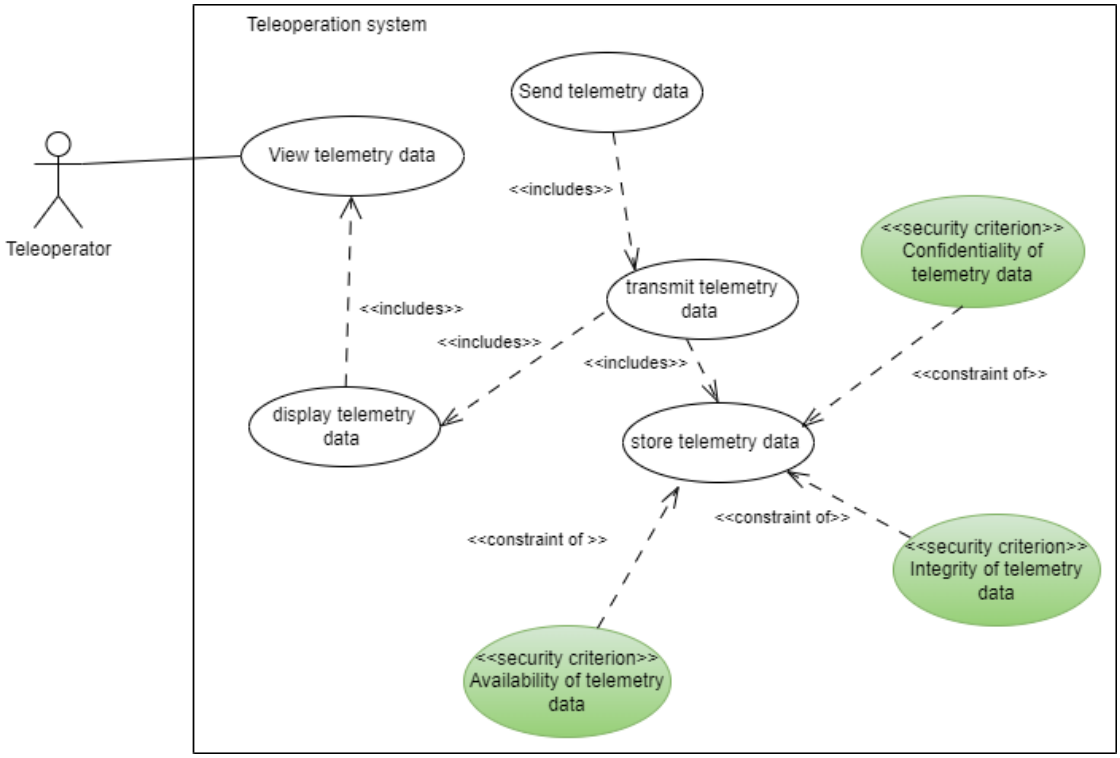


Figure 29. Security criteria for store telemetry data in **S3**

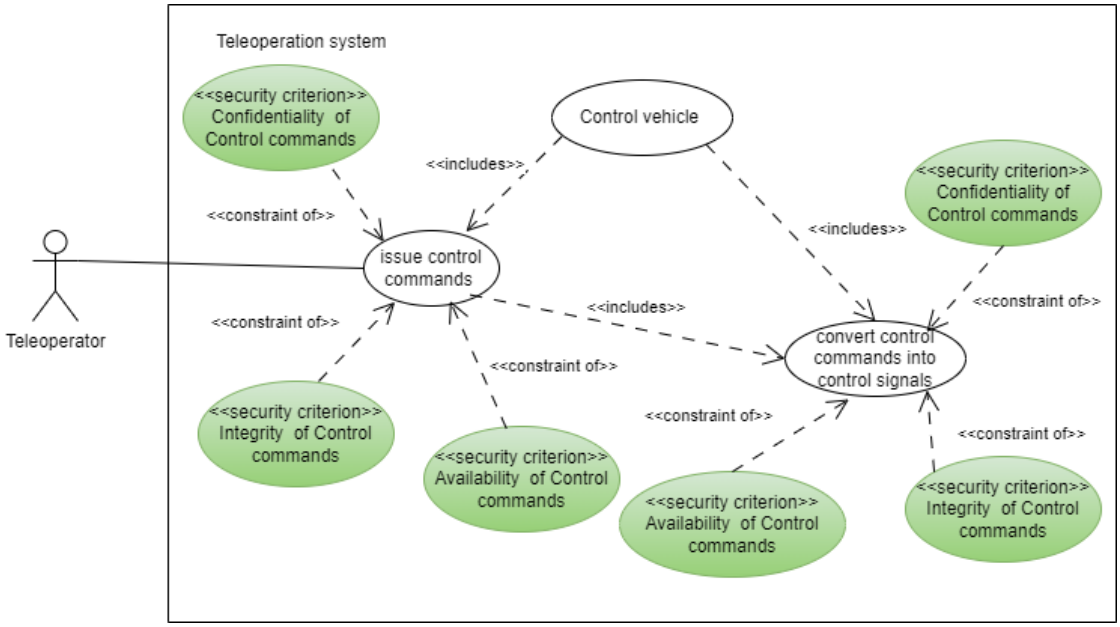


Figure 30. Security criteria for issue control commands in **S1**

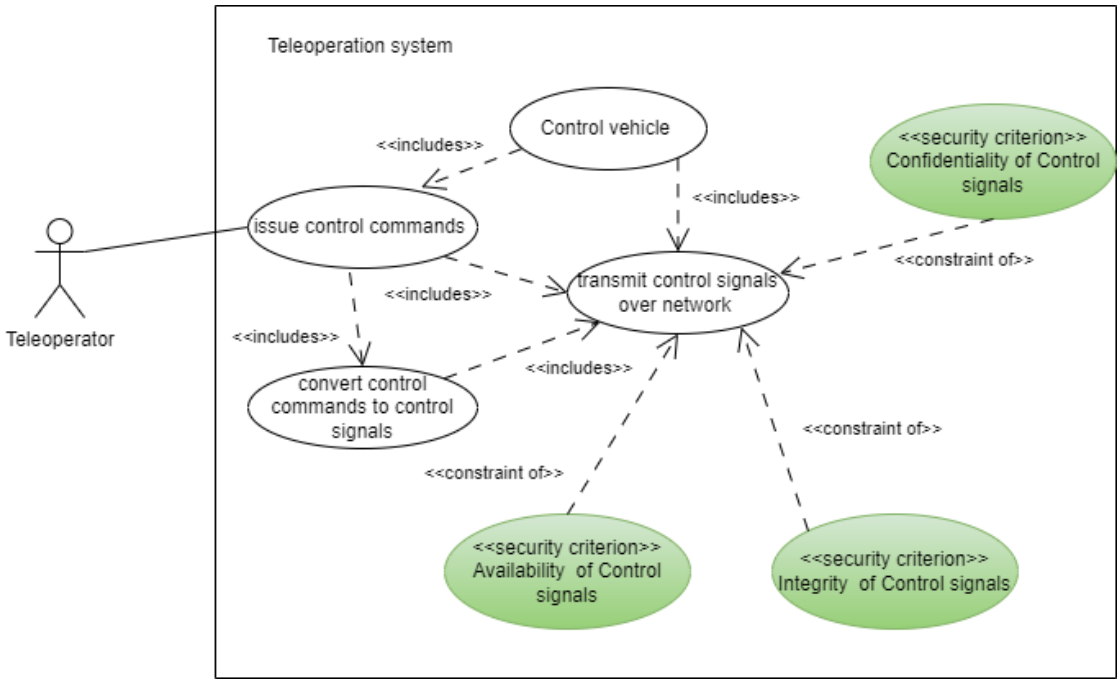


Figure 31. Security criteria for issue transmit control commands over network in **S1**

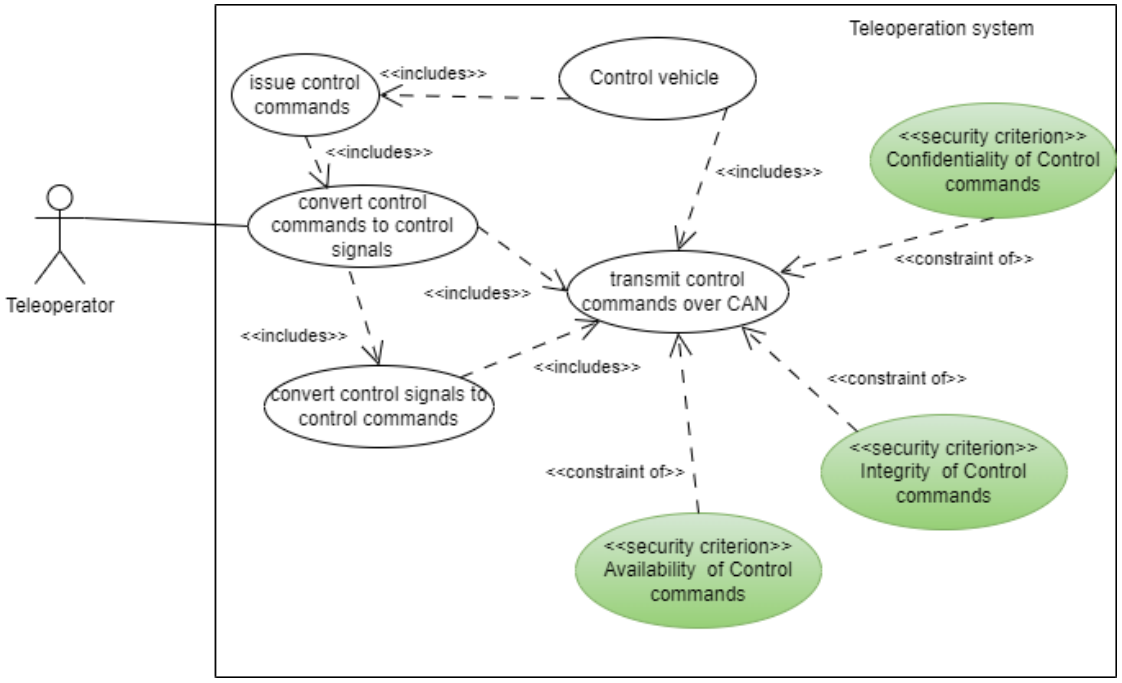


Figure 32. Security criteria for issue transmit control commands over CAN in **S1**

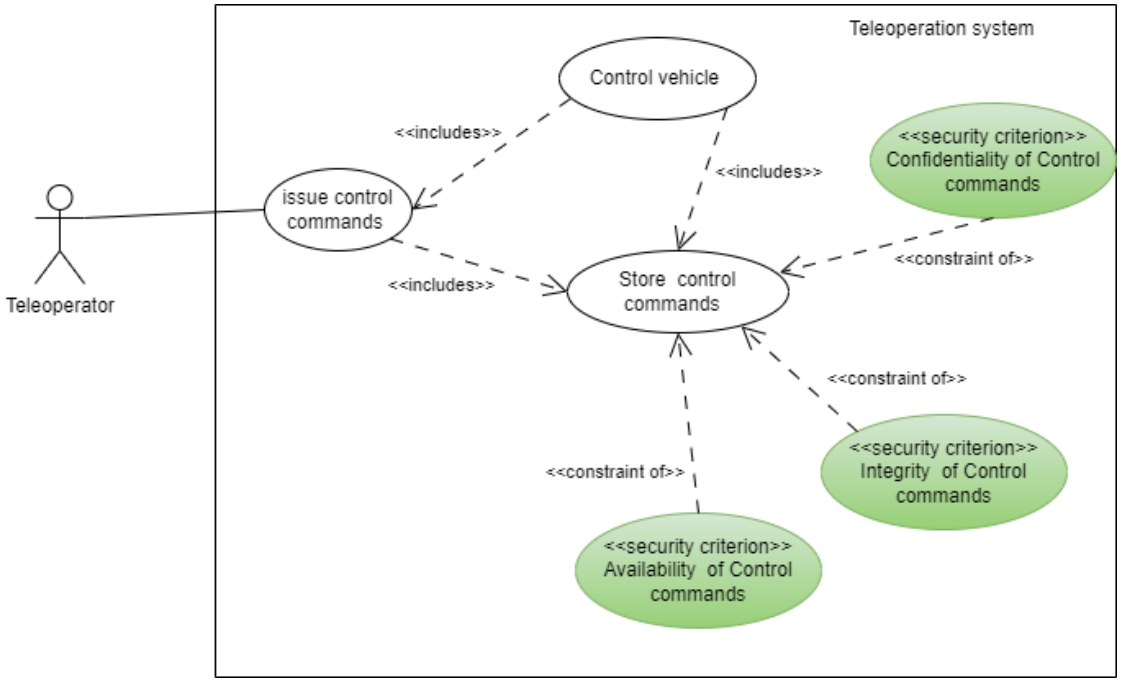


Figure 33. Security criteria for store control commands in **S1**

VI. AHP Process

This section shows the stages for the Analytic Hierarchy Process for Importance and Impact criteria.

Table 22. Step 1: Filling in values for importance criteria

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S1	1	9	1	1	8	9	8	9	9	8
S2	1/9	1	1/9	1	2	1/2	1	5	7	2
S3	1	9	1	1	8	9	9	9	9	8
S4	1	1	1	1	9	8	8	9	9	8
S5	1/8	½	1/8	1/9	1	1/2	1/2	1/2	2	1
S6	1/9	2	1/9	1/8	2	1	1	2	3	2
S7	1/8	1	1/8	1/8	2	1	1	3	5	4
S8	1/9	1/5	1/9	1/8	2	1/2	1/3	1	2	2
S9	1/9	1/7	1/9	1/9	1/2	1/3	1/5	1/2	1	1/2
S10	1/8	½	1/9	1/8	1	1/2	1/4	1/2	2	1

Table 23. Step 2: Table showing summation of columns for importance criteria

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S1	1	9	1	1	8	9	8	9	9	8
S2	1/9	1	1/9	1	2	1/2	1	5	7	2
S3	1	9	1	1	8	9	9	9	9	8
S4	1	1	1	1	9	8	8	9	9	8
S5	1/8	½	1/8	1/9	1	1/2	1/2	1/2	2	1
S6	1/9	2	1/9	1/8	2	1	1	2	3	2
S7	1/8	1	1/8	1/8	2	1	1	3	5	4
S8	1/9	1/5	1/9	1/8	2	1/2	1/3	1	2	2
S9	1/9	1/7	1/9	1/9	1/2	1/3	1/5	1/2	1	1/2
S10	1/8	½	1/9	1/8	1	1/2	1/4	1/2	2	1
SUM	**3.819**	**24.343**	**3.806**	**4.722**	**35.5**	**30.333**	**29.283**	**39.5**	**49**	**36.5**

VII. Risk Definition

This section shows the identification of threats to each system asset in the selected scenarios and the number of papers that exist for the critical threats to the Network.

Table 24. Step 3: Table showing normalisation of each column and averages of each row for importance criteria

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	**AVE**
S1	0.262	0.37	0.263	0.213	0.225	0.297	0.273	0.228	0.184	0.219	**0.253**
S2	0.029	0.041	0.029	0.213	0.056	0.016	0.034	0.127	0.143	0.055	**0.074**
S3	0.262	0.37	0.263	0.213	0.225	0.297	0.307	0.228	0.184	0.219	**0.257**
S4	0.262	0.041	0.263	0.213	0.254	0.264	0.273	0.228	0.184	0.219	**0.220**
S5	0.033	0.021	0.033	0.024	0.028	0.016	0.017	0.013	0.041	0.027	**0.025**
S6	0.029	0.082	0.029	0.026	0.056	0.033	0.034	0.051	0.061	0.055	**0.046**
S7	0.033	0.041	0.033	0.026	0.056	0.033	0.034	0.076	0.102	0.110	**0.054**
S8	0.029	0.008	0.029	0.026	0.056	0.016	0.011	0.025	0.041	0.055	**0.030**
S9	0.029	0.006	0.029	0.024	0.014	0.011	0.007	0.013	0.020	0.014	**0.017**
S10	0.033	0.021	0.029	0.026	0.028	0.016	0.009	0.013	0.041	0.027	**0.024**
SUM	**3.819**	**24.343**	**3.8**	**4.72**	**35.5**	**30.33**	**29.28**	**39.5**	**49**	**36.5**	

Table 25. Step 1: Table showing the filled value for impact criteria

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S1	1	7	1	1	8	6	8	9	9	7
S2	1/7	1	1/9	1/9	3	1/2	1/3	3	4	2
S3	1	9	1	1	8	7	8	9	9	8
S4	1	9	1	1	8	8	9	9	9	9
S5	1/8	1/3	1/8	1/8	1	1/3	2	4	7	1
S6	1/6	2	1/7	1/8	3	1	2	7	8	4
S7	1/8	3	1/8	1/9	1/2	1/2	1	5	8	1/2
S8	1/9	1/3	1/9	1/9	1/4	1/7	1/5	1	2	1/4
S9	1/9	1/4	1/9	1/9	1/7	1/8	1/8	1/2	1	1/7
S10	1/7	1/2	1/8	1/9	1	1/4	2	4	7	1

Table 26. Step 2: Table showing summation of columns for impact criteria

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
S1	1	7	1	1	8	6	8	9	9	7
S2	1/7	1	1/9	1/9	3	1/2	1/3	3	4	2
S3	1	9	1	1	8	7	8	9	9	8
S4	1	9	1	1	8	8	9	9	9	9
S5	1/8	1/3	1/8	1/8	1	1/3	2	4	7	1
S6	1/6	2	1/7	1/8	3	1	2	7	8	4
S7	1/8	3	1/8	1/9	1/2	1/2	1	5	8	1/2
S8	1/9	1/3	1/9	1/9	1/4	1/7	1/5	1	2	1/4
S9	1/9	1/4	1/9	1/9	1/7	1/8	1/8	1/2	1	1/7
S10	1/7	1/2	1/8	1/9	1	1/4	2	4	7	1
SUM	**3.925**	**32.42**	**3.85**	**3.81**	**32.89**	**23.85**	**32.66**	**51.5**	**64**	**32.89**

Table 27. Step 3: Normalisation of impact table

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	AVE
S1	0.255	0.216	0.26	0.263	0.243	0.252	0.245	0.175	0.141	0.213	**0.226**
S2	0.036	0.031	0.029	0.029	0.091	0.021	0.010	0.058	0.062	0.061	**0.043**
S3	0.255	0.278	0.26	0.263	0.243	0.293	0.245	0.175	0.141	0.243	**0.24**
S4	0.255	0.278	0.26	0.263	0.243	0.335	0,276	0.173	0.141	0.274	**0.224**
S5	0.032	0.010	0.032	0.033	0.030	0.014	0.061	0.078	0.109	0.030	**0.043**
S6	0.042	0.062	0.037	0.033	0.091	0.419	0.061	0.136	0.125	0.122	**0.113**
S7	0.032	0.093	0.032	0.029	0.015	0.021	0.031	0.097	0.125	0.015	**0.049**
S8	0.028	0.010	0.029	0.029	0.008	0.006	0.006	0.019	0.031	0.008	**0.017**
S9	0.028	0.008	0.029	0.029	0.004	0.005	0.004	0.010	0.016	0.004	**0.014**
S10	0.036	0.015	0.032	0.029	0.030	0.010	0.061	0.078	0.109	0.030	**0.043**
SUM	**3.925**	**32.42**	**3.85**	**3.81**	**32.89**	**23.85**	**32.66**	**51.5**	**64**	**32.89**	

Table 28. Table showing threats

Scenario	Component	Source	Risk ID	Threat
S4 S3	Computer Server Sensors (All) Car PC CAN Network	[35, 45, 20, 38, 40]	R1	Spoofing
S4 S3 S1	Computer Car PC	[43]	R2	Unauthorised access
S4 S3 S1	Computer Server	[43]	R3	Data leakage
S4	Computer	[8]	R4	Forward listening
S4	Computer Server	[8]	R5	Reverse connection
S4	Server Car PC Network	[35]	R6	Information disclosure
S4	server	[45]	R7	Resource location spoofing
S4 S3	Server Car PC CAN	[39]	R8	Protocol manipulation
S4	Computer	[35]	R9	Tampering
S4	Computer	[35]	R10	Repudiation
S4	Computer Database	[35, 6]	R11	Elevation of privilege
S3	On Board Unit	[39]	R12	Jamming
S3	On Board Unit	[3]	R13	Congestion
S3	On Board Unit	[32]	R14	Malware
S3	Sensors (all)	[3]	R15	Modification /fabrication
S3	Lidar Radar GPS	[8]	R16	Side channel attacks

Table 29. Table showing threats cont

S3	Lidar Radar CAN Network Database	[3, 45, 6]	R17	Dos
S3	Camera	[39]	R18	Camera blinding
S3	Camera	[38, 39]	R19	Adversarial image
S3	Camera	[43]	R20	Device scanning
S3 S1	CAN Network	[38, 45, 20, 3]	R21	Eavesdropping
S3 S1	CAN	[38, 45, 40]	R22	Falsifying
S3 S1	CAN	[20, 38, 40]	R23	Packet sniffing
S3 S1	CAN	[38, 20, 45]	R24	Fuzzing
S3 S1	CAN	[45]	R25	Communication channel manipulation
S4 S3 S1	CAN NetWork	[45, 10]	R26	man in the middle (MiTM)
S3 S1	CAN	[45]	R27	Traffic injection
S4 S3 S1	CAN Network	[45]	R28	Flooding
S3 S1	CAN	[45]	R29	Excessive allocation
S3 S1	CAN	[40, 39]	R30	Masquerade attack/ impersonation
S3 S1	CAN	[45]	R31	Resource injection
S3 S1	Network	[35]	R32	Bidding down attack

Table 30. Table showing threats cont

S4 S3 S1	Network	[35, 38, 43, 45]	R33	5G replay
S4 S3 S1	Network	[35]	R34	IMSI catchers
S4 S3 S1	Network	[35, 43]	R35	Radio interference attack
S4 S3 S1	Network	[43, 5]	R36	Worm hole attack
S4 S3 S1	Network	[45, 5, 39]	R37	Black hole attack
S4 S3 S1	Network	[43]	R38	Selective forwarding
S4 S3 S1	Network	[43]	R39	Routing Information attacks
S4 S3 S1	Network	[8, 45]	R40	Active activation attacks / packets listening
S4 S3 S1	Network	[32]	R41	Spamming
S4 S3 S1	Network	[32]	R42	Timing attack
S3 S4	Network	[35]	R43	Router Stack overflow
S4 S3 S1	Network	[35]	R44	Bootstrapping attack

Table 31. Table showing threats cont

S4 S3 S1	Computer	[45]	R45	Command injection
S4 S3 S1	Database	[6]	R46	SQL injection
S4 S3 S1	Database	[6]	R48	Cross site scripting

Table 32. Table showing number of papers existing on critical threats

	MiTM	Routing information	Router stack overflow	Bootstrapping	5G replay	Dos
Science direct	2,012	55,812	1,526	3,059	1,392	28,524
Scopus	1,082	2,930	5	143	87	9122
IEEE	522	4,814	1	296	189	7,393
ACM	1,310	16,209	1,185	2,186	625	58,759
Total	4,926	79,765	2,717	5,684	2,293	103,798

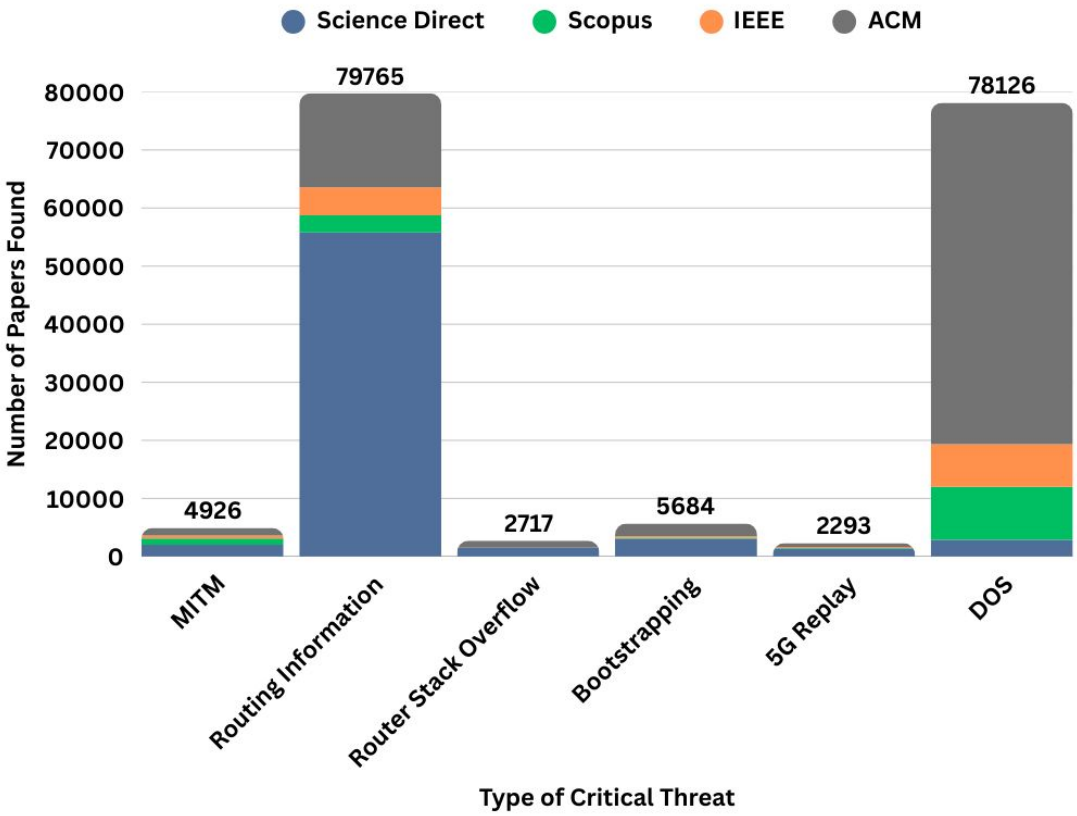


Figure 34. Graph showing the number of papers on each critical threat

VIII. Risk Analysis

This section shows the analysis of selected risks in the different scenarios selected, presented using Security Risk Oriented Misuse Cases. The section illustrates how the selected threats would occur in different scenarios, besides the ones illustrated in the thesis, such as Router Stack Overflow in Scenario 3 (S3) and the impact of the risks on defined security criteria.

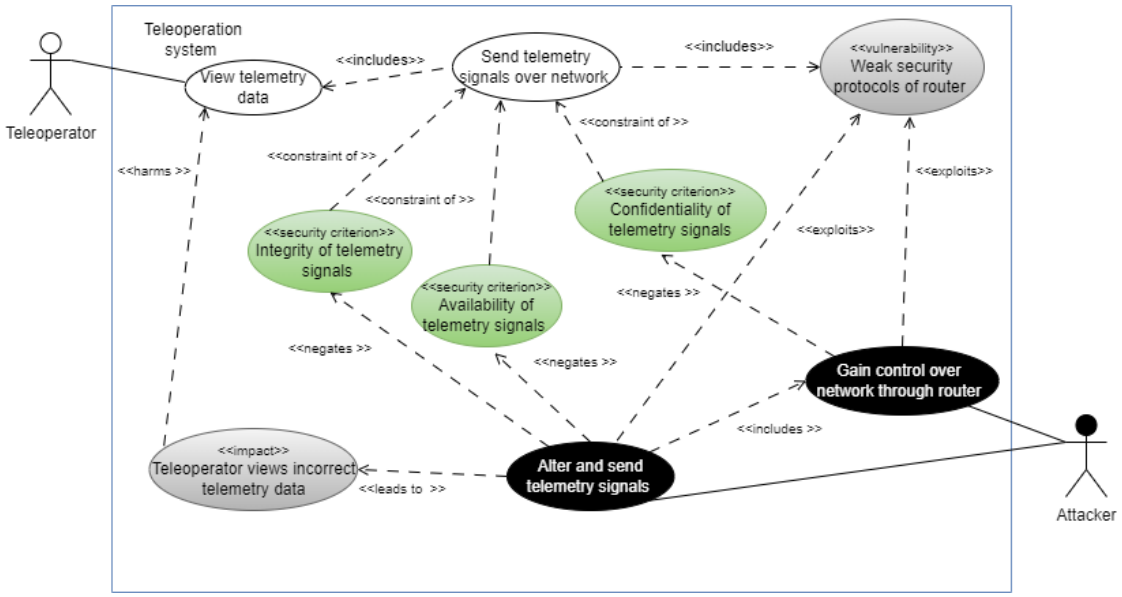


Figure 35. Misuse case showing router stack overflow for scenario S3

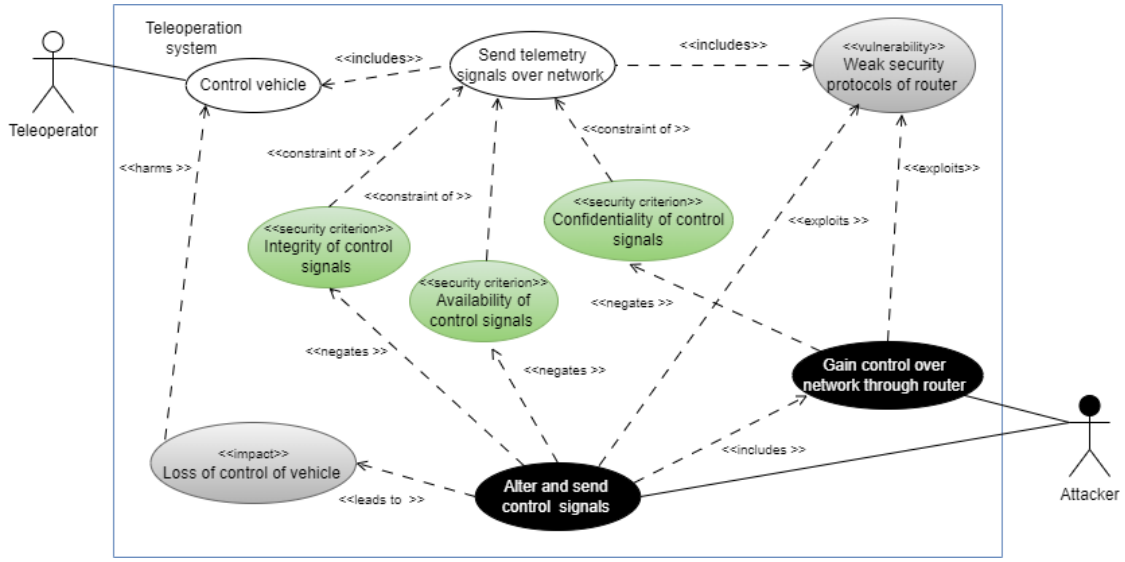


Figure 36. Misuse case showing router stack overflow for scenario S1

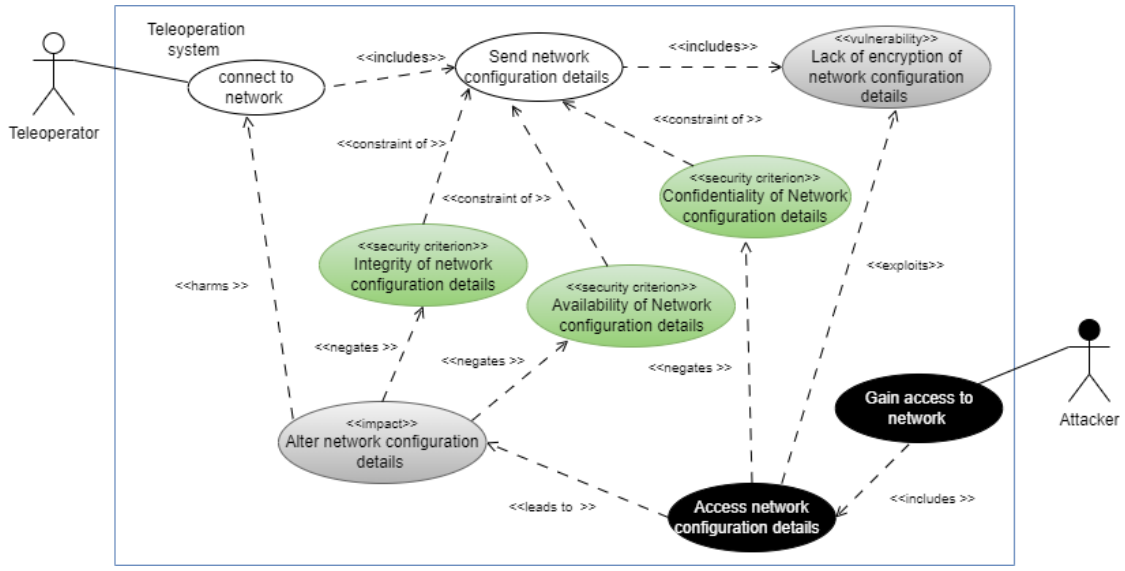


Figure 37. Misuse case 1 showing MiTM for scenario S4

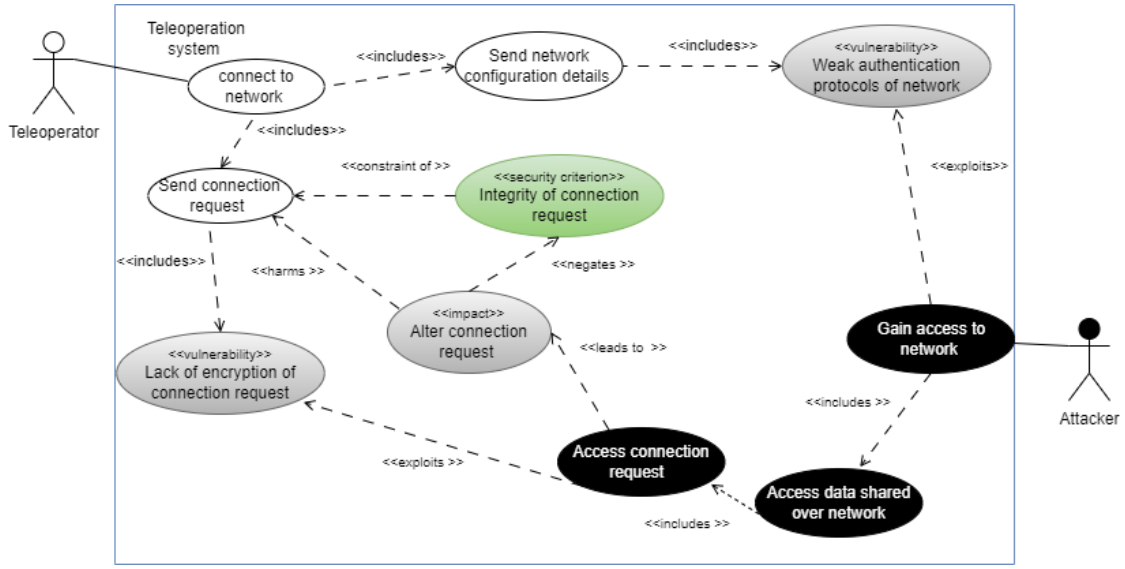


Figure 38. Misuse case 2 showing MiTM for scenario S4

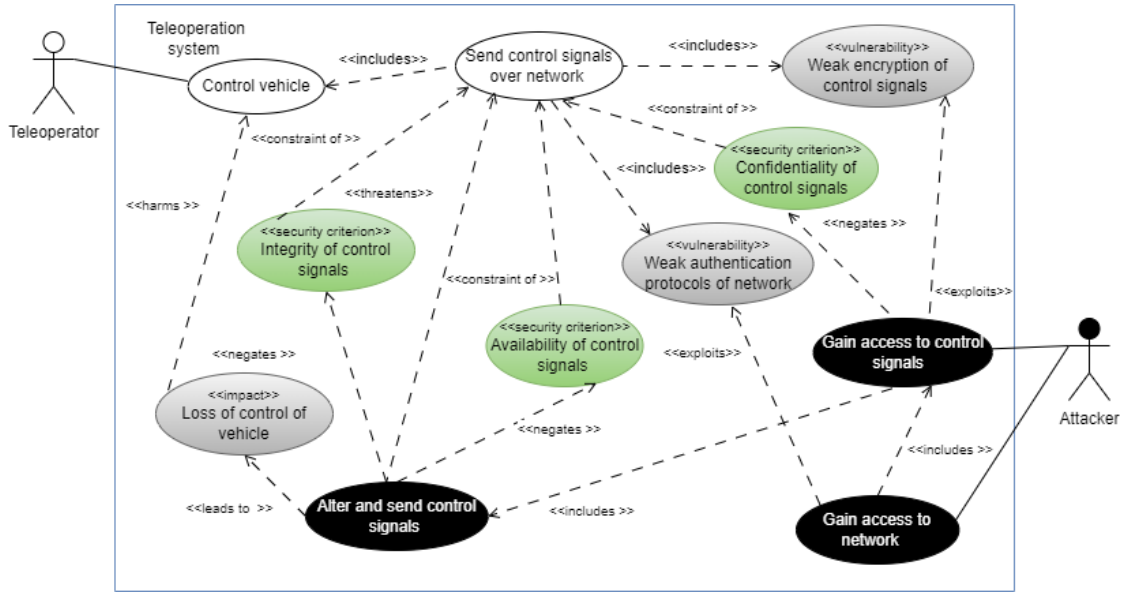


Figure 39. Misuse case showing MiTM for scenario S1

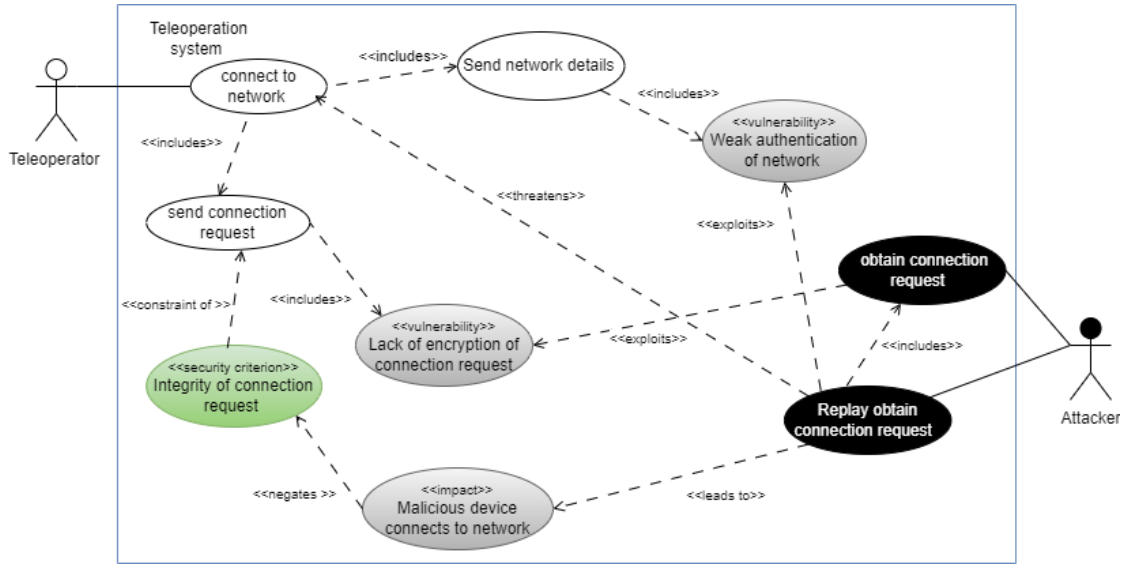


Figure 40. Misuse case showing 5G replay 1 in scenario S4

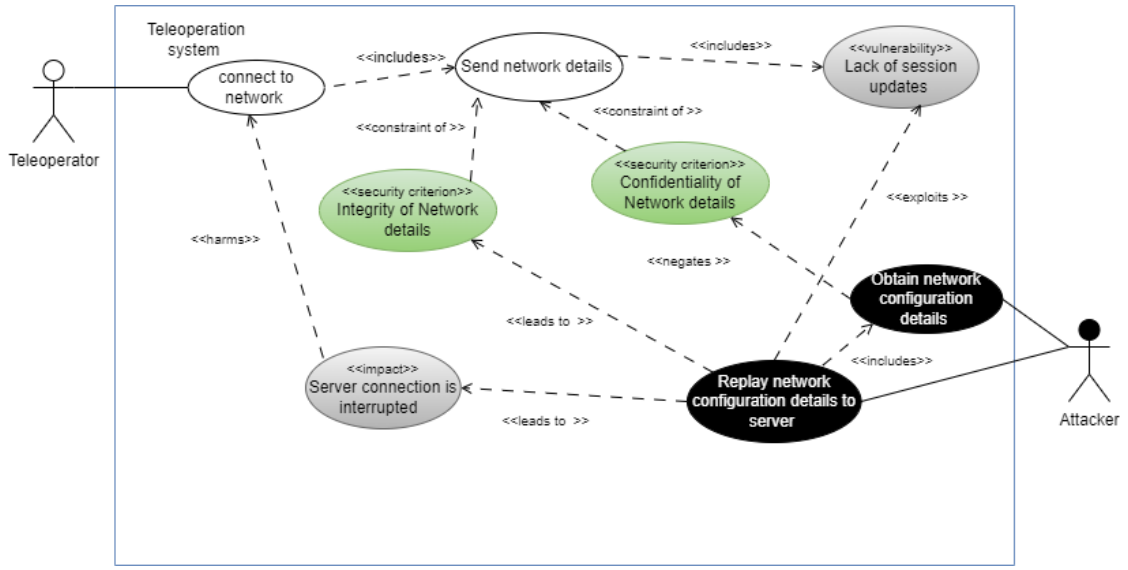


Figure 41. Misuse case 2 showing 5G replay 2 in scenario S4

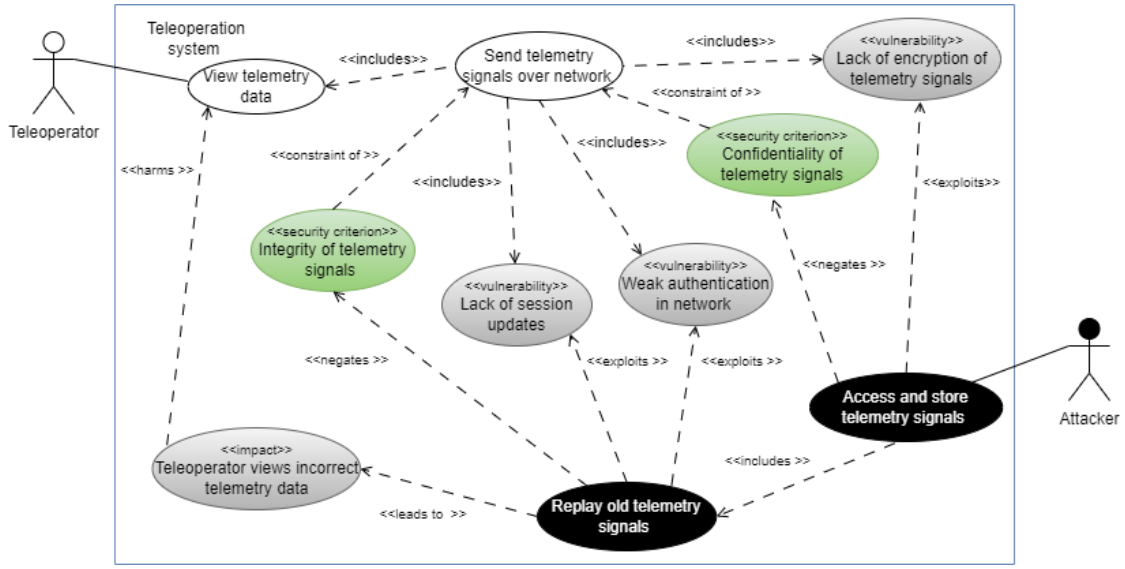


Figure 42. Misuse case showing 5G replay for scenario S3

IX. Risk Treatment

This section shows the Risk Treatment for the analysed risks in Section VIII defined using Security Risk Oriented Misuse cases. The misuse cases show how the selected threats elaborated i The section also defines Textual Misuse cases for the scenarios.

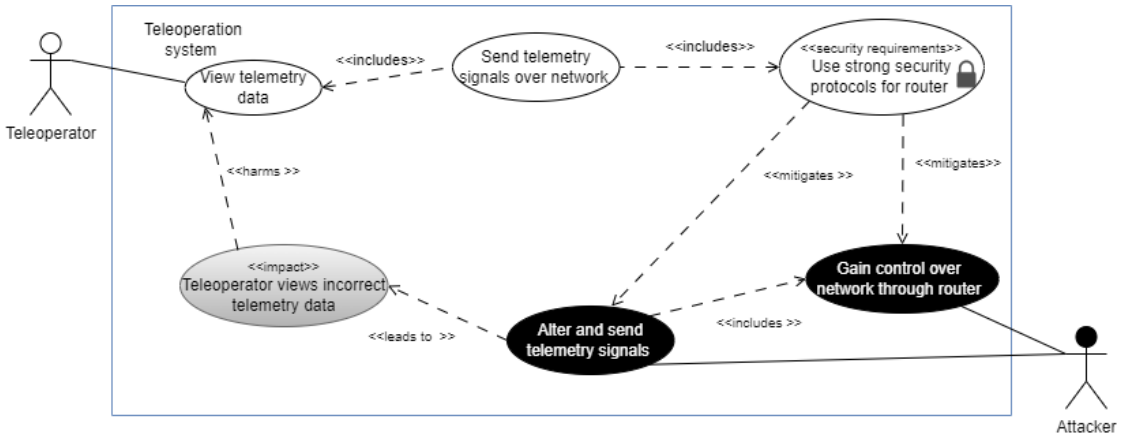


Figure 43. Security risk treatment for router stack overflow in S3

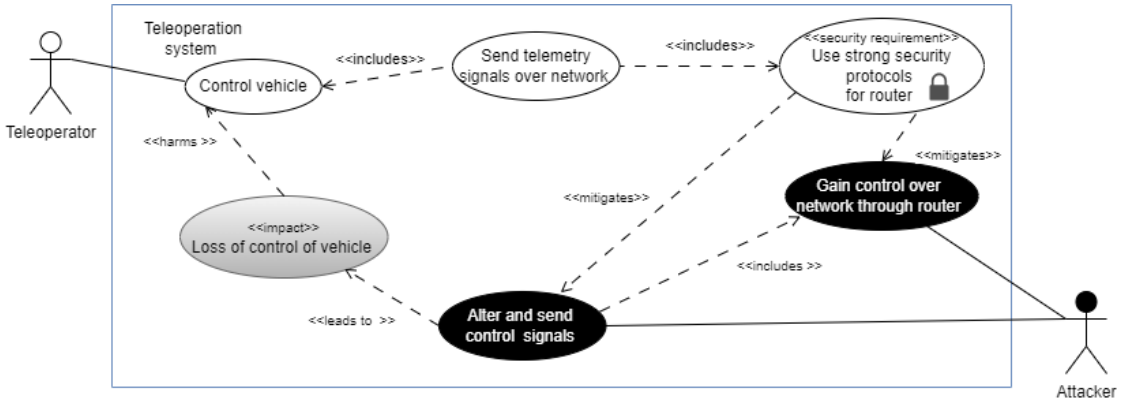


Figure 44. Security risk treatment for router stack overflow in scenario S1

Table 33. Textual misuse case for router stack overflow in S4

Name	Overwrite router software
Summary	Attacker scans router for vulnerabilities and sends oversized packets to router till it overflows and overwrites router system software.
Basic path	**bp1:** Attacker scans router **bp2:** Attacker sends oversized packets to router **bp3:** Attacker overwrites router software **bp4:** Attacker issues their own connection request
Alternative path	**ap1:** Attacker alters network configuration details
Mitigation points	**mp1:** Regularly test network software **mp2:** Use strong security protocols **mp3:** Use router memory protection
Extension points	**ext1:** Includes scan router
Trigger	Connection request is sent to network
Assumption	**as1:** Router is unsecure **as2:** Router software is not up to date
Precondition	**pr1:** Router does not validate input **pr2:** Router lacks memory protection
Worst case threat	Attacker gains control over network and is able to control communication and issue commands eg connection request; Integrity of connection request is negated; Integrity of Network configuration details is negated; Availability of Network configuration details is negated; Confidentiality of Network configuration details is negated
Mitigation guarantee	Network software is regularly tested and vulnerabilities are constantly patched up with recent updates; Attacker is unable to overwrite system due to use of strong security protocols;
Related business rules	Connection to the network should be done only by authorized parties.
Misuser profile	Attacker with knowledge on router functionality and vulnerability and has expertise on how to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Connecting to network

Table 34. Textual misuse case for router stack overflow in S3

Name	Alter and send telemetry signals
Summary	Attacker overwrites router system software and gains access over network. Attacker then alters and sends telemetry signals
Basic path	**bp1:** Attacker gains control over network **bp2:** Attacker accesses telemetry signals **bp3:** Attacker alters and sends telemetry signals
Mitigation points	**mp1:** Use strong access controls **mp2:** Validate input to router
Extension points	**ext1:** Includes gain control over network through router
Trigger	Telemetry signals are sent over network
Assumption	**as1:** Router uses weak access controls **as2:** Router acts as a gateway to network **as3:** Alter includes changing and deleting
Precondition	**pr1:** Router does not validate input
Worst case threat	Attacker alters and sends telemetry signals; Integrity of telemetry signals is negated; Confidentiality of telemetry signals is negated; Availability of telemetry signals is negated.
Mitigation guarantee	Attacker cannot gain access to network through router due to use of strong access controls; Telemetry signal inputs made to the router are first validated before they are transmitted.
Related business rules	Access to the network should be done only by authorized parties. Telemetry signals should be securely transmitted
Misuser profile	Attacker with knowledge on router functionality and vulnerability and has expertise on how to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Send telemetry signals over network

Table 35. Textual misuse case for router stack overflow in S1

Name	Alter and send control signals
Summary	Attacker overwrites router system software and gains access over network. Attacker then alters and sends control signals
Basic path	**bp1:** Attacker gains control over network **bp2:** Attacker accesses control signals **bp3:** Attacker alters and sends control signals
Mitigation points	**mp1:** Use strong access controls **mp2:** Validate input to router
Extension points	**ext1:** Includes gain control over network through router
Trigger	Control signals are sent over network
Assumption	**as1:** Router uses weak access controls **as2:** Router acts as a gateway to network **as3:** Alter includes change and delete
Precondition	**pr1:** Router does not validate input
Worst case threat	Attacker alters and sends control signals; Integrity of control signals is negated; Confidentiality of control signals is negated; Availability of control signals is negated.
Mitigation guarantee	Attacker cannot gain access to network through router due to use of strong access controls; Any control signal inputs made to the router are first validated before they are transmitted.
Related business rules	Access to the network should be done only by authorized parties. Control signals should be securely transmitted
Misuser profile	Attacker with knowledge on router functionality and vulnerability and has expertise on how to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Send control signals over network

Table 36. Textual misuse case for MiTM in S3

Name	Gain access to telemetry signals
Summary	Attacker gains access to telemetry signals. He then alters and sends telemetry signals
Basic path	**bp1:** Attacker gains access to telemetry signals **bp2.1:** Attacker alters Telemetry signals **bp2.2:** Attacker sends altered telemetry signals
Mitigation points	**mp1:** Use strong security mechanisms **mp2:** Protect data shared over network
Extension points	**ext1:** Includes alter and send telemetry signals
Trigger	Telemetry signals are sent over network
Assumption	**as1:** Network is unsecure **as2:** Attacker established himself as man in the middle
Precondition	**pr1:** Telemetry signals are unencrypted
Worst case threat	Telemetry signals are changed or deleted; Integrity of Telemetry signals is negated; Availability of Telemetry signals is negated; Confidentiality of Telemetry signals is negated; Teleoperator receives incorrect or no data
Mitigation guarantee	Attacker cannot access Telemetry signals due to use of secure communication; In case attacker accesses network, he cannot access Telemetry signals as they are encrypted
Related business rules	Telemetry data is required and needs to be accurate, since it is needed by teleoperator to issue control commands.
Misuser profile	Attacker with knowledge on vulnerabilities of computer networks as well as expertise on how to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Sending Telemetry signals

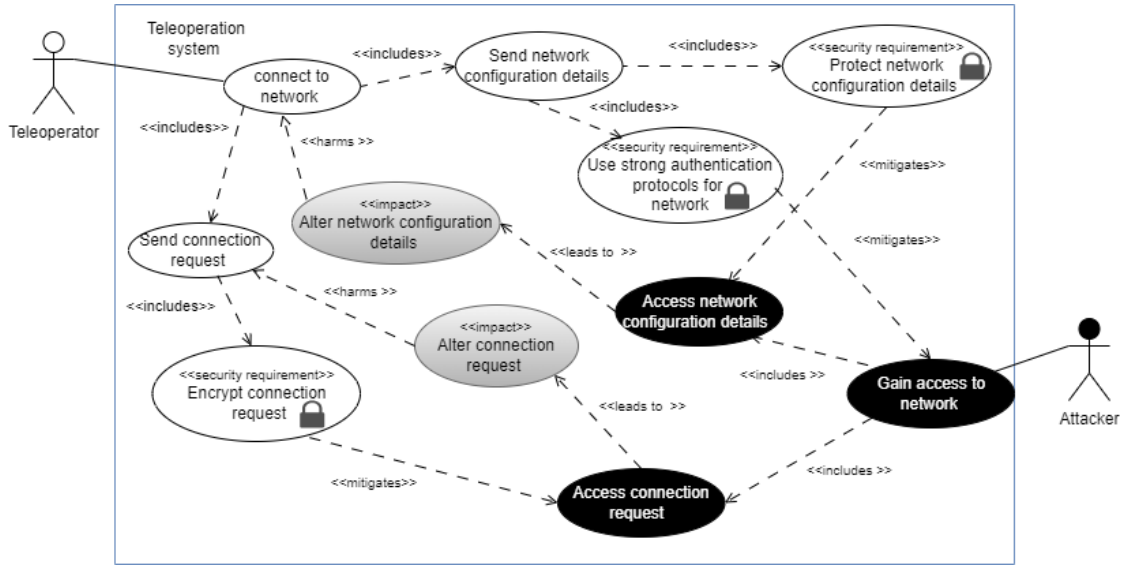


Figure 45. Security risk treatment for MiTM in S4

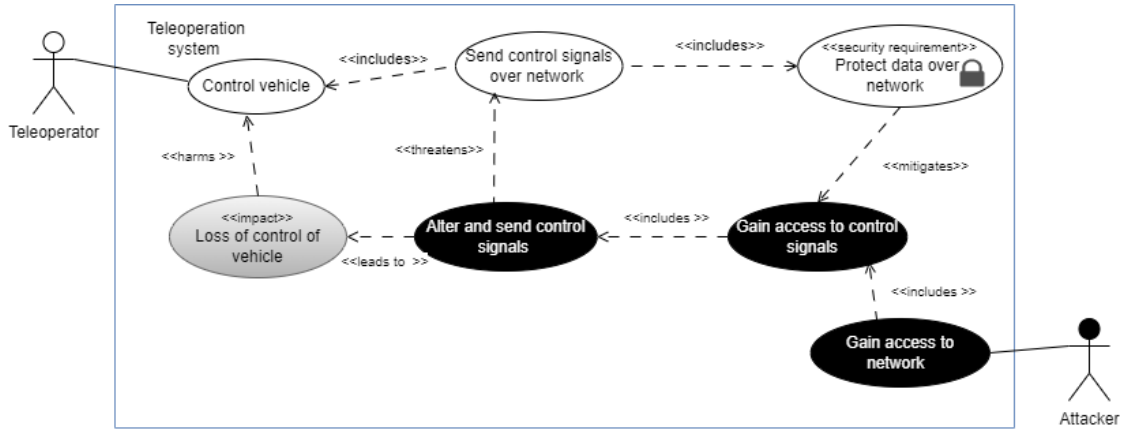


Figure 46. Security risk treatment for MiTM in scenario S1

Table 37. Textual misuse case for MiTM in S4

Name	Gain access to network
Summary	Attacker gains access to network and establishes himself as man in the middle. He accesses and alters network details
Basic path	**bp1:** Attacker gains access to network **bp2:** Attacker accesses network configuration details
Mitigation points	**mp1:** Use secure communication **mp2:** Make network configuration details unreadable
Extension points	**ext1:** Includes access network configuration details
Trigger	Connection request is sent to network
Assumption	**as1:** Network is unsecure
Precondition	**pr1:** Network configuration details are unencrypted
Worst case threat	Network configuration details are changed; Integrity of network configuration details is negated; Network configuration details are unavailable; Confidentiality of network configuration details is negated
Mitigation guarantee	Attacker cannot connect to network due to use of secure communication; In case attacker accesses network, he cannot access Network configuration details as they are encrypted
Related business rules	Connection between the remote station and vehicle is required for teleoperation
Misuser profile	Attacker with knowledge on vulnerabilities of computer networks as well as expertise on how to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Connecting to network

Table 38. Textual misuse case for MiTM in S1

Name	Gain access to control signals
Summary	Attacker gains access to control signals. He then alters and sends control signals over network.
Basic path	**bp1:** Attacker gains access to control signals **bp2.1:** Attacker alters control signals **bp2.2:** Attacker sends altered control signals
Mitigation points	**mp1:** Use secure communication **mp2:** Make control signals unreadable
Extension points	**ext1:** Includes alter and send control signals
Trigger	Control signals are sent over network
Assumption	**as1:** Network is unsecure **as2:** Attacker established himself as man in the middle
Precondition	**pr1:** Control signals are unencrypted
Worst case threat	Control signals are changed or deleted; Integrity of control signals is negated; Availability of control signals is negated; Confidentiality of control signals is negated; Car PC receives and executes incorrect commands or receives no commands at all; Car crashes.
Mitigation guarantee	Attacker cannot access control signals due to use of secure communication; In case attacker accesses network, he cannot access control signals as they are encrypted
Related business rules	Control signals are required and need to be accurate so as to ensure proper control of vehicle.
Misuser profile	Attacker with knowledge on vulnerabilities of computer networks as well as expertise on how to exploit them
Stakeholder risks	The reputation of vehicle company is tarnished. Organisation is faced with legal troubles
Scope	Sending control signals

Table 39. Textual misuse case for 5G replay in S1

Name	Access and store control signals
Summary	Attacker accesses legitimate control signals over network and stores them. The attacker later replays the transmitted signals over the network to the vehicle.
Basic path	**bp1:** Attacker accesses control signals **bp2:** Attacker stores control signals **bp2:** Attacker replays control signals to vehicle
Mitigation points	**mp1:** Use strong authentication mechanisms **mp2:** Protect data shared over network **mp3:** Regularly update sessions
Extension points	**ext1:** Includes replay old control signals
Trigger	Control signals are sent over network
Assumption	**as1:** Network uses weak authentication protocols **as2:** Network used is 5G
Precondition	**pr1:** Session is not updated **pr2:** Control signals are not encrypted
Worst case threat	Attacker replays old control signals to vehicle and vehicle executes them; Loss of control of vehicle; Integrity of control signals is negated; Confidentiality of control signals is negated.
Mitigation guarantee	Strong authentication ensures control signals are not tampered with; Encryption of control signals ensures signals are not accessible even when network is compromised; Updated sessions ensure control signals of old sessions are not replayed in new session.
Related business rules	Control signals need to be accurate to ensure proper vehicle control.
Misuser profile	Attacker with knowledge on network sessions and their vulnerability and has expertise to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Send control signals

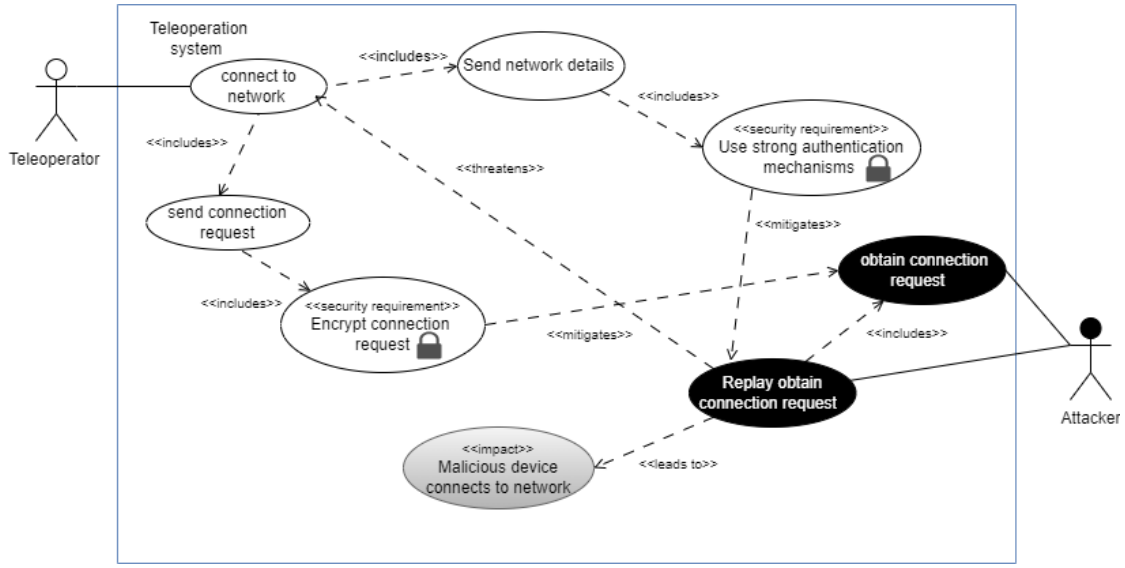


Figure 47. Security risk treatment for 5G replay 1 in Scenario S4

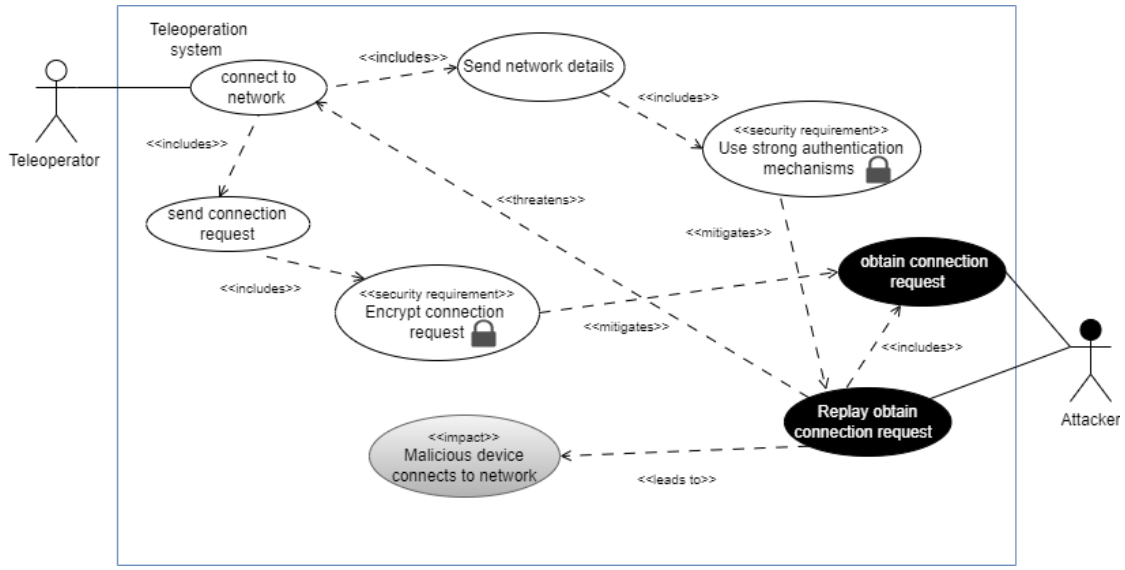


Figure 48. Security risk treatment for 5G replay 2 in Scenario S4

Table 40. Textual misuse case for 5G replay in S4

Name	Replay network configuration details to server
Summary	Attacker obtains legitimate network configuration details. Attacker replays network configuration details to server and gets server to accept malicious connection. Attacker can also replay connection request and get the network to accept a malicious device to connect to network.
Basic path	**bp1:** Attacker accesses network configuration details **bp2:** Attacker replays network configuration details to server
Alternative path	**ap1:** Attacker obtains connection request **ap2:** Attacker replays captured connection request
Mitigation points	**mp1:** Update and refresh sessions **mp2:** Make network configuration details unreadable **mp3:** Make connection request unreadable
Extension points	**ext1:** Includes obtain network details **ext2:** Includes replay obtained connection request
Trigger	Connection request is sent to network
Assumption	**as1:** Network uses weak authentication protocols
Precondition	**pr1:** Session is not updated **pr2:** Connection request is not encrypted
Worst case threat	Attacker replays network configuration details and server connects to wrong network; Attacker replays connection request and network allows malicious device to connect to network; Integrity of connection request is negated; Integrity of network configuration details is negated; Confidentiality of network configuration details is negated.
Mitigation guarantee	Updated sessions ensure old connection requests and network configuration details are invalid; Encryption ensures network configuration details and connection requests are unaccessible
Related business rules	Access to the network should be done only by authorized parties. Only authorized devices should connect to network
Misuser profile	Attacker with knowledge on network sessions and their vulnerability and has expertise to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Connect to network

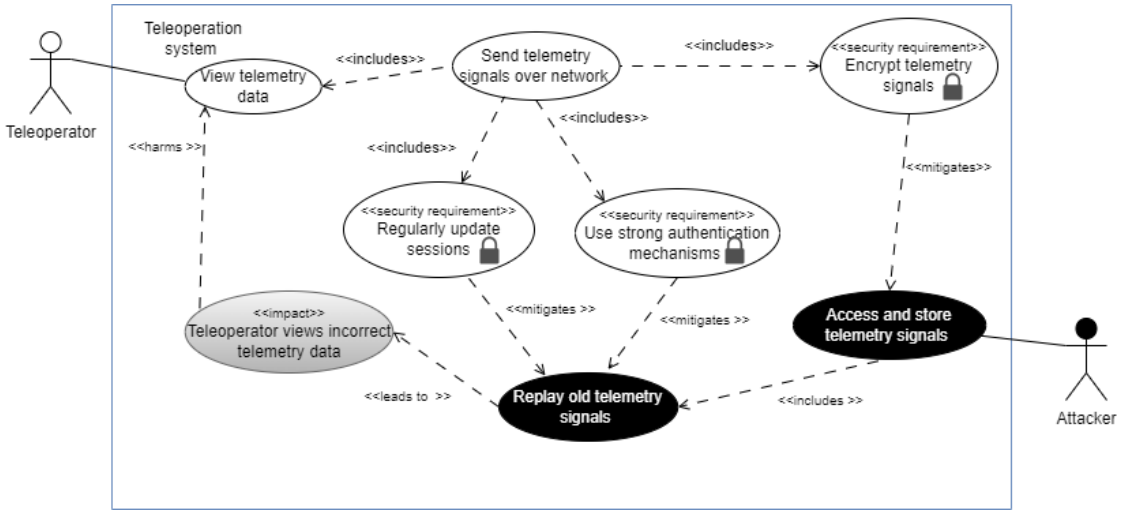


Figure 49. Security risk treatment for 5G replay in Scenario S3

Table 41. Textual misuse case for 5G replay in S3

Name	Access and store telemetry signals
Summary	Attacker accesses legitimate telemetry signals over network and stores them. Attacker later replays the transmitted signals over the network to the remote station.
Basic path	**bp1:** Attacker accesses telemetry signals **bp2:** Attacker replays telemetry signals to server
Mitigation points	**mp1:** Use strong authentication mechanisms **mp2:** Make telemetry signals unreadable **mp3:** Regularly update sessions
Extension points	**ext1:** Includes replay old telemetry signals
Trigger	Telemetry data is sent over network
Assumption	**as1:** Network uses weak authentication protocols
Precondition	**pr1:** Session is not updated **pr2:** Telemetry signals are not encrypted
Worst case threat	Attacker replays telemetry signals to remote station and teleoperator issues new commands based on old telemetry data; Integrity of telemetry data is negated; Confidentiality of telemetry signals is negated.
Mitigation guarantee	Strong authentication ensures data is not tampered with; Encryption of telemetry signals ensures signals are not accessible even when network is compromised; Updated sessions ensure telemetry signals of old sessions are not replayed in new session.
Related business rules	Telemetry signals need to be accurate to ensure correct control commands are issued.
Misuser profile	Attacker with knowledge on network sessions and their vulnerability and has expertise to exploit them
Stakeholder risks	The reliability of Network provider is lost
Scope	Send telemetry signals

X. Validation

This section shows the structure of the Google Forms used for the validation of the Architecture and Security Risk Management approaches presented in the thesis. The section also presents results for each of the questions from the survey.

For Architecture

Design

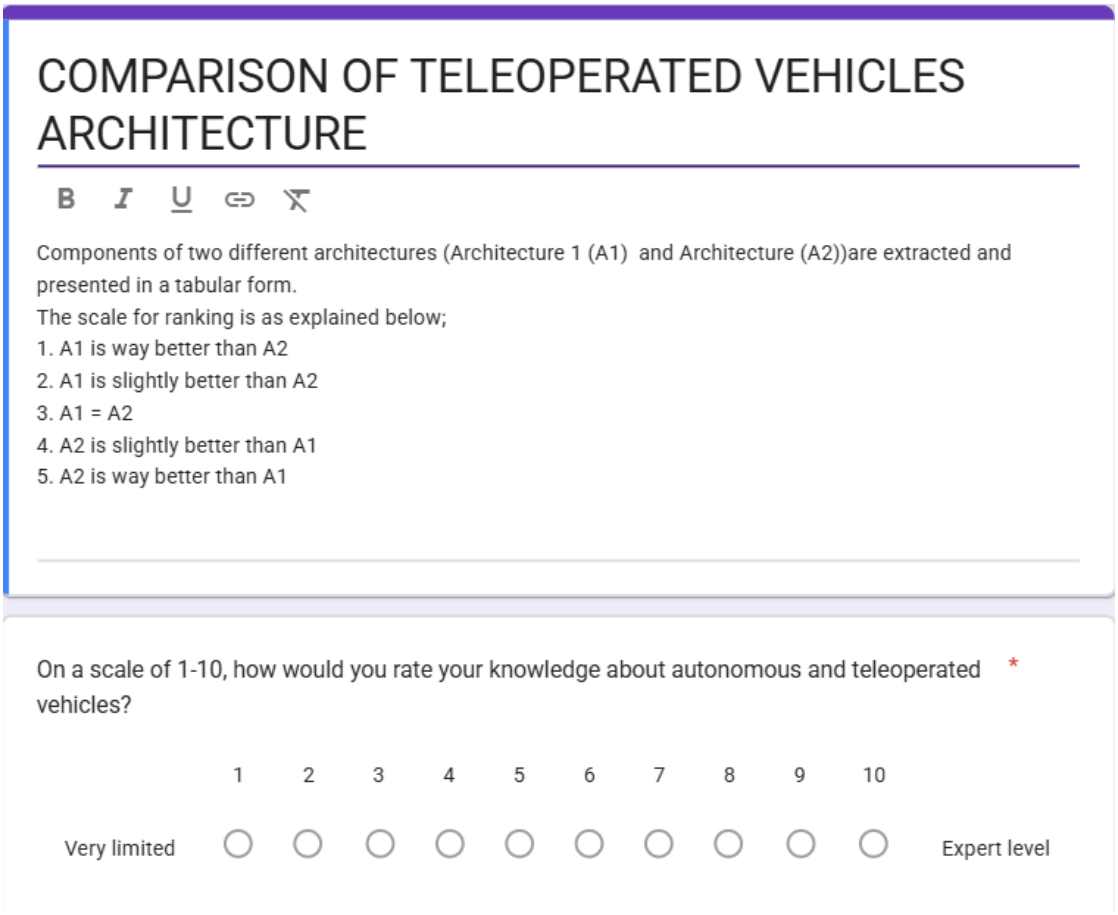


Figure 50. Figure showing ranking criteria and knowledge scale

Tables showing function of each component in each architecture.

Description of components for architecture 1

Vehicle	Refers to the remote vehicle
Bridge	Connects components of the vehicle
LIDAR	Uses light for object detection
GPS	Tracking and vehicle navigation
Odometry sensor	Estimates vehicle position
Camera	Captures video data
State feedback	Measures
Network	Connects operator interface to the vehicle
Operator Interface	Enables teleoperator to control vehicle
Input devices	Enable the teleoperator to create commands
Display	Shows data transmitted from vehicle

Component description for Architecture 2

Component	Description
Car PC	Manages all components and interfaces of the vehicle
ECU	Controls vehicle actuators
Actuators	Move the vehicle
On Board Unit	Interfaces with sensors and actuators Allows communication to external infrastructure
CAN	Enables communication between vehicle components
Sensors	All devices that collect information about the vehicle and its surroundings
LIDAR	Uses light for object detection
RADAR	Uses radio waves for object detection
Camera	Captures video data
Inertia Measuring Unit	measures and reports vehicle speed and orientation
GPS	Tracking and vehicle navigation
Network	Connects vehicle to the remote station
Modem	Enables vehicle and remote station to connect to the internet. It creates an Airlink
Router	Router is connected to the modem and enables wireless communication
Airlink	Allows sharing of data over the network
Gateway	Connects airlink to the remote station
Remote station	Refers to the place where the teleoperator controls and monitors vehicle from
Server	Provides services to other components connected to the network
Computer	Device connected to the server. It could be a mobile phone or laptop.
Application	Runs on computer and Car PC. It enables teleoperation
Control devices	Issue commands to control vehicle.
Display devices	Show data transmitted from the vehicle
Antennae	Connects vehicle to external infrastructure

Figure 51. Figure showing a description of components in both architectures

1. Which architecture shown below captures more components

Architecture 1

Vehicle	Network	Operator Interface
Bridge		Input devices
LIDAR		Display
GPS		
Camera		
Odometry		
State feedback		

Architecture 2

Vehicle	Network	Remote station
Car PC	Modem	Server
ECU	Router	Computer
Actuators	Airlink	Application
On Board Unit	Gateway	Control devices
CAN		Sensors
Human Machine Interface		Display devices
Sensors		
Inertia Measuring Unit		
LIDAR		
RADAR		
Camera		
GPS		

Figure 52. Question 1 of survey

Results

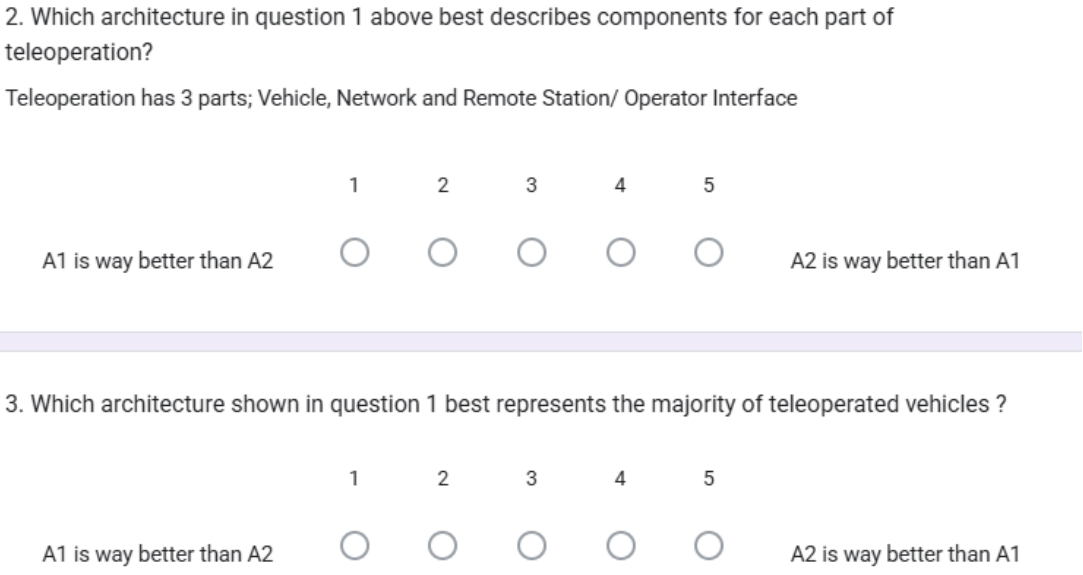


Figure 53. Question 2 and 3 of survey

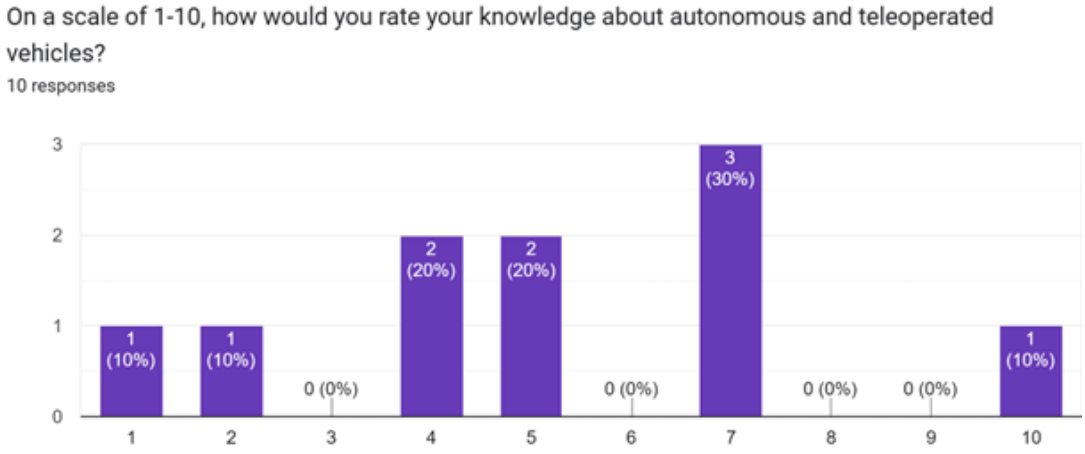
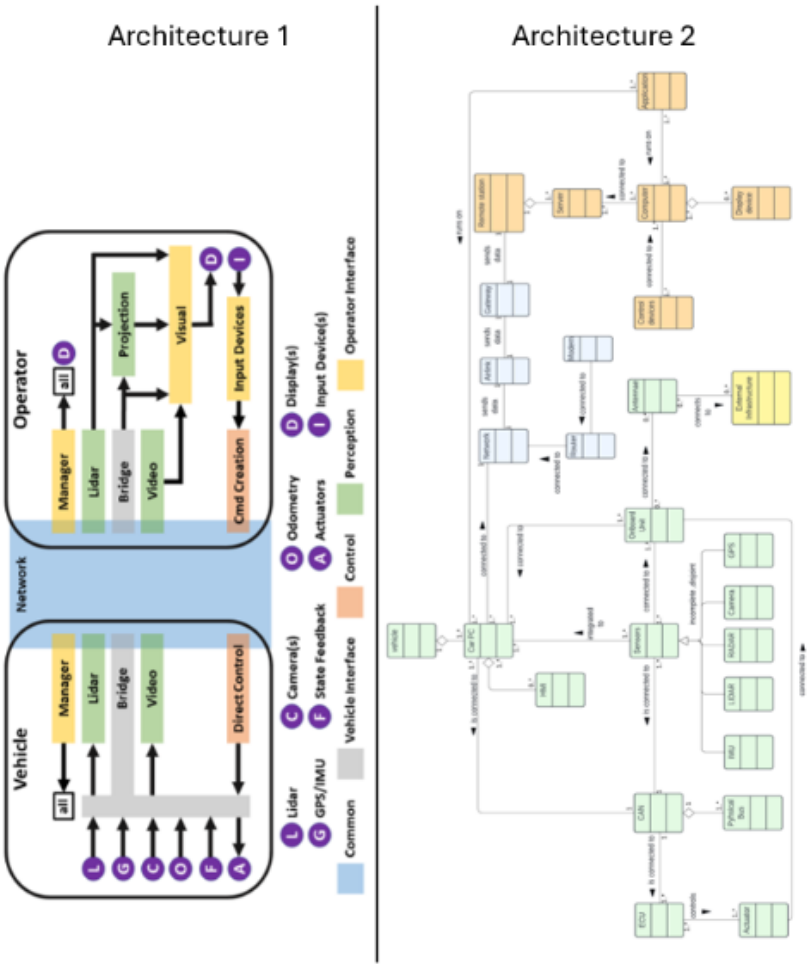


Figure 55. Ranking of knowledge for architecture

4. Which architecture shown below is easier to understand? Kindly *click here for large-scale images.*



	1	2	3	4	5	
A1 is way more easier to understand	○	○	○	○	○	A2 is way more easier to understand

5. Altogether, which architecture do you prefer and why? *

Long-answer text

H

Figure 54. Question 4 and 5 of survey

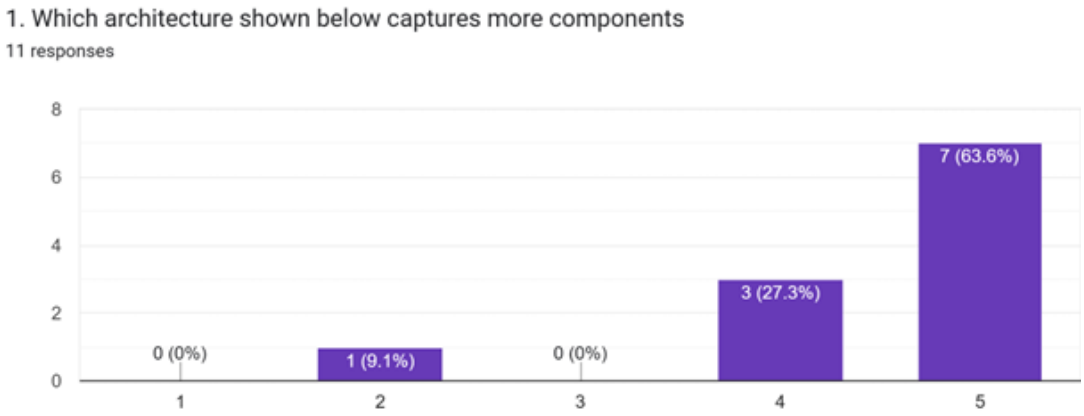


Figure 56. Architecture validation question 1

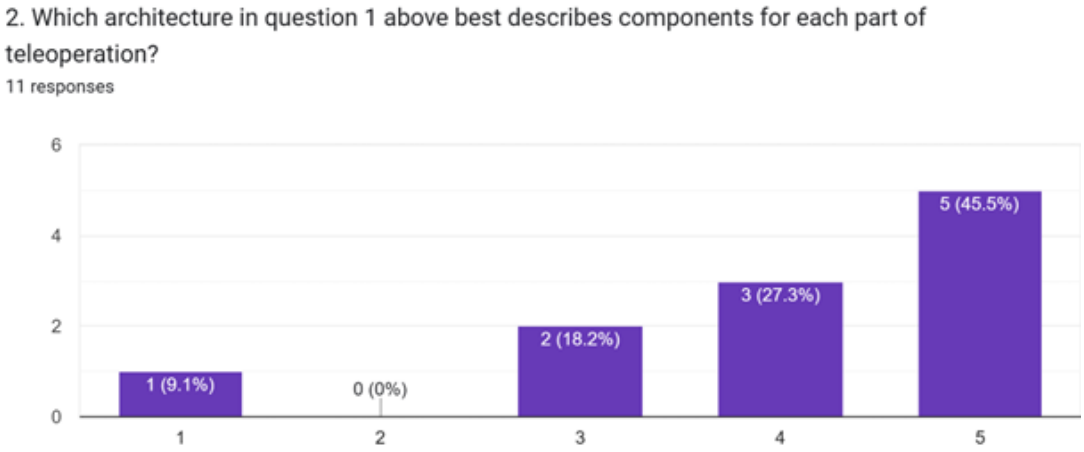


Figure 57. Architecture validation question 2

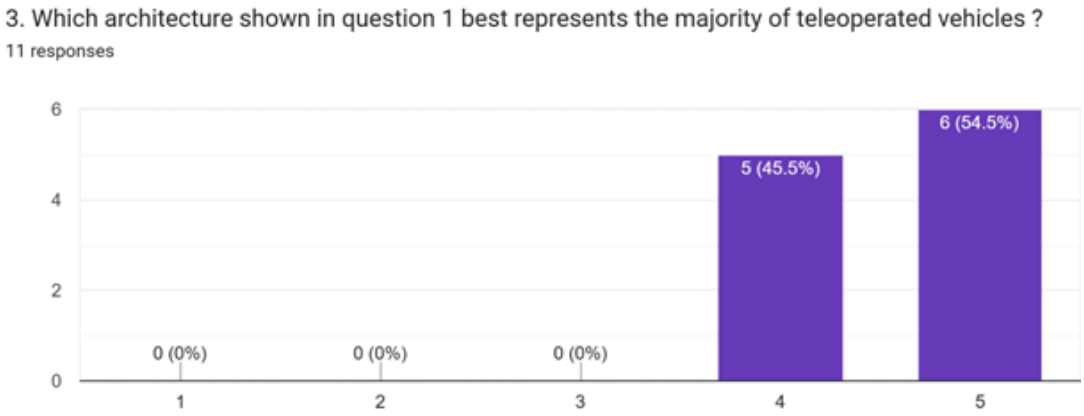


Figure 58. Architecture validation question 3

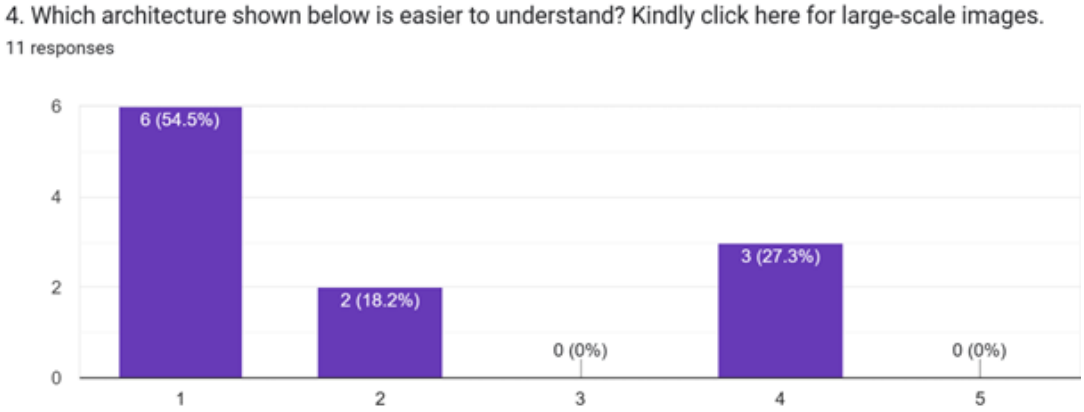


Figure 59. Architecture validation question 4

5. Altogether, which architecture do you prefer and why?

11 responses

A2 because it covers all three parts of teleoperation

Architecture 2 is way more detailed and highlights the details better for full understanding.

I prefer A1, because it is compact and focuses on things that are important - vehicle and remote operator workstation. But A2 also has some value, as it more clearly highlights different components in communication, which might be important for security analysis.

I would go with A1. As it's much organised and less complex.

For a person who don't have a background in architecture, option 1 seems much more easy to understand

A2

Architecture 2. It is more informative.

Figure 60. Architecture validation question 5.1

A2, because there is a more in depth view about the components and it helps to better understand the concept

The less components a system has, the more secure it is. That's a basic principle of cybersecurity. The reason why security and system features is in constant optimization is due to balance both aspects. I think that the A1 is more balanced.

Architecture 2 shows a well detailed design and illustration

Architecture 2 because it is a broader and more encompassing architecture detailing all components founds in TOVs and their interconnectivity.

Figure 61. Architecture validation question 5.2

Table 42. Table showing grouped summary of responses for architecture questionnaire

Criteria	Question	7-10	4-6	1-3
Completeness	Qn 1	4,5,5, 2	4,5,5,4	5,5
Completeness	Qn2	5,4,5,1	4,5,5,3	5,3
Comprehensiveness	Qn 3	4,5,4,5	4,5,5,4	5,5
Intuitiveness	Qn 4	2,1,4,1	4,1,1,2	1,1

For Security Risk Management

Design

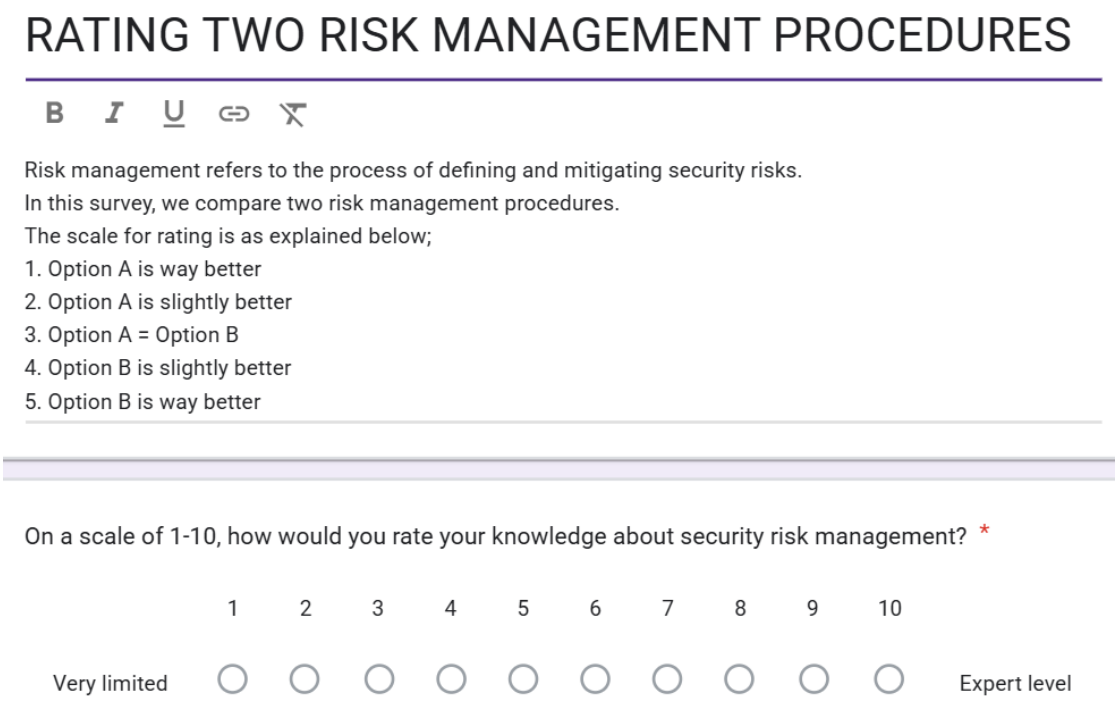
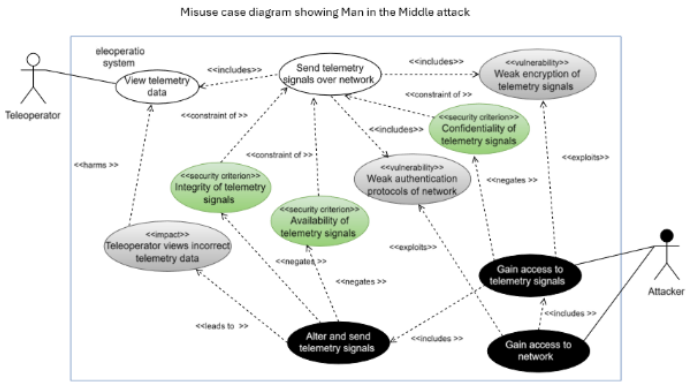


Figure 62. Figure showing ranking criteria and knowledge scale

1. Which of the two options better describes mentioned attack(s)?

A is a Misuse case diagram. B is textual description

Option A



Option B

Attacks targeting communication channels. Communication channels' security should be paramount in AV teleoperation, as the communication channels transmit critical information between the vehicle and the remote driver. The main types of cyberattacks on communication channels are DoS attacks, blocking all communications between the vehicle and the control station. An adversary may modify or drop transmitted video signals, sensor readings, control command sent by RO, and messages coming from road infrastructures or other vehicles.

	1	2	3	4	5	
Option A is way better than Option B	○	○	○	○	○	Option B is way better than Option A

Figure 63. Question 1 of survey

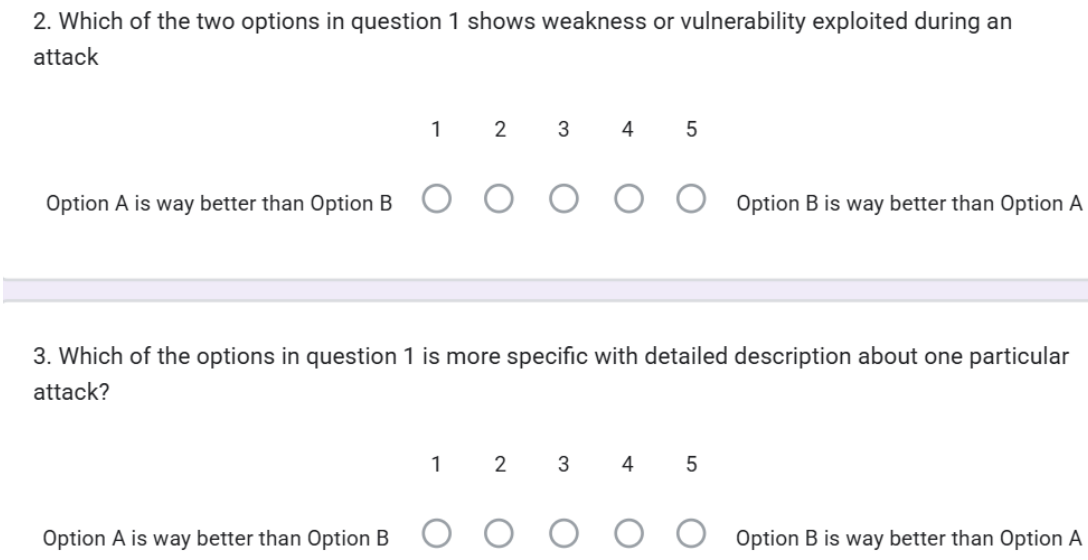


Figure 64. Questions 2 and 3 of survey

4. The figures below show mitigation approaches to the risks presented in question 1. How similar are the two approaches? *

OPTION A includes both figure and table. OPTION B is a textual description.

OPTION A

Figure 2 Mitigation for Man in the middle attack

Security requirement	Security control
SR4: Network should use strong security mechanisms	Enable 2 factor authentication (2FA) Implement SSL and TLS certificates[12] Intrusion detection systems (IDS) [12]
SR5: Data shared over network should be protected	Structured exception handling overwrite protection (SEHOP) [3] Encrypt communication using cryptography [12]

OPTION B

Ensuring robust communication between vehicle and remote operator. The communication between vehicle and teleoperation control center should be strongly protected, using proper encryption and authentication to prevent different types of attacks such as DoS, the Man in the Middle, information spoofing, etc. Moreover, multiple trusted entities like session servers can be introduced between vehicle and teleoperation control centers [29] to ensure secure data transfer. The session server can perform a list of tasks, including registering vehicles and ROs, handling vehicle remote control requests, selecting a suitable teleoperator for each request, and initiating an encrypted peer-to-peer connection between vehicles and ROs.

	1	2	3	4	5	
Not similar at all	○	○	○	○	○	Very similar

Figure 65. Question 4 of survey

5. Which option in question 4 better describes activities to mitigate risks shown in question 1? *

	1	2	3	4	5	
Option A is way better than Option B	○	○	○	○	○	Option B is way better than Option A

6. Which of the mitigation options in question 4 is more elaborate with necessary information for implementation.

	1	2	3	4	5	
Option A is way better than Option B	○	○	○	○	○	Option B is way better than Option A

7. Which of the two security risk management options in question 4 do you prefer and why?

Short-answer text

Figure 66. Questions 5, 6, and 7 of survey

Results

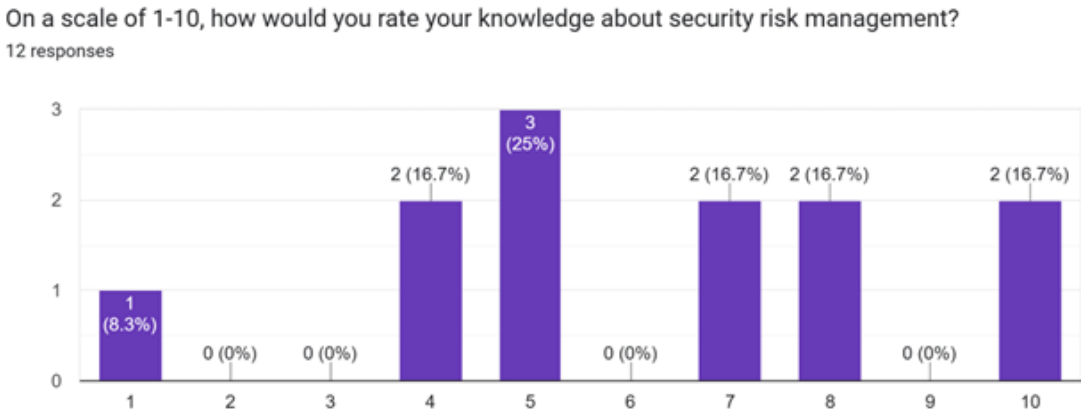


Figure 67. Ranking of knowledge for security

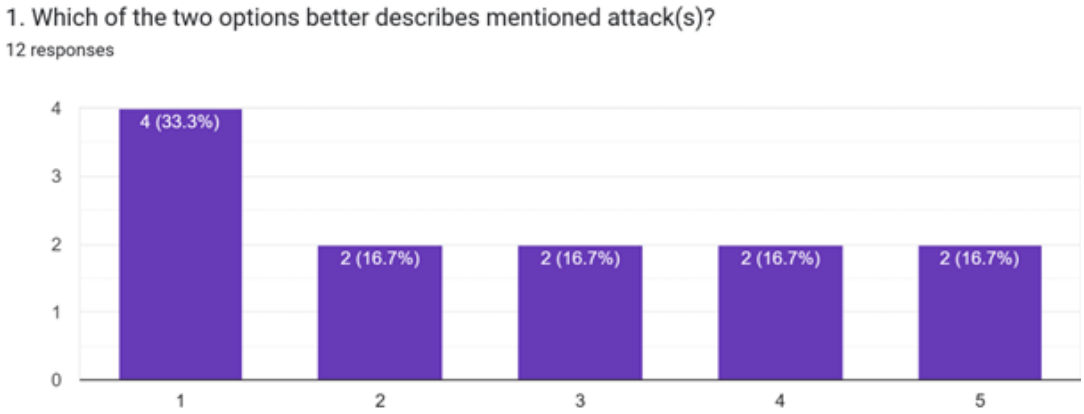


Figure 68. Security validation question 1

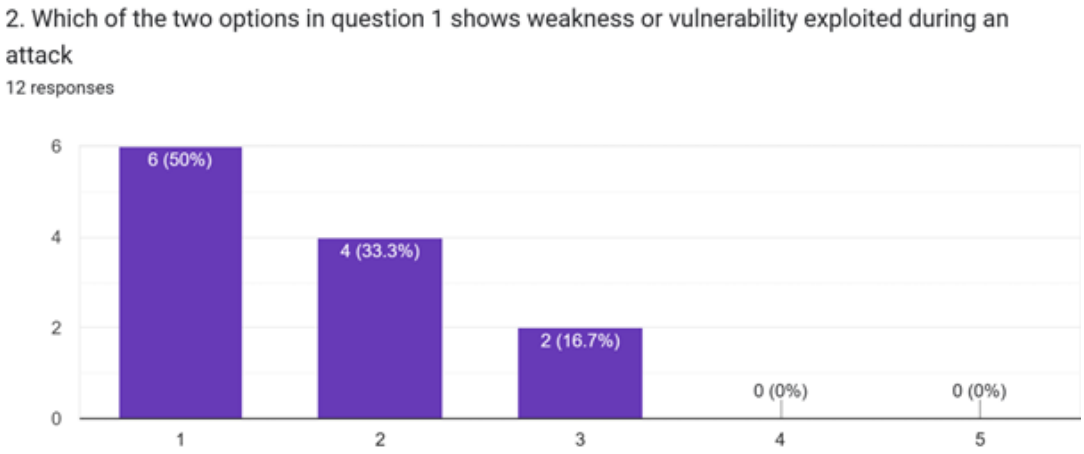


Figure 69. Security validation question 2

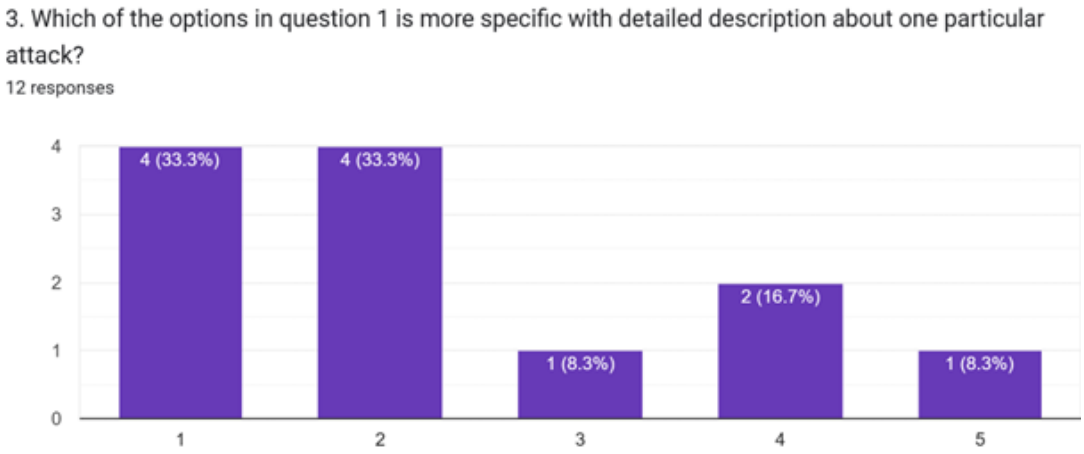


Figure 70. Security validation question 3

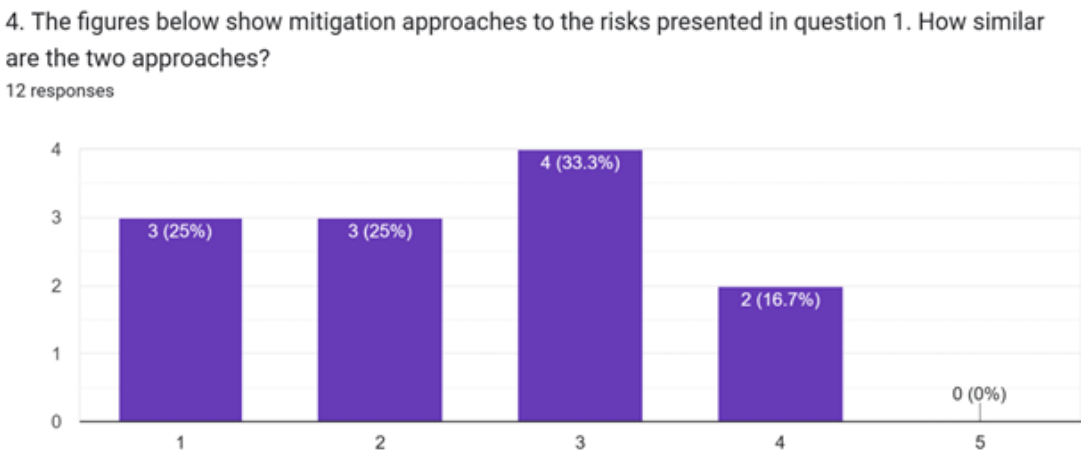


Figure 71. Security validation question 4

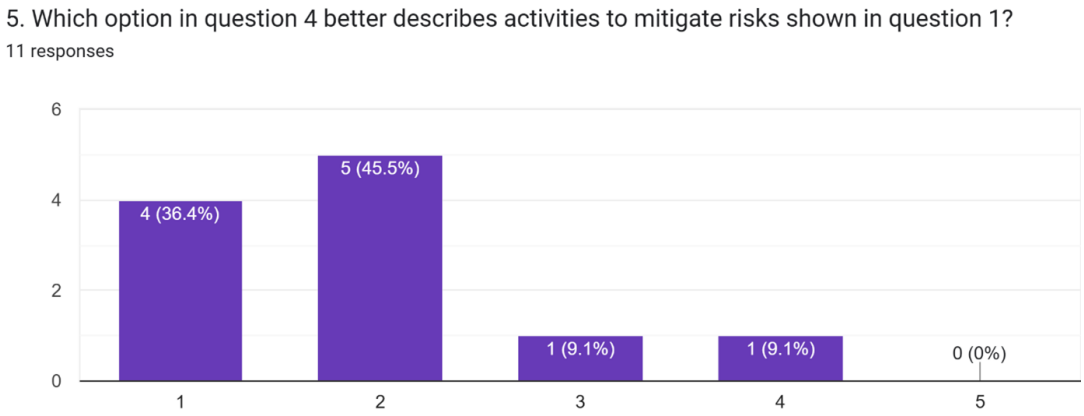


Figure 72. Security validation question 5

7. Which of the two security risk management options in question 4 do you prefer and why?

11 responses

B, butnit could be improved by including the meaning of abbreviations or a description of thr attacks for a better understanding.

Option A as it's well detailed and designed to show to protect from the attack

Option A because it clearly outlines a method for implementing risk mitigation.

Option A clearly and pricisely discusses secuirty requirements to mitigate the risk.

Option 1 because it uses a table to highlight the vulnerability and its risk management options side by side

I would go for diagram as all the parameters are interlinked with proper connection and elaboration of actual context.

A1, visuals are easier to understand and hence build upon than the textual description

Figure 73. Security validation question 6.1

I think option A. It's concise and a bit easy to follow with the use of diagrams (But this question in not very clear imo)

The table in Option A is more actionable.

The textual and graphical representation of risk gives describes where risk are found, what can be done to mitigate them. This provides a clearer context in the security risk management process

Figure 74. Security validation question 6.2

Table 43. Table showing grouped summary of responses to risk management questionnaire

Criteria	Question	7-10	4-6	1-3
Descriptiveness	Qn 1	1,1,1,2,4,5	1,3,3,4,5	2
	Qn 2	1,1,1,2,2,2	1,3,2,3,1	1
	Qn 5	2,1,2,2,4,1	1,2,3,2,1	-
	Qn 6	2,1,2,2,4,1	2,4,2,5,1	1
Specificity	Qn 3	3,1,2,2,1,2	2,4,4,1,5	1
Uniqueness	Qn 4	4,3,1,3,4,1	1,3,2,3,2	2

XI. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Aqel Rizza Ndifuna** ,
*(*author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   On The Road To Security Risk Management in Vehicle Teleoperation Scenarios
   *(*title of thesis)

   supervised by Raimundas Matulevičius .
   *(*supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Aqel Rizza Ndifuna
15/05/2025