UNIVERSITY OF TARTU
Institute of Computer Science
Software Engineering Curriculum

**Rando Tõnisson**

# Security Risk Management in Autonomous Driving Vehicles: Architecture Perspective

**Master's Thesis (30 ECTS)**

Supervisors: Raimundas Matulevičius, PhD
Abasi-Amefon O. Affia, MSc

Tartu 2020

## Security Risk Management in Autonomous Driving Vehicles: Architecture Perspective

**Abstract:**

Security risk management is an essential part of any system development, including autonomous driving vehicles. For autonomous driving service providers, it is necessary to know what risks exist in the system and how they could be mitigated. Security risk management methods allow system stakeholders to manage the security risks within their systems. Unfortunately, an accepted standard to carry out security risk management, specifically for autonomous vehicles, is not presented in the reviewed literature.

In this thesis, we propose a method for security risk management in the autonomous driving field, with a focus on the architecture of the car. The proposed method combines two well-known methods: the security risk management (SRM) method to define the asset, risk and risk-treatment related concepts, and the OCTAVE Allegro method for risk impact assessment. Asset, risk and countermeasure findings from reviewed literature were first used to illustrate the proposed security risk management approach. Then, a case study -- a Bolt autonomous vehicle prototype -- was introduced to demonstrate a practical security risk management scenario, validated by experts in autonomous vehicles and security risk management.

The study finds that the combination of SRM and OCTAVE Allegro combines the strong suits of both methods to provide a systematic approach for security risk management in autonomous driving vehicles, useful to the system stakeholders.

**Keywords:**

Security risk management, SRM, Autonomous driving, OCTAVE Allegro.

**CERCS:**

T120 – Systems engineering, computer technology

## Turvariskide Haldamine Autonoomsetes Sõidukites: Arhitektuuri Perspektiiv

**Lühikokkuvõte:**

Turvariskide haldamine on tähtis osa iga süsteemi arenduses, sealhulgas ka autonoomsetes sõidukites. Ettevõtetele, mis pakuvad autonoomsete sõidukite lahendust tarnes või transpordis, on oluline teada, mis turvariskid süsteemis on ja kuidas nendega tegeleda. Turvariskide haldamise meetodid aitavad süsteemihaldajatel tegeleda turvariskidega oma süsteemis. Kahjuks ei leitud üldsuse poolt heakskiidetud standardit turvariskide haldamiseks autonoomsetele sõidukitele antud lõputöös käsitletud kirjandusest.

Selles lõputöös soovitame meetodit turvariskide haldamiseks autonoomsete sõidukite teadusharus, fookusega sõiduki süsteemi arhitektuuril. See soovitatud meetod ühendab kaks tuntud meetodit. Esiteks turvariskide haldamise meetod (SRM), et defineerida süsteemi osad, riskid ja muud riskidega seotud mõisted ning teiseks OCTAVE Allegro meetod riski mõju hindamiseks. Kirjandusel põhinevad süsteemi osi, riske ja vastumeetmeid kasutatakse esmalt soovitatud meetodi illustreerimiseks. Peale seda rakendatakse antud meetodit konkreetsele juhtumile, Bolt autonoomse auto prototüübile. Tänu sellele saame loodud meetodit demonstreerida praktilisel juhtumil, mis hiljem sai üle vaadatud ja kinnitatud ekspertide poolt, kes tegutsevad autonoomsete sõidukite ja riskide haldamise valdkonnas.

Antud uuring leiab, et SRM ja OCTAVE Allegro kombinatsioon toob välja parima mõlemast meetodist ja loob sellega süstemaatilise meetodi turvariskide haldamiseks autonoomsete sõidukite valdkonnas.

**Võtmesõnad:**

Turvariskide haldamine, SRM, Autonoomsed sõidukid, OCTAVE Allegro

**CERCS:**

T120 - Süsteemitehnoloogia, arvutitehnoloogia

# Table of Contents

## List of Figures

## List of Tables

## Terms and Notations

| | |
|---|---|
| RE | Requirements Engineering |
| SE | Security Engineering |
| SRM | Security Risk Management |
| NIST | National Institute of Standards and Technology |
| FAIR | Factor Analysis of Information Risk |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| IS | Information System |
| AV | Autonomous Vehicle |
| ITS | Intelligent Transport System |
| IoT | Internet of Things |
| NHTSA | National Highway Traffic Safety Administration |
| VANET | Vehicular ad-hoc Network |
| VSN | Vehicular Social Network |
| LiDAR | Light Detection and Ranging (device) |
| CAN | Controller Area Network |
| LAN | Local Area Network |
| ECU | Electronic Control Unit |
| GPS | Global Positioning System |
| GNSS | Global Navigation Satellite System |
| IMU | Inertial Measurement Unit |
| PACMod | Platform Actuation and Control Module |

# 1 Introduction

## 1.1 Motivation

With the technological evolution, the car and transportation industry is not left behind. Autonomous driving is a rapidly growing research field, where many of the biggest car manufactures and transportation companies try to develop the best solutions. The best solutions then need to have a comprehensive risk analysis done. Knowing possible vulnerabilities and the associated risks can provide crucial information to mitigate the risks to provide secure solutions to keep the customers and their data safe and protected.

Autonomous driving is researched to provide transportation of goods and people. The process of autonomous driving will generate a lot of sensitive information about the customers: where they have been, at what times. Also, the vehicle will collect data about the environment it is driving in while scanning the surroundings for different objects like obstacles and traffic signs. For the companies, it is important to keep all the sensitive information confidential. The information is processed, transmitted and manipulated by several parts and components of the vehicle during the process of driving and even after that. As such, these components and parts need to be documented and their possible vulnerabilities analysed in a meaningful manner.

## 1.2 Scope

The research field focused on answering the questions from the previous section is security risk management. Many different methods for risk management are available to use. Security risk management methods focus on finding the system and business assets in the system and the connections between all the components. In addition, the security risks and their countermeasures are selected and defined.

The security risk management process in this work is carried out on an *on-the-move* vehicle. This means the car is built to be driving autonomously in real-life settings, following all the traffic rules and without setting pedestrian and other drivers' lives in danger. There are other autonomous vehicles like planes and boats that are out of the scope of this thesis.

The focus in the security risk management process in this thesis is on the architecture of the vehicle. This includes the components and data required for autonomous driving. General security risks on road legal cars are not discussed in this work. An example of such risk could be faking the signal of the key to unlock the doors of a car. This risk affects all cars with support for remote controlled door locks and not just autonomous vehicles. Because of the focus on the architecture, processes in autonomous vehicles are not explicitly discussed. Some knowledge on the processes is still required, but defining all the processes and finding security risks and vulnerabilities in the processes carried out in the car are out of scope of this work.

## 1.3 Problem Description

Autonomous driving will save money for the companies providing transportation of goods or people in the long run as the system works without needing payment like human drivers do. The built autonomous driving systems will have completely different risks affecting it than human drivers do. Risk management is required to know the possible risks. Having a systematic way for the risk management and the mapping of the components and data flow in the system is needed. Currently, no such standardized way of doing such risk management for autonomous vehicles was found. In this work, one possible way of managing the security risks for autonomous vehicles is provided.

## 1.4 Research Question

To carry out the research for this thesis, the main research question is proposed and is as follows.

**How can data and components be protected against cybersecurity attacks in autonomous vehicles?**

To answer the main research question, three question with smaller scope need to be answered:

**RQ1. What are the protected assets in autonomous vehicles?**

**RQ2. What are security risks and its impact in autonomous vehicles?**

**RQ3. What are security countermeasures in autonomous vehicles?**

Answering **RQ1** will give us the assets present in an autonomous vehicle. Those assets will be the basis for the security risk management.

To answer **RQ2,** we will use the assets from **RQ1** and find the security risks for them. Having the security risks for all the assets will let us measure the impact of the security risks.

Knowing the security risks and their impact from **RQ2**, will let us find and define the countermeasures for them. The risks impact will let us prioritize the implementations of the countermeasures. The answer for **RQ3** will provide possible risk treatment options based on the assets used in the autonomous vehicle, found in **RQ1.**

To answer those questions, an overview of some of the most popular security risk management methods is discussed. Most suitable of them is then chosen. The method is then used to define and illustrate the findings from a literature review. Using the chosen method will provide the primary answer to the research question. Later the findings will be used in a case study. The case study is a University of Tartu and Bolt collaboration on developing an autonomous driving vehicle to later provide taxi service for the customers of Bolt. After the case study, validation on the findings is done.

## 1.5 Structure

The thesis is divided into six chapters as follows;

**Chapter 1** introduces the thesis. This includes motivation, scope, problem description and the research questions.

**Chapter 2** explains the security risk management and some of the methods currently available. The method to be used in this work is discussed. This chapter also provides and explains the research method to be used in this thesis.

**Chapter 3** gives and overview of the state of the art in the intelligent transportation systems and uses the findings from Chapter 2 to present preliminary answers to the research questions. This is done as defining the system assets, business assets, risks and countermeasures based on the literature.

**Chapter 4** uses the findings from Chapter 3 and applies them in a case study. An overview of the case study is presented and the security risk management process is applied to the case study.

**Chapter 5** is for the validation. In there, the validation method is described and the results of it are discussed.

**Chapter 6** provides the conclusion for the thesis with providing the limitations, answers to the research questions, conclusion, continuous and future work.

In addition to the main thesis file, an Appendix file will be included. In there, Appendix IV and V fill be present. Appendix IV has all the OCTAVE worksheets filled in the case study section. Appendix V has the OCTAVE worksheets modified based on the validation.

# 2 Security Risk Management

Security risk management is not a simple task and consists of many smaller, but still necessary tasks. In this chapter, an overview of Security Engineering is given, the existing Security Risk Management methods are discussed, the chosen method is presented and the research method is explained.

## 2.1 Security Engineering

Requirements Engineering (RE) helps the stakeholders to explain the system they are building, how the system works and what are its components. Having done the preparation work as the RE, it helps finding risks and start thinking about possible countermeasures. Security Engineering (SE) is defined as an engineering discipline to lower the risks of intentional[1] unauthorized harm to assets within an acceptable level to the system's stakeholders by preventing, detecting and reacting to malicious harm, misuse, threats and risks [10]. Security Engineering is performed during the whole development process, starting from RE, continuing with design, implementation, and later stages as evaluation and measurements. It can be used to modify an existing system, but all the development steps should still be considered. Considering the security from the start can and will help the development to be more security orientated and making the changes to the overall system is easier than in later stages, helping the stakeholders to save money and provide better solutions. Security Engineering concentrates on tools, processes and method that support and help analysing, designing and implementing the systems according to its needs [7].

## 2.2 Overview of Existing Security Risk Management Methods

There are a lot of standards to manage security risks. Some of them are mentioned by Matulevičius [7] and Dubois et al. [8] lists many RE modelling languages which are specifically made for use in security-sensitive contexts. Those allow to address security concerns in the early stages of the system development. Some of them are described below.

**ISO/IEC 2700X.** The 2700X standard is made to provide reference for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System. 27001 standard [11] focuses on gathering the requirements for the risk management process, 27005 standard [12] is for the actual security risk management.

**ISO/IEC 13335-1.** This standard [13] is series of guidelines providing basic fundamentals and understanding for planning, managing and implementing IT security. It is generally used in information and communication technology, but could be applicable to different organizations.

**Common Criteria v3.1.** Common Criteria [14] provides a set of requirements for IT products and systems security aspects and during the security evaluations, an assurance measure is applied to them. Dubois et al. [8] mention that only the part named "Introduction and general model" was most relevant.

**NIST 800-30**. The National Institute of Standards and Technology (NIST) has published series of different publications and the most relevant ones are the 800 series [15], which focus on the computer security part. Concepts and terminology is provided in those series.

[1] Not to be confused with *unintentional harm,* which is defined as Safety Engineering

**FAIR.** Factor Analysis of Information Risk **(**FAIR) [16] is a sequential approach to risk analysis. It provides risk evaluation framework. In analysis of different approaches by Wangen et al.[17], fair stood up as most dedicated to risk estimation and quantification. FAIR's strength is in risk estimation, but lacks in the risk identification phase, where concepts like vulnerability and threat is not considered.

**OCTAVE Allegro.** Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [6] is a method to asses information security risks to get sufficient results for a small investment of resources (time, money, people etc.). In the recent analysis [17] it was found that OCTAVE's strong suit is in the impact estimation, but lacks support for vulnerability and threat assessment.

**SRM.** SRM method and its domain model seen on Figure 1 was created by Dubois et al. [8]. The new method focuses on solving the problems they found during their research. The lack of efficiency to show cost-effectiveness in the countermeasures and support for different modelling languages. Before it, many other methods supported similar concepts to SRM like assets, risks, vulnerabilities and countermeasures, but lacked the support mentioned before. Those methods were dependent on informal documents with natural language. SRM and its domain model provide concrete risk related concepts to define and the relationships between them. The SRM method excels in defining the assets and risk related concepts but lacks on measuring the impact of the defined risks.

## 2.3 Methodologies Used in this Work

From the previous list of methods, one or more will be chosen to be used in this work. The ones not chosen are ISO/IEC 2700X and 13335-1, NIST800-30, FAIR and Common Criteria. The chosen ones are SRM and OCTAVE allegro. A short explanation on the decision is provided below.

ISO/IEC 2700X and 13335-1 are well known standards with focus on communication systems. AV's could be categorized as that, but more suitable options were found. Even when using other methods, influence from those two standards are present. NIST800-30 is a strong contender for its detailed steps of risk analysis. It is initially made for organizations that gather and process delicate information. This, with combination of lacking additional guidelines and documentation for risk management made NIST800-30 not suitable. Common Criteria has decent initial phase, but falls behind in the later phases of risk management. FAIR was not chosen for the reasons mentioned before, it falls behind in the risk identification phase.

SRM provides concrete method for the risk identification. It supports concepts like attack method, threat, risk, assets and countermeasures. SRM starts with finding the assets in the system, defines the vulnerabilities that the threat and risk will be based on and also supports providing countermeasures to mitigate the risk. SRM is also general enough to be applied to AV's. The method is lacking in measuring the risk impact, which will be addressed by using OCTAVE allegro.

OCTAVE allegro (also referred to as OCTAVE in this work) has a lot of similar concepts to the SRM. It also provides many premade worksheets and documents to support the process. Using the sheets, the impact measuring can be done, which SRM was lacking on. Because of this, OCTAVE will be used to present the risks and countermeasures in their provided worksheets and also measuring the impact of the risks.

## 2.4 Reference Model for Security Risk Management

The domain model (Figure 1) for Security Risk Management is composed of three parts: *assets, security risks and countermeasures*.

*Assets* are defined as something that has value to the company and help them achieve their goals. Those can be categorized into two: *IS assets* (also referred to as *system asset*) and *Business assets*. Generally, *Business assets* are some data, information, skill, process or anything similar that helps the business to achieve their goals. *IS asset* is generally a component or part of the overall system. This includes hardware, software, network etc. All the business assets are constrained by *Security criterion* in SRM. It is defined to give detailed characteristics of the assets' security needs. Typically, the criteria are expressed as confidentiality, integrity and availability of business assets.

*Risk* is defined as a combination of *threat* and *vulnerability* which leads to harm to at least one *asset*. *Event* represents a carried out attack using the defined *threat* and *vulnerability*. In case of the *event* happening, it leads to *impact*. It is a potentially negative harm to some assets or business itself. *Impact* can affect both types *IS* and *business assets*. *Vulnerability* is some weakness in *IS asset* that can be used to cause harm. The one that carries out the attack is called *threat agent*. They use some standard *attack method* to carry out the attack. The combination of *threat agent* using an *attack method* is defined as *threat*.

The countermeasures start with the definition of *controls*. Those can be processes, policies devices or other actions that will help the organisation to reduce risks. Controls themselves are not enough, the company needs to make detailed *security requirements* based on the *controls*. With that, the requirements will show how something is done and what it should cover. Finally, *risk treatment* is defined. That is done in generic and functional terms and shows the decisions on how to treat the identified risks. The decisions can be of four types: *avoiding risk, reducing risk, transferring risk, retaining risk*.

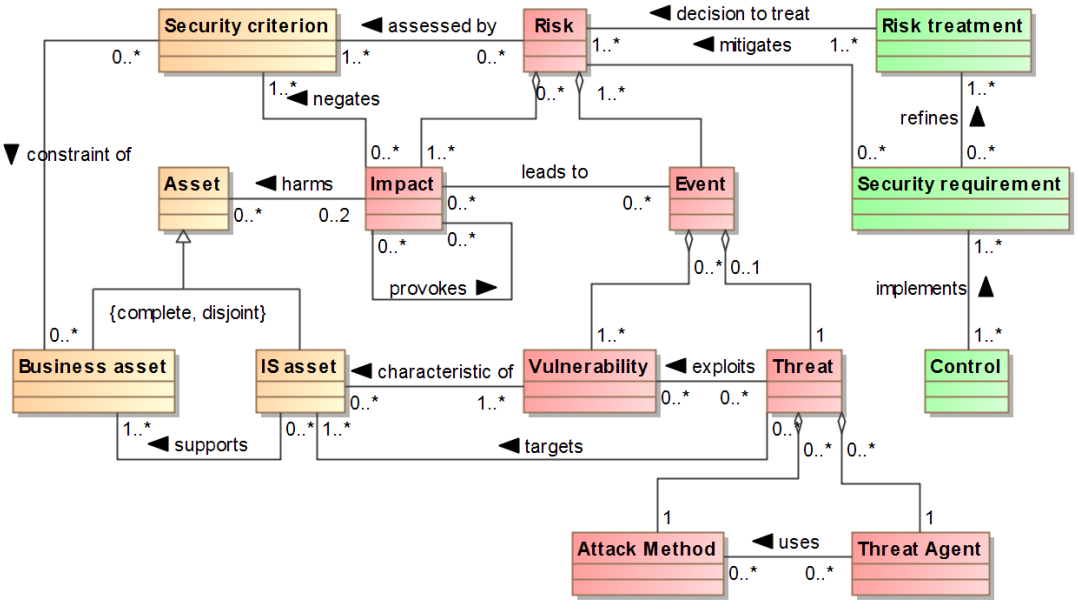


Figure 1. Domain model adapted from [7, 8].

## 2.5 Impact Estimation with OCTAVE Allegro

OCTAVE is a method for organizations to identify, manage and evaluate their risks. The method can be used in a collaborative setting as it provides guidance, worksheets and questionnaires. OCTAVE Allegro is variant of the original OCTAVE method, that has finetuned for systems working and processing information. The OCTAVE method provides a standard set of worksheet templates to create these criteria in several impact areas and then to prioritize them. The workflow in OCTAVE is divided into eight steps, as illustrated on Figure 2.

The first step in OCTAVE Allegro is to define the risk measurement criteria. The risk measurement criteria are basis for the next steps. In the worksheets provided by the method, the criteria have an impact area, which can have low, medium or high impact on the organization. This will be used to evaluate the risks impact in the later stages of the method and is the main reason OCTAVE is used here.

The final impact and risk evaluation is done by using the criteria defined in the first step and combining it with the worksheets provided by OCTAVE. The score will be subjective as the risk measurement criteria is defined by the organization themselves. To counter this, OCTAVE provided the worksheet and guidelines to make it less subjective and unify different types of risks with the impact score. Getting the score for every risk with one unified measurement, will help stakeholders to prioritize more severe risks and understand the risks impact.

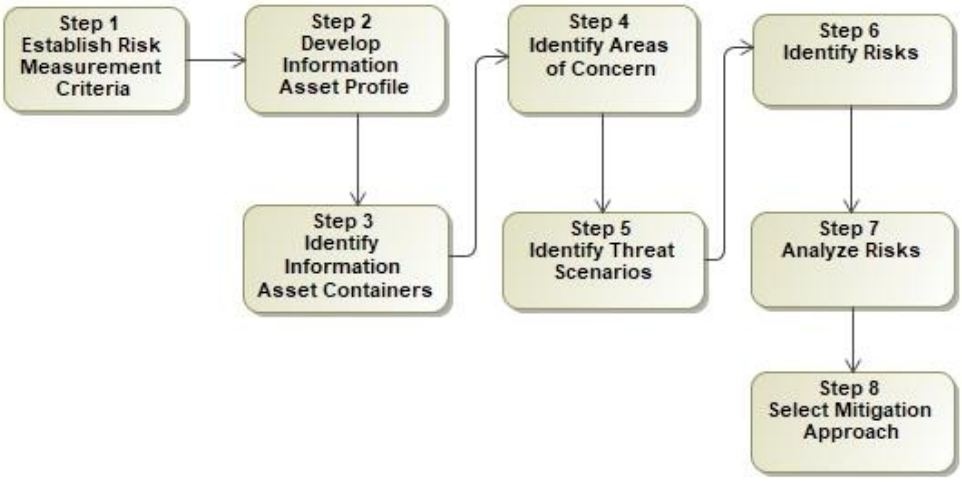


Figure 2. OCTAVE steps, adapted from [6].

## 2.6 Using SRM and OCTAVE

Going forward, a combination of SRM and OCTAVE methods will be used. As seen from the previous overviews, both consist of similar steps and components. Those include defining assets, identifying threats and constructing risks. Because of the similarities, SRM will be used to identify assets, threats and risks while OCTAVE will be used to establish risk measurement criteria and getting the impact of the risks defined using SRM. Such approach was not found during the literature review. Combining the two will allow to use the strong

suits from both methods: the detailed risk defining from SRM and the impact measuring from OCTAVE.

To achieve the compatibility between SRM and OCTAVE, some modifications are needed. As mentioned before, SRM will be used fully for defining risks and later countermeasures for them. OCTAVE provides spreadsheets and questionnaires to analyse risks and their impact but are made to support slightly different approach than SRM. To use those spreadsheets provided by OCTAVE, they need to be modified. Fortunately, modifications are supported as OCTAVE was built to support different types of businesses and needs. This allows changes to be applied without ruining the integrity of the method.

SRM components like attacker, attack method, vulnerability can easily be mapped to different concepts from the risk impact worksheet in OCTAVE. Predefined risk measurement criteria are used as in OCTAVE. Similar criteria will be defined for likelihood too, which is not done in OCTAVE. After filling in the modified asset risk worksheet from OCTAVE, the mitigation table will be used to present the chosen countermeasures and actions.

The outcome will be a system model and risk definition using SRM and evaluating the defined risk and its countermeasures using the modified worksheets from OCTAVE. Using this approach will show all the aspects of a risk in a compact way, with its score and countermeasures for easy presentation options.

## 2.7 Research Method

In this section the research method is described. The quick overview of that can be seen on Figure 3.

The research starts out with a literature review on different methods to use. The ones chosen in this thesis are SRM and OCTAVE allegro. The literature review continues with finding relevant works, but also looking through ITS and IoT fields as AV's are part of them. During the literature review, papers describing the assets or risks in AV are looked for. The found literature is used to define assets and risks based on the SRM method. In addition to the risks and assets, countermeasures are also found from the literature. Mostly, the literature describing the risks also provide some countermeasures to mitigate them. The output of the Background section will be a literature based risk management example for autonomous vehicles. It consists of the defined assets, risks and countermeasures that can be used in the case study.

The case study is based on a research agreement between University of Tartu and Bolt to develop an autonomous driving car. The output from the background section will be used as a base for the Bolt case study. This means that the risks and countermeasures for the Bolt prototype car are also based on the literature. Assets follow the same structure as in the literature, but now are replaced with the actual components used in the prototype. The case study section starts with defining and describing the components installed into the car, that make the autonomous driving possible. Using the OCTAVE sheets the risks is presented and the risk score is calculated. Countermeasures and their costs are defined using OCTAVE worksheets too. The output of the case study section will be the filled out OCTAVE sheets showing the risks, their score and countermeasures with estimated costs.

In the validation section, the OCTAVE sheets defined in the case study will be used as a starting point. The validation is done by interviewing experts familiar with security management and autonomous driving. The experts' feedback is used to validate the work done in the case study section. That is done by adding the proposed changes into the sheets or getting confirmation about the information presented before. In the validation chapter in the

thesis, the main findings from the interviews are presented. The outcome from validation will be the validated security risks in AV's.

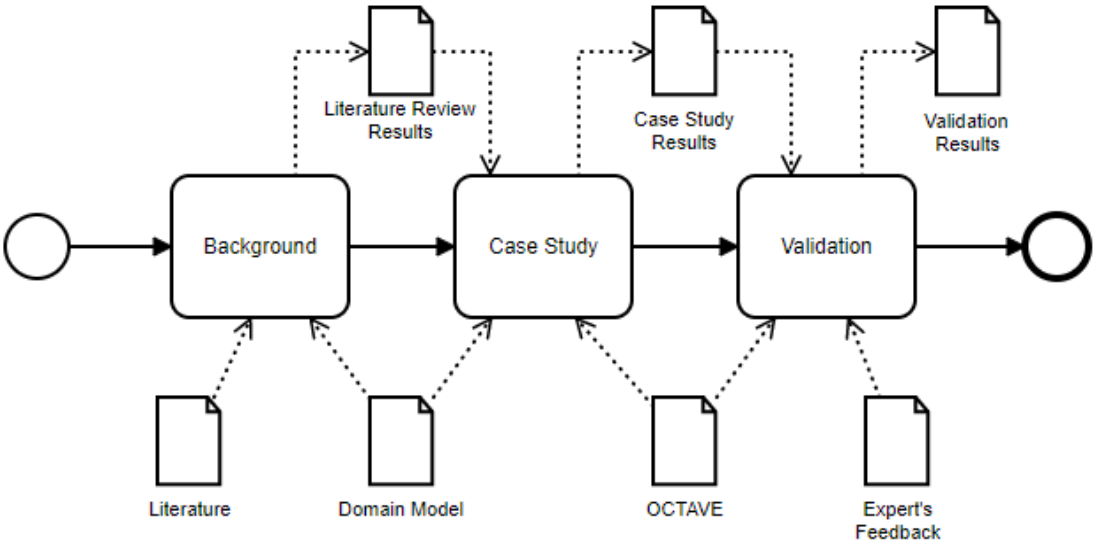


Figure 3. Research Method diagram.

## 2.8 Summary

In this chapter the Security Risk Management is discussed. The definition to what it is, some methods and concepts are given. Later, SRM and OCTAVE, are chosen and explained in more detail. Next, the combined method of using SRM and OCTAVE together is provided. Finally, the research method is explained. In the next chapter state of the art and literature review is done.

# 3 Background

In this chapter the State of the art is presented. A literature review is conducted to find relevant literature about the system, risks and countermeasures in the autonomous vehicle research field. Based on the literature discussed in the literature review system assets, business assets, risks and countermeasures are defined.

## 3.1 State of the Art

Autonomous vehicles (AV) are a sub class of Intelligent Transport Systems (ITS) which in their concepts are part of Internet of Things (IoT). All of those parts are connected to each other, so looking into the existing research is necessary. It is important to understand that concepts from IoT and ITS also apply to AV as it is a part of them. The focus will be on the more recent research for IoT and ITS fields, from 2018 and onwards, as the field is rapidly evolving. AV literature did not have a specified publish date to gather more relevant literature for better coverage.

In the recent years, Internet of Things (IoT) is only getting more popular and with that, the research on its security is in more demand. In the work by Sengupta et al. [18] they report object based categorization of attacks in IoT, which by their words is useful for the people using IoT solutions in their work domain. Finally, they present robust solutions to some of the risks described. Meneghello et al. [19] discuss multiple different cybersecurity scenarios and challenges are explained. Later they provide analysis on some existing security algorithms and protocols. Wang and their team [20] analyse 5G wireless technology impact on IoT applications. This was done by giving characteristics and threats in 5G IoT networks and later discussed physical-layer security solutions.

Intelligent transport systems are a research field growing rapidly in the recent years. As a part of the IoT, it shares the generic concepts from there, but is also focused on different transportation systems. A comprehensive survey on vehicular ad-hoc networks' (VANET) security is done by Malhi et al. [21]. Various attacks and problems are discussed, later proposing solutions to them. Similar topics are discussed by Sharma and Kaushik [22], where traffic efficiency and drivers' safety using different connection types is analysed. VANET's and other connections are analysed in a survey by Sheikh et al. [23]. The main focus for them was VANET security services, giving an overview of the current state-of-art. Based on that, they reviewed different authentication algorithms and looked into how fake malicious nodes could be identified. Vehicular social networks (VSN) are discussed by Wang et al. [24], who claim that they were the first to provide comprehensive review of the existing research on privacy preserving requirements and solutions on VSNs. It was done by comparing VSNs to Online Social Networks, MSNs and Social Internet of Vehicles, analysing the outcomes and providing the issues some countermeasures.

Autonomous vehicle research is quite new and rapidly growing. With that he security aspects of it is getting more important. A comprehensive work on risk management in AV was not found. The most relevant work was done by Sheeman and their team [25]. In that work, they use neural networks on Common Vulnerability Scoring System (CVSS) to calculate their score. Unfortunately, they do not provide support for choosing mitigation actions and defining own risks as all the risks are from CVSS database. Some other works give examples on some very specific parts or where the focus instead of security was actually on safety [26, 27]. NHTSA has provided their best cybersecurity practices to use in modern vehicles [28]. A review on safety failures, security attacks and countermeasures are analysed by Cui et al. in their work [29]. Different attacks on commonly used sensors like radar, LiDAR and cameras are described and carried out by Yan et al. and Petit et al. [1, 5]. Similar attack are

described by Thing and Wu [3], who also explain different attack on connections and networks. Scalas and Giacinto provide possible countermeasures for generic risks [9]. Some risk assessment was done by Dominic et al. [30], who list risks for AV and provide some scores for all of them based on their impact, likelihood and other similar characteristics.

## 3.2 Method for Literature Review

The literature review was done in a semi-systematic way. Most of the literature used in this work was gathered using Scopus with different search strings. In chapter 2 and 3.1 the focus was put on the parts needed to be looked into. For example, finding relevant literature for security management in IoT field was done using string "*TITLE-ABS-KEY ("Security management" AND "internet of things")*". Similar search terms were used for ITS and AV too. Additional search was also done using Google Scholar.

Papers used were selected based on the relevancy in their title, abstract and lastly their contents. The criteria for choosing was as follows:

- Focus on *security* and not *safety*,
- Focus on main research field (IoT, ITS, AV),
- Published 2018 or after for IoT and ITS, no specified time for AV,
- Relevance for this topic.

As seen in the state of art review in the literature, a comprehensive analysis of risks, their impact and countermeasures on AV's was not found. There is work done with a few concrete attacks and risks on only some parts of the AV system, like attacks on LiDAR. The closest to a comprehensive overview of risks in AV is done by Thing and Wu in [3]. In that work, some risks are described with some potential defences against them. Unfortunately, it lacks giving motivation and impact of the risks to AV. Petit and Shaldover [4] identify some cybersecurity risks, estimate the severity and give some mitigation strategies for them. It is mentioned that their work was the firsts steps to show risks in AV and was done to raise awareness in the field. Attack experiments on sensors used in AV are explained by Yan, Petit and their respective teams [1, 5]. Sung and their team [31] discussed the AV infrastructure and how the components work together to make the autonomous driving possible. Maple et al. [2] provide AV reference architecture and attack surface analysis. They only mention possible risks and do not go in detail in their description for most of them. Scalas and Giacinto list some possible vulnerabilities and some ways to deal with them [9].

## 3.3 Assets

**System Assets.** Security modelling is based on knowing and having a good overview of the system assets (referred as *IS asset* in SRM). Affia et al. [32] provide a systematic way to do it based on analysis of IoT and ITS. Autonomous vehicles are a subset of those, so the findings can be used for this too. According to them, the system can be divided into three different parts: *perception, network* and *application layers.* Such layering can be applied to the concepts explained in SRM. All the system assets can be seen in Figure 4.

*Perception layer* includes the software and hardware of the system responsible for collecting and controlling the data. In AV, those include the devices for sensing, positioning, seeing. In the literature, examples of such devices are radars, LiDAR, GPS, cameras [1, 3, 5, 31].

In *network layer* all the data collected by *perception layer* is transferred. The transfer can be wireless or wired, depending on the components and system's needs. The vehicles own network is also added to this layer. The in-vehicle networks are controller area network

(CAN) and local area network (LAN) [3, 31]. CAN is used to exchange data between different components in the vehicle. In AV, LAN is used to deliver data from the different sensors to the application layer where the data will be used. The cars are also connected to the Internet.

The last layer is *application layer*, that is responsible for connecting the previous layers to the end users. It consists of computers, servers, data storage or even humans if needed. In the AV context, the application layer can work with the data from sensors to calculate routes and control the car based on the calculations. The calculations are done using a computing unit (industry oriented computers in most cases) [3, 31]. The calculation results are then converted into commands and actuation module will use those to drive the car. The layer also includes Electronic Control Units (ECU) which are developed and installed by the car manufactures and control the electronics in the car.

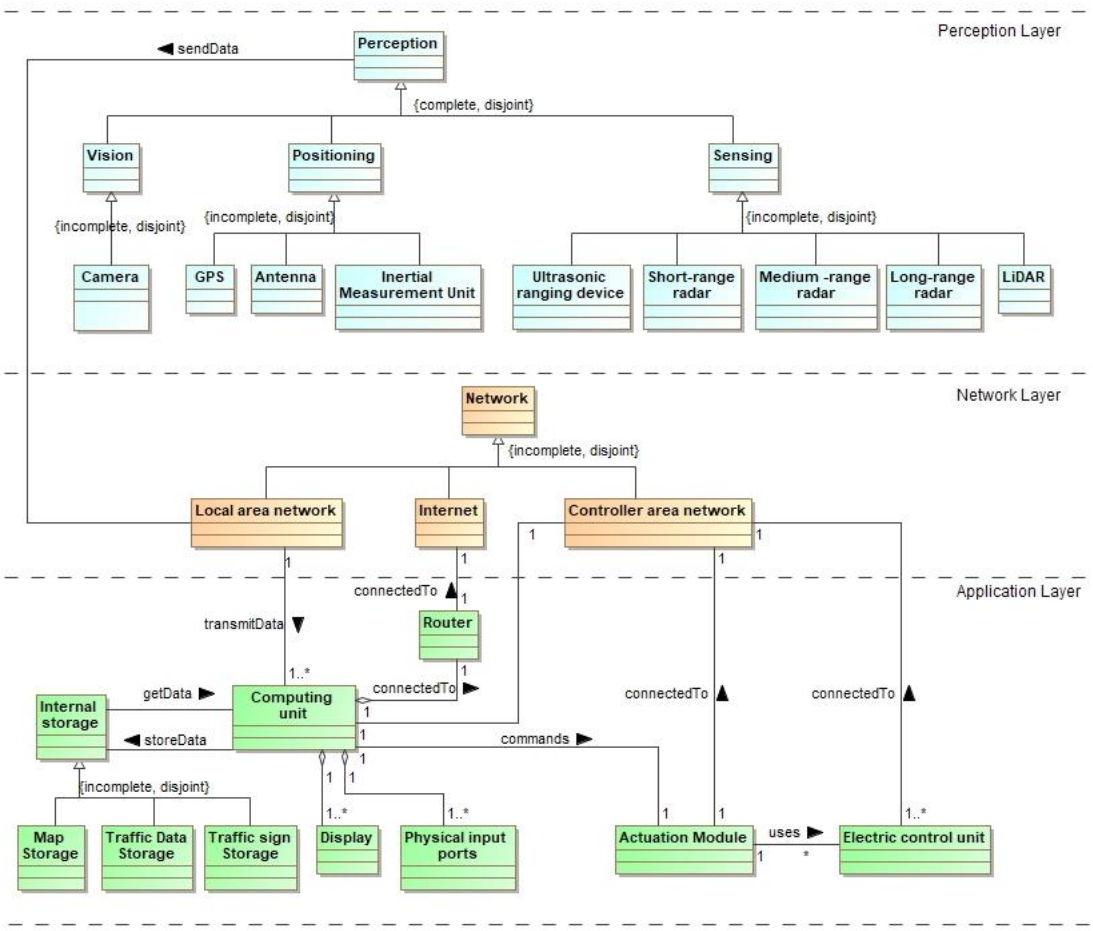


Figure 4. Autonomous Vehicles' system model.

**Business assets.** Business assets are generally some data or software that the system assets are working with. The business assets are defined in Table 1. The business assets are divided into different groups depending on which layer their origin is on the system assets model. The layers are perception, network and application. On Figure 5 the basic data flow in an AV is shown. It is divided into three steps: sensing, understanding and acting. Sensing is done in the perception layer while understanding and acting are done in the application layer.

Table 1. Business assets

| Layer | Business asset |
|---|---|
| Perception | Video and picture data, image data, vehicle location data, vehicle travel data, working vehicle data, ultrasonic sensors data, surrounding environment data, radar data, inertial measurements data, measurement data |
| Network | Communication data |
| Application | Map data, traffic data, traffic sign data, computing data, actuations' commands data, fused data, ECU's data, decision maker, driving planner, system software, autonomous driving |

All the business assets in the perception layer are data collected by the system assets in the same layer. This includes *video and picture data* from cameras, *vehicle location data* from GPS and so on. All that data can be described as *perception data*. After the data is collected, it is transmitted through the network, where it is considered *communication data*. It is not only the data from perception layer, but also different messages and data exchanged between different system assets in the application layer.

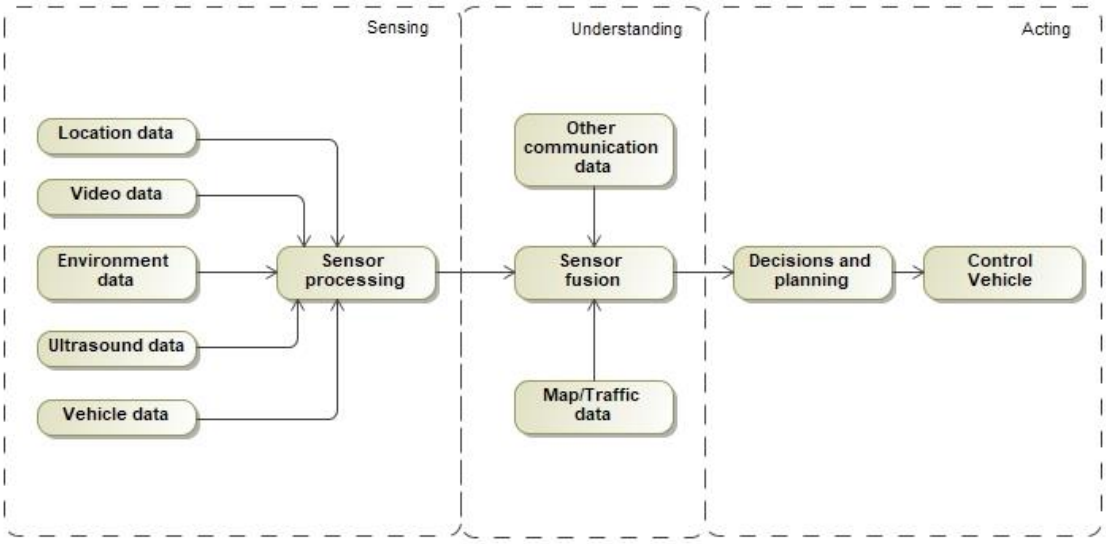


Figure 5. Data flow in AV, adapted from [5].

In the application layer, the data from the perception layer is worked with. The cameras and sensors deliver raw, unprocessed data as the *communication data* that needs to be transformed by the computing unit. After the first processing, the perception data will be fused with the data from storage and is considered *fused data*. Different *driving planners* will find the optimal way to proceed with the driving, based on the *fused data* and *stored data (map, traffic and sign data). Decision maker* is the final action from computing unit and is responsible to act on obstacles, limitations etc. from the *fused data.* Combining the planned route

with the *decision maker* and *driving planner* the final commands to the actuation unit (*actuations' command data*) are delivered and the vehicle will start acting based on those. The controlling is done by the actuation unit, which uses the ECU's to do so. All the processes, systems and data can be generalized as *autonomous driving*.

## 3.4 Security Threats and Risks

The threat descriptions are selected from the literature [1-5, 9] and the risks based on those defined using SRM method. The summary of risks is presented in Table 2. The summary consists of affected layer or layers, risk ID, the source for the risk and its name. Detailed definitions for all the selected risks are provided in Appendix I. The risks are mapped onto the assets model as illustrated in Figure 6. A total number of 23 risks are defined: 10 for perception layer, 7 for application layer and 4 for network layer. R17 can be found at all layers and R18 is defined for both network and application layer.

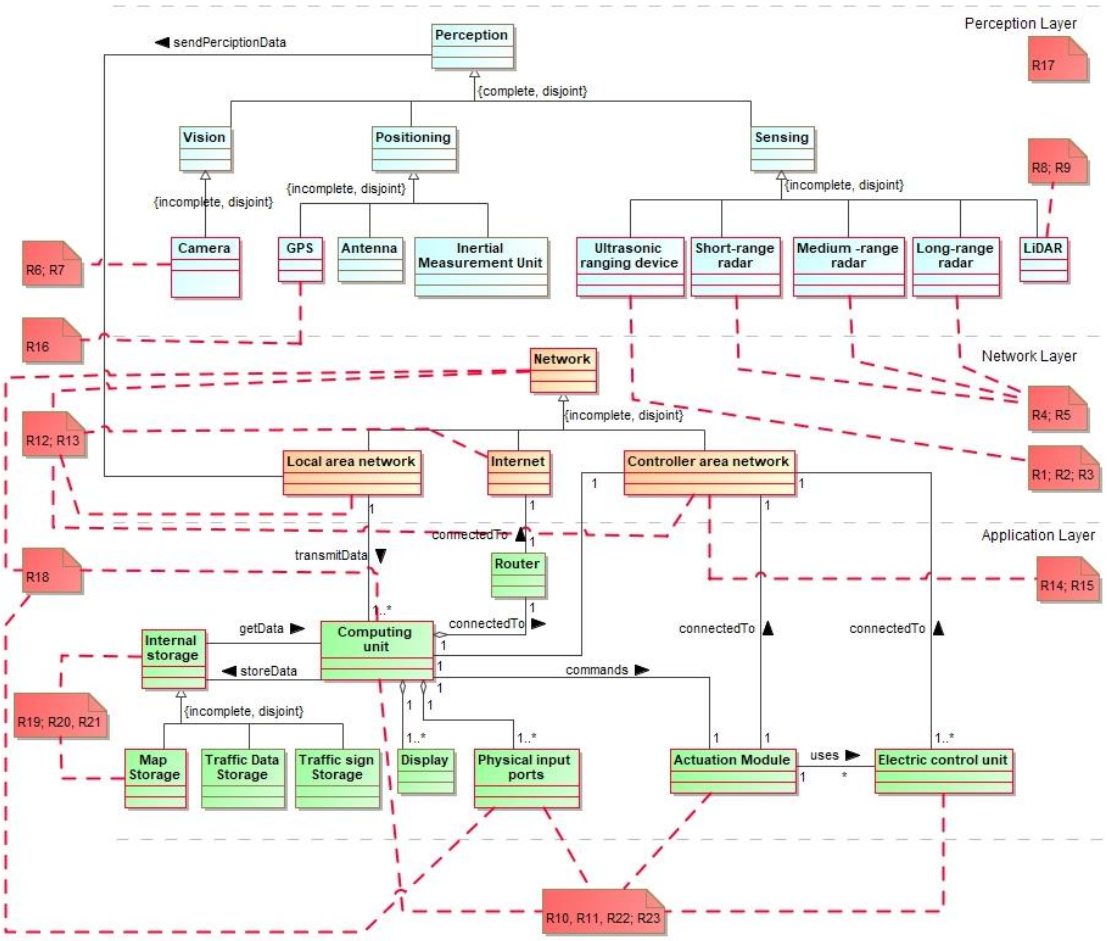


Figure 6. Risks mapped to system assets.

The found risks all apply to an autonomous car. Risks describing normal, street legal cars were not included. This means, the risks defined affect the sensors used in an AV, the communication between the components or the other parts installed in the car to make autonomous driving possible. An example of a rejected risk is faking wireless signal to open doors of the car. A risk like that also affects an autonomous car, but is out of the scope in this thesis.

Table 2. Table of defined risks

| Layer | Source | Risk ID | Risk name |
|---|---|---|---|
| Perception | [1-3] | R1 | Jamming ultrasonic sensors |
| Perception | [1-3] | R2 | Spoofing ultrasound sensors |
| Perception | [1, 2, 4] | R3 | Acoustic quieting on ultrasound sensors |
| Perception | [1-4] | R4 | Jamming radar |
| Perception | [1-4] | R5 | Spoofing radar |
| Perception | [1, 2, 5] | R6 | Blinding cameras |
| Perception | [5] | R7 | Confusing car controls using camera inputs |
| Perception | [2, 5] | R8 | Relay attack on LiDAR |
| Perception | [2, 3, 5] | R9 | Spoofing LiDAR |
| Application | [3] | R10 | Code modification |
| Application | [3] | R11 | Code injection |
| Network | [3, 9] | R12 | Packet sniffing |
| Network | [2, 3, 9] | R13 | Packet fuzzing |
| Network | [4] | R14 | Inject CAN messages |
| Network | [2, 4] | R15 | Eavesdropping CAN messages |
| Perception | [2, 4] | R16 | GPS jamming |
| All | [4] | R17 | EMP attack |
| Network and Application | [4] | R18 | Malware injection |
| Application | [2, 4] | R19 | Manipulate map data |
| Application | [2] | R20 | Extract map data |
| Application | [2] | R21 | Delete map data |
| Application | [2] | R22 | Disable actuation module |
| Application | [2] | R23 | Induce bad analysis |

## 3.5 Countermeasures

The proposed countermeasures for the defined risks are listed in Table 3. The table consists of the risk ID what the countermeasure is for, the source for it and a short description. All the previous risks have at least one countermeasure given and one countermeasure can be linked to multiple risks. For example, noise detection and cancellation would mitigate any risk on the sensors affected by a jamming risk. The proposed countermeasures can be seen implemented on the system assets on Figure 7.

Countermeasures for the assets in perception layer are adapted from [1, 5]. In those papers, the risks for sensors were explained and some mitigation tactics for them given. In the work by Yan et al. [1] one of the countermeasures mentioned was noise detection and rejection. Small amount of noise is normal for the sensors to pick up, but detecting sudden big outburst of that can indicate some malicious activity. It was said that many of the sensor applications have been implemented with noise detection in mind. The second countermeasure for attacks on perception layer was to simply have multiple sources of similar input for redundancy check [1]. Having multiple of same type of sensors covering the same area will greatly reduce the risks impact as affecting all the sensors at the same time requires more tools and knowledge. Redundancy check will allow the AV to keep working even if multiple sensors are under attack as long as one of them can provide the necessary inputs. To make it harder to work around the redundancy check, it is recommended to add randomness to the control

parameters, have some kind of logic check and attack detection system built in. Thing and Wu [3] focus was on cameras and LiDAR. For both of them, the similar countermeasure was to have multiple of the same type of inputs. Cameras could also be protected from some attacks using light filters to filter out harmful light sources, like lasers used in their experiment. The filters can vary on the use cases, some can only filter one type of light while others are made from materials capable of filtering multiple sources and chance its colour and opacity depending on the input. For LiDAR the recommended countermeasure was to use random probing. For the attacks described by Petit et al [5] the attacker needed to know the scanning interval to fire the pulse back. Adding some randomness to the rotation speed or scanning interval will make it a lot harder for the attacker send the pulse at the right time. Unfortunately, some LiDAR's require constant rotating speed so the random probing cannot be used. In such cases, shortening the pulse period will make it harder for attacker to send the pulse at the exact right time, but will also shorten the working radius of the LiDAR. Thing and Wu [3] say that a way to avoid GPS jamming is nullification. Nullification refers to the usage of cybersecurity and electronic capabilities of the devices to invalidate or neutralize the attack.

Table 3. Countermeasures

| Risk ID | Source | Countermeasure descriptions |
|---|---|---|
| R1 | [1] | Noise detection and rejection; Multiple sensors for redundancy check |
| R2 | [1] | Noise detection and rejection; Multiple sensors for redundancy check |
| R3 | [1] | Multiple sensors for redundancy check |
| R4 | [1] | Noise detection and rejection; Multiple sensors for redundancy check |
| R5 | [1] | Noise detection and rejection; Multiple sensors for redundancy check |
| R6 | [1, 5] | Overlapping image output (multiple cameras); Filter to remove harmful light |
| R7 | [1, 5] | Overlapping image output (multiple cameras); Filter to remove harmful light |
| R8 | [1, 5] | Multiple LiDAR inputs; Random probing; Shorten pulse period |
| R9 | [1, 5] | Multiple LiDAR inputs; Random probing; Shorten pulse period |
| R10 | [3, 9] | Device authentication; Anti-Malware; Isolation |
| R11 | [3, 9] | Device authentication; Anti-Malware; Isolation |
| R12 | [3, 9] | Encryption; Device and user authentication |
| R13 | [3, 9] | Encryption; Device and user authentication |
| R14 | [3, 9] | Encryption; Device and user authentication |
| R15 | [3, 9] | Encryption; Device and user authentication |
| R16 | [3] | Nullification |
| R17 | [3, 9] | Isolation |
| R18 | [3] | Firewall; Anti-Malware; Isolation |
| R19 | [3, 9] | User authentication; Device authentication; Isolation |
| R20 | [3, 9] | User authentication; Device authentication; Isolation |
| R21 | [3, 9] | User authentication; Device authentication; Isolation |
| R22 | [3, 9] | Isolation; Access control |
| R23 | [3, 9] | Isolation; Access control; Input validation |

The most recommended countermeasure for network layer is using encryption [3, 9]. Thing and Wu [3] say that encryption is fundamental to use in communication. Some schemas will allow the identification of the sender by using their personal key. Device and user authentication is the next recommended countermeasure for the network layer [3, 9]. Knowing where the data came from will make it easy to avoid getting harmed by the attacker sending malicious code or malware. Using encryption and authentication the integrity and confidentiality of the communication data can be assured.

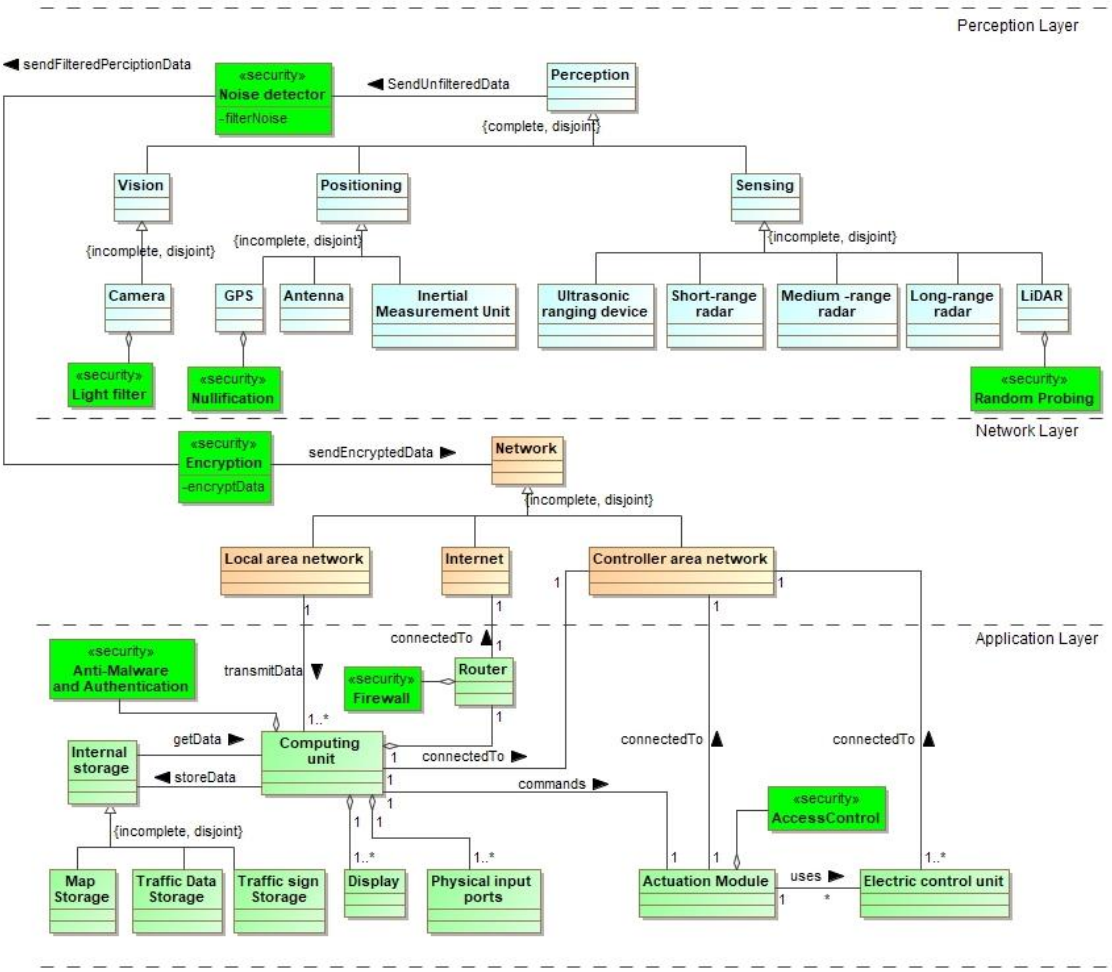


Figure 7. Countermeasures on system assets.

The countermeasures for the application layers are based on the works by Thing, Wu [3] and Scalas, Giacinto [9]. The first recommended countermeasure is to install anti-malware software on the computing unit. It will help even if some malware is installed in the system, anti-malware can stop its work and remove all the malicious software. It will also help detecting any tries to install malware from source. With the anti-malware, firewall needs to be installed as well. Another important to mitigate risks is to have authentication integrated. Knowing who or what sends the data was already mentioned, but any component in the system should not be able to use others if it not explicitly required for the AV to work. Authentication will reduce the chance for outsiders to gain access to any of the components. Similar to authentication, access control methods should be implemented. Knowing who and when have tried to gain access to some component is crucial to stop the spread of malicious software or patch up any appeared vulnerabilities. As a last resort, there should be a

way to isolate any affected components to avoid giving access to the attacker or stopping the spread of malicious software.

## 3.6 Countermeasure Descriptions and Estimated Costs

In this section, the countermeasures selected from the literature are given a description and an estimated value of implementing them in an AV.

**Noise detection and rejection** can be done by implementing noise detection algorithms. Ultrasonic sensors, radar and LiDAR inputs can be filtered that way. The algorithms and exact way of the implementation varies between them, but an overall estimate cost will be similar. In [33] an approach to detect and filter unwanted noise for radars is explained. The radars were used for traffic monitoring in a tunnel in their case, instead of autonomous driving. Similar approach can be applied for autonomous driving. They concluded that using their module provided better accuracy and less detection delay. The only cost for this kind of approach is the implementation of the algorithm, which is relatively low.

**Multiple sensors for redundancy check.** The easiest way to detect errors and unwanted inference on the sensors is to have multiple of them. Having an overlap from the same type of sensors makes it easy to discard invalid inputs and could provide enough coverage to continue driving even if one of the sensors goes offline. The cost to implement this is the price of an additional senor. Depending on the component, the price can vary a lot. For example, getting additional LiDAR is expensive as they can cost around €8,000, but have seen price reductions in the recent times.

**Filter to remove harmful light** can reduce the interference caused by sudden bursts of light inputs. Those can be caused by high brightness flashlights or lasers. Using such devices on cameras does not only make the image useless, but also can damage the camera lens and sensors. Adding filters to the lens will reduce the possible damage caused by harmful lights. The filters, depending on the cost, may also interfere with the image quality in normal conditions. Off the shelf products (under €100) can provide some protection but reduce the image quality. Custom filters could detect to reduce normal condition interference and protect against multiple types of harmful light, but will cost many times more.

**Random probing.** Normally, LiDAR fires its pulses with fixed intervals, making it easier to interfere with. Knowing the exact scanning speed makes it easier for the attacker to synchronize the attack. Implementing random probing to randomly change the firing periods will make it harder for the attacker to synchronize their attack. Random probing can be implemented by tinkering with the LiDAR settings, making it relatively cheap. Doing this on a rotating LiDAR will be problematic, as it requires constant speed and needs to know exact firing angles and periods. Random probing in this case can be implemented as periodically skipping some pulses, making it easy to detect interference if some input is received at times where none should have been received.

**Shorten pulse period.** Similar to the random probing, shortening pulse period on LiDAR will make it harder for attacker to carry out their attack. Shortening the pulse period also reduces the attack window for the attacker. Implementing this countermeasure will again require some LiDAR setting changes. Unfortunately, reducing the pulse period also lowers the maximum range and because of that, it requires carefully thought out implementation to avoid further problems.

**Device and user authentication, Access control.** Knowing who, what and from where tries to connect to the system is important to avoid any kind of unwanted interferences. Implementing authentication for every device and user greatly reduces the risk of unwanted connections. Many different ways to implement authentication can be found. For autonomous driving, Haggerty et al. [34] present a solution gateway to implement communication in a AV with authentication in mind. As AV could be used for a taxi service, Lu et al. [35] present a solution to authenticate customers at the pickup location, based on their computing device. Authentication is important for access control too. Limiting the access for certain users or device will increase the overall security in the system.

**Anti-Malware and firewall**. Having a firewall to block unwanted connections and using anti-malware software is a norm nowadays. Both of those are easily used in the AV computing unit too. The cost of business orientated solutions for both of them is around €300 per month, making it relatively cheap for smaller amount of systems [36]. With the vehicle count going up, the price will too.

**Encryption.** Encrypting sensitive data is an easy way to mitigate the damage done by an attacker. Getting encrypted data has near to no use for the attacker without any ways to decrypt it. Depending on the solution required the price can vary a lot. Setting up a custom encryption service can cost €10,000 or even more, while using premade solutions from a third party is a lot cheaper.

**Isolation.** Cutting any connection to an infected component is crucial to save data from leaks and more damage done by an attack. To do it, some solution to detect an attack real-time is needed. Also, in AV, the system needs to guarantee the passengers safety in case of attack and some component needs to be isolated. Implementing such solution requires the engineers' time and could cost a lot in the long run.

**Nullification**. Nullification in this case refers to GPS ability to invalidate and neutralize cyberattacks. For some models, anti-jamming technology is available. It can be implemented by installing antennas with anti-jamming support. Those were originally made for military use [37] and because of that, the price range is high.

**Input validation.** Checking the inputs for harmful code snippets or various logic errors is required for the AV to work without any interruptions. Finding any invalid or harmful inputs before they are worked with greatly reduces possible harm. Implementing input validation should be done while building the system to avoid more expenses later on. Doing error handling and checking the inputs will only slightly increase the cost of the overall system implementation.

## 3.7 Summary

In this chapter the state of the art and literature review is presented. Based on the findings assets, the risks on those and countermeasures are defined. In the next chapter, the findings are put to use in a case study.

# 4 Case study

University of Tartu and Bolt work together to develop an autonomous driving vehicle capable of providing taxi service for customers. In the project, eight work package are present focusing on different aspects. This work is part of the *security* package. The other packages work on controlling the car, end-to-end driving, mapping, safety and human interaction. All the packages depend on the other ones to provide competitive solutions in the research area. The prototype is built on Lexus RX450h. An overview of the car and its components is presented in this chapter. After that, based on the literature, the system assets and business assets are defined. All the risks and countermeasures defined in Chapter 3 are analysed in the Bolt project context.

## 4.1 Components

The Bolt car base model is Lexus RX450h. The Lexus model is chosen for its compatibility with different autonomous driving methods and components. It is also supported by AutonomousStuff [38]. The car has prebuilt system to support driving by wire, meaning the car is controllable using a game controller. That system is the basis for autonomous driving as it allows controlling the car using electrical inputs. The game controller can be replaced with a computer giving the inputs instead of a human. Into that car, many other components required for autonomous driving are installed. In the following, short description of the components is given with the model used in Bolt.

**LiDAR**. As most of the autonomous vehicles, Bolt uses Light Detection and Ranging device (LiDAR) in their prototype. In concept, LiDAR uses lasers to measure and map the data of its surroundings. It consists of a laser, scanner and GPS receiver made specially for use in LiDAR systems. Using the components, the laser is used to send out a beam which is after contact with some object is mapped out into a point cloud. After running the system, the outcome will be a detailed point cloud of the surrounding objects mapped out with exact coordinates relative to the system itself. In autonomous vehicle field, LiDAR is used to map out of surrounding vehicles and objects while driving. The data then is used to make driving decisions. The LiDAR model used in Bolt system is VLP32C [39]. It is a product by Velodyne and has 360° horizontal and 40° vertical field of view. The VLP32C LiDAR has a working range of 200m.

**Cameras**. In autonomous vehicles, cameras are used to get real-time high-definition footage of the surroundings. The footage is used to detect and identify traffic signs and lights using machine learning and AI algorithms. It can also be used for detecting pedestrians and other vehicles and predict their movements to avoid collisions. In Bolt car, multiple different cameras are used. First, Mako cameras [40] which are made for usage in machines to gather visual data. Those are mounted in the front window rack. The second type of cameras are SF332X-10X from Sekonix [41] with 120° field of view. A total of four of them are mounted on the roof of the vehicle.

**Radar**. Radars are used to gather information about the surroundings. In autonomous vehicles, it is used to get speed and range data of the vehicles around the radar. Radar is mostly used in automatic braking and lane changing systems, which require confirmation of the surroundings that the manoeuvre will be safe. The range of the radar can vary from short to long, depending on the model and application of it. The radar used in Bolt autonomous vehicle is Delphi ESR 2.5 24V [42]. It has the capabilities of medium and long range radar. Both of the options can be used to get the best results. The medium range radar has a wide angle, making it possible to detect even pedestrians on the road sides. Long range one is

used to gather the data from vehicles ahead, giving accurate speed and range data from up to 64 different objects.

**GPS and IMU**. For navigation through the traffic, the AV needs very accurate data of its location. GPS is used for that. GPS systems use the satellites around the earth to get accurate data of the location and also time. Both of which are important for autonomous vehicles. Bolt AV is equipped with Novatel GPS PwrPak7 [37]. It uses the Global Navigation Satellite System (GNSS) technology with a small internal storage. It is compact and lightweight with support for multiple different communication interfaces. In this vehicle, the GPS is paired with an Inertial Measurement Unit (IMU): IMU-IGM-S1/STIM30 [43]. The IMU uses gyro and accelerometer to give 3D navigation data which can be accurate even in cases where the satellite connection is temporarily blocked. In addition, Novatel GPS Antennas are used to get better tracking performance.

**Computing Unit**. All the data from the sensors needs to be analysed and worked with. Using high-end computer parts is the standard for this in autonomous vehicles. The computer needs to be able to handle large amount of information all at once and calculate the optimal routes. Spectra industrial computer [44] is chosen to be used in the Bolt machine. The computer is installed with a GTX2080 GPU, GIGe Ethernet card and Kvaser 4x channel card. All this lets it handle large amount of data from multiple sources at once.

**Actuation module.** Actuation module in the AV is used to carry out the driving. It is responsible for steering, accelerating, braking and so on. The driving is done by controlling the Electronic Control Units (ECU). ECU's are part of the car and are responsible for controlling the car in normal driving mode to assist the drive. The actuation module used in the Bolt prototype is Platform Actuation and Control Module (PACMod) version 3.0 from AutonomousStuff [45]. It provides support for by-wire control and many safety features. The system uses CAN interface for communication and is based on Robot Operating System (ROS).

**Convenience features.** The AV built by Bolt is equipped with many components and features that help the testing, driving and development process to be more convenient. The wAP router [46] is installed to connect the car to the internet. To connect the computer and other components to the CAN network, the Kvaser USB to CAN hub is used. In addition to the CAN hub, a normal USB hub is added to connect different convenience components like a keyboard and mouse. Multiple screens are installed in the car to monitor the driving process. The convenience components are listed here:

- wAP ac LTE6 kit router,
- Kvaser USB-CAN hub,
- 1x Wireless keyboard and mouse;
- 1x Centre console mounted USB hub with 4 ports;
- 1x 1Gbit Ethernet switch;
- 1x Ethernet hub on dashboard;
- 2x Headrest mounted monitors;
- 1x Custom roof and trunk racks;
- 1x HDMI splitter;
- 1x Custom conduit design;
- 1x Custom cooling system;
- 1x 16 channel power distribution system with touchscreen.

## 4.2 Bolt Prototype's Assets

**System assets**. Based on the component descriptions the Bolt prototype's system assets model is made (Figure 8). The placement of the components is made by following the system asset model (Figure 4) based on the literature, where the assets are divided into three layers. Individual components from the Bolt are mapped to the similar ones in the literature based system asset model and changes are done if the Bolt prototype car had differences in the architectural decisions (i.e. radar is connected to CAN).

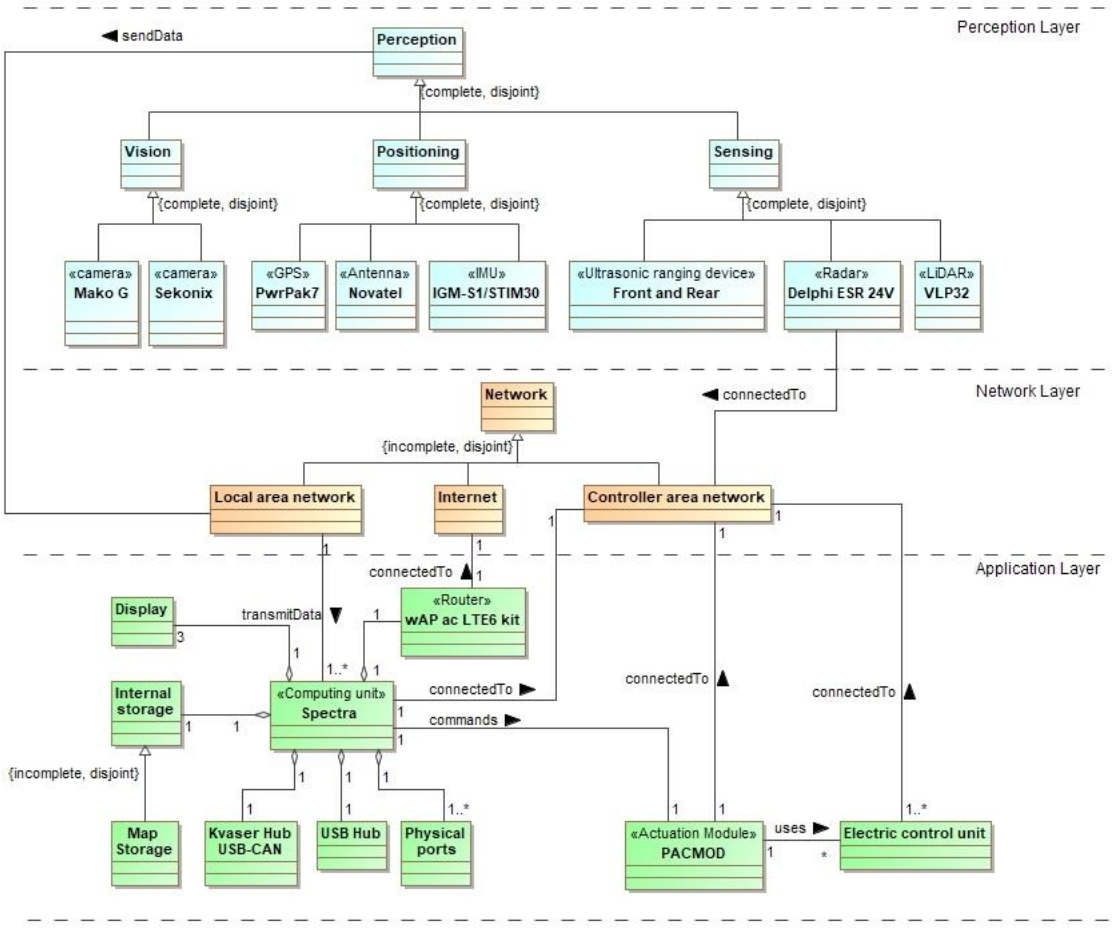


Figure 8. Bolt AV system assets.

**Business assets.** The business assets are defined in Table 4. The table consists of the primary layer of the asset, the business asset name with a short description and associated system assets. The overall structure of the business assets is based on the literature (see Chapter 3.3). There, the basic model of data flow is present with a short discussion on how it works.

Table 4. Bolt AV business assets.

| Layer | Business asset | Description | Associated system assets |
|---|---|---|---|
| Perception | Video data | Video from surrounding environment | Mako G, Sekonix cameras |
| | Picture data | Pictures from surrounding environment | Mako G, Sekonix cameras |
| | Vehicle location data | Current location of the vehicle | PwrPak7 GPS, IGM-S1 IMU |
| | Vehicle travel data | Routes used with the time | PwrPak7 GPS, IGM-S1 IMU |
| | Working vehicle data | Vehicle speed, direction etc. | PwrPak7 GPS, IGM-S1 IMU |
| | Ultrasonic sensors data | Data from the ultrasound sensors about surroundings | Ultrasonic sensors |
| | Radar data | Data from radar | Delphi ESR 24V |
| | Surrounding environment data | Data about the surrounding environment and objects | VLP32 LiDAR, Delphi ESR 24V, Ultrasonic sensors |
| | Inertial measurements | Vehicle speed, angle, location (used in case no satellite connection) | IGM-S1 IMU |
| Network | Communication data | Data and messages exchanged by different components | Network |
| Application | Map data | Map used for autonomous driving | Map storage |
| | Fused data | Combined data from perception layer | Perception layer, network, Spectra computer |
| | Computing data | Results from analysing the fused data | Spectra computer |
| | Actuation commands data | Commands generated to be sent to actuation module | Spectra computer, PACMod v3.0, ECU |
| | Decision maker | Software for making driving decisions | Spectra computer |
| | Driving planner | Software for planning out the route used | Spectra computer |
| | System software | All software used for autonomous driving | Spectra computer |
| All | Autonomous driving | Overall process of vehicle self-driving | All parts |

## 4.3 Security Risks

The security risks for Bolt car are adapted from the literature and can be seen in Chapter 3.4, with descriptions and sources. As the system and business assets for Bolt are defined based on the literature, all the risks found for literature can also be defined for the Bolt AV. In Table 5 the previously defined risks are associated with the corresponding assets from

Bolt's model. The table consists of the risk ID with its name, associated system assets and the risk score. Risk score is calculated by getting the relative risk score from the OCTAVE sheet and multiplying it with likelihood. To fill in the sheets, some criteria is defined and used (Appendix III). The sheets include risk definition, asset values, likelihood, impact and also the countermeasures to mitigate those risks. An empty worksheet can be seen in Appendix II. All the filled sheets can be seen in Appendix IV.

Table 5. Bolt AV security risks.

| Risk ID | Risk name | Associated system assets | Risk score |
|---|---|---|---|
| R1 | Jamming ultrasonic sensors | Ultrasonic ranging devices | 32 |
| R2 | Spoofing ultrasound sensors | Ultrasonic ranging devices | 32 |
| R3 | Acoustic quieting on ultrasound sensors | Ultrasonic ranging devices | 12 |
| R4 | Jamming radar | Delphi ESR 24V | 32 |
| R5 | Spoofing radar | Delphi ESR 24V | 32 |
| R6 | Blinding cameras | Mako G, Sekonix cameras | 48 |
| R7 | Confusing car controls using camera inputs | Mako G, Sekonix cameras | 32 |
| R8 | Relay attack on LiDAR | VLP32 LiDAR | 16 |
| R9 | Spoofing LiDAR | VLP32 LiDAR | 14 |
| R10 | Code modification | ECU, Spectra computer | 17 |
| R11 | Code injection | ECU, Spectra computer | 18 |
| R12 | Packet sniffing | Network components | 24 |
| R13 | Packet fuzzing | Network components | 15 |
| R14 | Inject CAN messages | Controller area network | 12 |
| R15 | Eavesdropping CAN messages | Controller area network | 15 |
| R16 | GPS jamming | PwrPak7 GPS | 32 |
| R17 | EMP attack | All parts | 12 |
| R18 | Malware injection | Spectra computer | 36 |
| R19 | Manipulate map data | Map storage | 12 |
| R20 | Extract map data | Map storage | 12 |
| R21 | Delete map data | Map storage | 12 |
| R22 | Disable actuation module | PACMod v3.0 | 14 |
| R23 | Induce bad analysis | Spectra computer | 14 |

## 4.4 Countermeasures and Their Cost

In this section the approximate cost for each countermeasure defined in Table 3 is given.. In Table 6 all countermeasures and its estimated costs for Bolt prototype are shown. *Low* cost means the countermeasure can be implemented by working engineers without requiring expensive purchases. *Medium* cost is given to countermeasures which require moderate amount of time and money (€1,000 to €10,000) for new components or services. Anything *High* requires a lot of time and costs can go over €10,000. Some costs will be abstract there, like *multiple sensors for redundancy check*, because of the different cost for the components. Countermeasures and their costs are also presented in mitigation section of the OCTAVE sheets (Appendix IV).

First countermeasure for perception layer is noise detection and rejection, which can be used for all the sensors in the Bolt prototype. The cost of implementing that is *Low* as it only

requires implementing an algorithm for it. The second countermeasure, multiple sensors for redundancy check, can also be used for all the sensors. It can be implemented by duplicating all the sensors to check for errors between them, but also using different type of sensor to cross-check their validity. The cost of having multiple sensors depends on the sensor type. While cameras could have *Low* cost, having multiple VLP32 LiDAR's in one car will be expensive. Both model of the cameras used in the Bolt prototype can be protected by using filters to remove harmful light. Depending on the filter solution the cost varies from *Low* to *High*. The next two countermeasures are for the VLP32 LiDAR. Both, random probing and shortening the pulse time, will have a *Low* cost as they only require some tinkering in the settings.

Device and User authentication is a good countermeasure for different type of attacks requiring having access to some devices. Implementing it would require *Medium* funds as every component in the system needs to be identified. Authentication should also be combined with access control. Removing unnecessary access for users lowers the possibility of a high impact attack after an attacker gets access to such user profile. In similar category would be input validation. All inputs should be checked for where it came and if the sent data is valid and not been modified. Isolation is used to cut off components to avoid additional infection in case of an attack, implementing such solution is evaluated at *Medium*.

Installing anti-malware and firewall in the system is basic security countermeasure. The cost is *Low*, but having them in the system greatly reduces the chance of malware being installed. Anti-malware is also used to find harmful software and getting rid of it.

Having fully encrypted connection in the system would protect the data exchanged. Building such system is expensive, the different components in the system might not support encryption. In such case, having additional components to provide the encryption will greatly increase the cost of implementing the countermeasure.

Nullification is a countermeasure proposed for GPS spoofing. To implement nullification, a military grade antenna from Novatel is required. As the antenna is made for military use, the cost of it is *High*.

Table 6. Contermeasure estimated costs.

| **Countermeasure** | **Estimated cost** |
|---|---|
| Noise detection and rejection | Low |
| Multiple sensors for redundancy check | Low to High (depends on the sensor) |
| Filter to remove harmful light | Low to High (depends on type) |
| Random probing on LiDAR | Low |
| Shorten pulse on LiDAR | Low |
| Device and user authentication | Medium |
| Access control | Low |
| Anti-Malware | Low |
| Firewall | Low |
| Encryption | High |
| Isolation | Medium |
| Nullification | High |
| Input validation | Low |

## 4.5 Additional Risks

During the process of risk management some additional risks could be found. The risks could affect an autonomous car, but were not found during the literature review. Because of that, they were left out from the risk management, but are still worthy to be mentioned. Even with the risks defined in this section, more could be found and the list is not complete.

First such risk is modifying street signs. AV's use image recognition algorithms to detect and understand street signs. Slightly modifying the sign using markers or stickers still makes them understandable for human drivers, but image recognition might struggle.

An attack on the actuation module could be possible. An attacker gains access to it and starts controlling the car by giving the orders directly to the module. Letting an attacker to freely control the vehicle is catastrophic.

Attacking the router with a denial of service attack is possible. The car needs to be connected to the internet to download updates and losing the connection can lead to accidents on the road. This could easily happen if the map could not be updated after some construction works on the streets.

## 4.6 Summary

In this chapter the case study of Bolt autonomous driving vehicle is presented. First, the car used and all the components installed for autonomous driving are explained. Next the risks and countermeasures found in the literature are analysed in the Bolt project context to estimate their cost. Finally, some additional risks are mentioned. In the next chapter a validation of the work done in the Bolt project security aspects is discussed.

# 5 Validation

In this chapter the process of validation is described. Chapter 5 includes the feedback gotten during the validation, different suggestions and the main findings on the security risk management process done in the previous chapters.

## 5.1 Validation Process

The method chosen to carry out the validation was interviews with the experts familiar with autonomous driving and its security working in the project from University of Tartu and Bolt side. Two interviews were done for this. The experts were chosen for their knowledge in the autonomous driving or security risk management.

In the first interview, the expert from University of Tartu was present (Expert1). Expert1 is the head of multiple work packages and their main focus is on getting the car autonomously driving. They are also responsible for all the components used in the car and knows what the components do and what the future plans in the project are.

In the second interview, the experts from Bolt were present (Expert2 and Expert3). Expert2 is a security specialist from Bolt and interested in the autonomous driving field. Expert3 is the coordinator between University of Tartu and Bolt. They know and plan the project and is interested in the research going on.

During the interviews a short overview of the security aspects in the Bolt project were presented. Following that, all the 23 risks were explained. From the explained risks, some were chosen for extra discussion by the interviewee. The main aspects and questions to be discussed were:

- *Why the assets targeted in the attack are important?*
- *What problems will rise when the asset is under attack?*
- *What are the possible countermeasures?*

The findings were then put into the OCTAVE sheets (Appendix V) used for the risks assessment as an additional information on the same risks. Comparing those two will be the basis for the validation. The different findings will be discussed in the later sections.

## 5.2 Findings from the Interviews

The findings will be presented by discussing all the risks one by one or grouped as similar entities. The grouping of the risks is done if they, for example, share the same assets that are affected. In those cases, not the exact risk was discussed, but overall importance of the assets. The risks not talked about in the interviews are skipped.

**Risk 1, 2 and 3 – attacks on the ultrasonic sensors**. Those three risks are all about the ultrasonic sensors present in the car. In the Bolt prototype, the sensors are present but not yet used in the context of the project. This was also confirmed in the first interview with Expert1. They also mentioned that the sensors could be used for automated parking and other similar situations in the future.

**Risk 4 and 5 – attacks on radar.** Risk 4 and 5 describe jamming and spoofing attack on the radar. Generally, radars are known to be used for obstacle detection in the AV's. In the interview with Expert1, they said that the radar is installed in the car, but not actively used for autonomous driving. Some experiments have been done with them, and it is planned to

be used more for obstacle detection in the future. Because of this, the value for radar data went from *High* to *Low*.

**Risk 6 and 7 – attacks on the cameras.** Risk 6 and 7 focus on the attacks on the cameras. In both of the interviews, the value of image and video data got confirmed to be *High*. The data is used as an input for image recognition algorithms to detect traffic sign, lights and pedestrians. Different attack methods were also found as discussed in the first interview with expert1. For example, even mirrors could be used to carry out a blinding attack. In addition, blinding of the cameras could happen by accident when windows or mirrors reflect sunlight into the cameras lens. Because of the value added by the cameras and the high likelihood and ease of the attack happening, countermeasures to deal with it is even more valuable. A possible new countermeasure discussed in the interviews was to turn off auto exposure settings, which may shorten the time when the attack has impact on the image. Auto exposure is the main reason that the camera would be "blind" after the attack, not just during it. Further experiments need to be done with the exposure, as just turning it off will require to manually adjust the settings before every use, or even during the use depending on the weather and outside environment. Even small changes in the weather or environment could cause problems without any auto exposure options as the camera would not be able to automatically adjust the exposure and with that, the incoming light levels. Overall, the high value of the cameras and their data in the project was confirmed.

**Risk 8 and 9 – attacks on the LiDAR**. In both of the interviews the importance of LiDAR was discussed. In the interview with Expert1 from the University of Tartu, LiDAR was mentioned to be the main obstacle detection tool in the car. A new way of spoofing the LiDAR was also mentioned - creating smoke clouds. Expert1 mentioned that during some of the test driving, smoke coming from the cars was detected as an obstacle. Because of the ease of creating smoke compared to using different, more complicated tools like oscilloscope used in the experiments in the literature, the likelihood of spoofing LiDAR happening had to be increased. A possible new countermeasure for spoofing attack was mentioned, improvements in the algorithms to help avoid spoofing using smoke. In the second interview with Bolt experts, similar reasoning for the importance in the LiDAR was presented. The question risen in there was if relay attack on LiDAR could actually be used to control the car. Further investigating is required to confirm that. Countermeasure gotten from the second interview is to use multiple sensors to duplicate the data and confirm the validity by comparing the inputs, which was also mentioned in the literature.

**Risk 10 – Code modification**. The risk was discussed in both of the interviews. In the first one, the focus went from the OBD-II scanner to different options to carry out the attack. A way found was to use the access to repository to modify the code and later it will be downloaded into the system. In that case, physical access to the ports is not required. The attack could be carried out by an insider, who is getting paid to do it or does it to get personal satisfaction of harming the company. In the second interview the question of how much access would using the OBD scanner give and how much code could be modified. The countermeasures discussed were adding unit tests to regularly check the validity of the code. Also blocking any kind of unauthorised access will help to mitigate this risk.

**Risk 13 – Packet fuzzing**. The risk was brought up by Expert1 because of the importance of having valid communication between the different components. Any kind of tampering with the packages could cause fatal errors in the system. The likelihood of an attack gaining access to the communication was said to be low. Some discussed countermeasures were implementing secure connection, encryption and splitting the communication into smaller networks. The last one would help to limit the access to the attacker could have after getting

into one of the smaller networks. The cost of implementing those varies from *Low* to *High* as support for encryption in the components is uncertain. Encrypting all connection using other tools like raspberry pi (said by Expert1) may harm the decision making speed, which is crucial in autonomous driving.

**Risk 16 – GPS jamming.** GPS jamming was discussed in both interviews. In the first with Expert1, a new way of attacking the GPS was discussed. The GPS used in the Bolt vehicle actually requires corrections from the map server, in real-time. The corrections are used to reduce the error from the GPS from a few metres to a few centimetres. Disabling the correction service would mean a few metre errors in the traffic, where those could mean accidents and harm to pedestrians. To counter GPS jamming and the new correction disabling attacks, a new way of localization was discussed. That could be done using LiDAR. Having a previous LiDAR scanned area known and comparing that to the new data gotten while driving makes it possible to localize with a very small error. LiDAR localization is not working at the time writing this, but there are plans to implement it in the future.

**Risk 17 – EMP attacks.** This risk was discussed in the second meeting with Bolt experts. The main focus was where and how much impact the attack could have in the Bolt vehicle. In conclusion, the likelihood of an EMP attack was said to be very low, as the tools required to disable the car are not available. Accepting the risk as an action to be made was chosen as how low the likelihood is.

**Risk 19, 20 and 21 – Attacks on the map storage.** The main focus was on risk 19, manipulating the map data. In both of the interviews it was brought up. In the first interview, the real importance of the map data was discussed. Currently, all the traffic lights, signs and lanes were manually added to the maps and then imported into the storage. All of the parts are required for safe driving and losing access to valid map data will cause problems. Manipulating the map data could allow the attacker to control the car and make it go where they want it to go. Detecting deletion of the maps will be easy, but detecting small changes will be harder. Even those small changes could lead to accidents in the traffic. Some countermeasures proposed were adding unit tests and simulating the driving before using the maps in the real traffic. Also duplicating the maps to compare for errors was mentioned.

## 5.3 Threats to Validity

The main threat to validity is the subjective opinion of the experts. The experts were chosen for their knowledge in the project, but their opinions on the topic could be subjective and because of that, the validation process could have been harmed. As the prototype in the case study is still in early development phase, the opinions on the topic could change by time. New priorities and viewpoints on the topics discussed could arise and change the overall feedback.

The validation was done in an interview style way. In the end, it shaped up to be more of an open discussion with some guiding questions by the interviewer. The threat to validity in that is the completeness of the questions. *Did the questions cover all the required topics? Were the right questions asked? Were the questions enough to do the validation?*

The feedback from the experts was supportive for the approach taken. As no other approach was discussed, the real motivation of trying other methods was not present. Because of this, the experts simply accepted the current approach and ignored any other, and possibly better, way of doing the security risk management.

Table 7. Main changes from validation.

| Risk | Previous statement | Validation statement | Comments |
|---|---|---|---|
| R1; R2; R3 | Sensors not used | Sensors not used | Ultrasonic sensors got confirmed to not be required for the current version of the car. |
| R4; R5 | Sensors required | Sensors not actively used | Radars are currently not required for the autonomous driving, plans to implement them in the future. |
| R6; R7 | R7 medium likelihood | R7 high likelihood | A new way of carrying out the blinding attack was discussed: using mirrors to reflect sunlight. This made the likelihood of R7 High. Turning off auto exposure could be used as countermeasure |
| R8, R9 | R9 medium likelihood | R9 high likelihood | During the interviews, a new way of spoofing the LiDAR with smoke was discussed, which increases the likelihood of it happening. Possible countermeasure of improving the obstacle detection algorithms. |
| R10 | Attack with only OBD-II scanner | Attack using code repository | In the interview a way of changing the code through the code repository was discovered. New countermeasures include unit tests and manual checks. |
| R13 | Low value of countermeasures | High value of countermeasures | The value of the asset was confirmed to be High. Possible countermeasure of encryption was said to be high. New countermeasures include implementing secure connection and splitting the network. |
| R16 | Jamming only the GPS | Jamming also the connection to the correction network | During the interview fetching the corrections for GPS localization was discovered. Using that as an attack vector is possible. New countermeasures found were duplicating the GPS data and using LiDAR for localization. |
| R17 | Mitigate the risk | Accept the risk | In the interview, the probability of the attack happening was said to be so low that instead of mitigating, it could be accepted. |
| R19 | Map is required to know where the roads are | Map is required to know where the roads, signs, lights and lanes are. | The importance of the map data was discussed and how it provides where all the signs, lights and lanes are on the roads. The mapping is done manually. Countermeasures include duplicating the data and testing the maps in simulations. |

## 5.4 Lessons Learnt

The main changes done after the validation can be seen in Table 7. The table consists of the risk number, previous and validation statement and comments for what the changes were. The changes can be seen in the Appendix V, where the previously filled OCTAVE sheet are updated. It is important to note that not all the risks are present in the Appendix V. Only the risks with large changes are there. Risks that were not discussed are skipped. The overall feedback on the risk management done for literature and the case study was good. Even when some of the risks were not present in the car currently, they could be in the future (i.e. attacks on the radar). In both of the interviews, it was mention that the current analysis is a good way to continue on and add into in the future. From Bolt side the concern was of how difficult the current method of using OCTAVE sheets to present risks could get overwhelming when even more risks would be added. To make it easier, a smaller table to give overview of all the risks and their scores could be presented like it was done in Table 5.

## 5.5 Summary

In this chapter the process of the validation is discussed. To do the validation, two interviews were done, both with experts in their field. The findings from the interviews is discussed and some threats to validity presented. In the next chapter, the thesis will be concluded.

# 6 Summary of Work

The final chapter of the thesis presents the summary of the work done with limitations of the research, answers to the research questions, conclusions and future work.

## 6.1 Limitations

The scope for the research done in this thesis was on the architecture of the autonomous vehicles. Because of that, the processes present in the car were not discussed and the security risk management for them was not done. Also, the generic security risks present in normal street legal cars were out of scope. The focus was on the risks affecting the assets defined to be used in autonomous vehicle. It is also important to mention that the all the assets, risks and countermeasures were found from the literature. During the literature review, some relevant papers could have been not found and because of that, the list is not complete. Other possible assets, risks and countermeasures could be found from the literature leading to the current security risk management being incomplete. Continuous iteration of the same method is required, to gather new risks and vulnerabilities and choosing action based on those.

The security risk management for this thesis was done using a combination of SRM and OCTAVE allegro. Any other similar methods for autonomous driving research field was not found during the literature review. There could be other methods to do the security risk management process for autonomous driving. Also, the workflow and sheets provided by the OCTAVE allegro were modified to better suit the needs in this work.

The measuring and risk scoring in the risk management process was subjective. Even when defining the measurement criteria and using guidelines provided in OCTAVE, the subjectiveness could not be completely disposed of.

## 6.2 Answers to Research Questions

In this section, the answers to the research questions will be given.

**RQ1. What are the protected assets in autonomous vehicles?**

In an autonomous vehicle the protected assets are the components used in the process of autonomous driving. This includes both system and business assets. The assets were divided into three layers based on their characteristics: *precision, network* and *application layer*. System assets in autonomous driving context were defined as the sensors, different communication devices, computing units etc. Business assets consist of the data exchanged between the components, the software and processes used in the AV. Full details and illustrative models on the assets can be seen in Chapter 3.3. The defining and presenting of the assets follow the guidelines provided by SRM (Chapter 2.4).

**RQ2. What are security risks and its impact in autonomous vehicles?**

The security risks were selected from the literature. In this thesis, 23 different security risks were defined and analysed. The risks selected have immediate effect on the autonomous driving application, general security risks on modern cars were ignored.

The impact of those risks was found in the Bolt case study. The metrics used to evaluate the risks were:

- Impact on confidentiality;
- Impact on availability;
- Impact on integrity;

- Value of the affected business asset;
- Likelihood of the attack happening.

Using a combination of those metrics, the *Total Risk Score* for each risk was calculated. The risk definitions can be found in Chapter 3.4 and the impacts with corresponding the risk scores are in Chapter 4.3.

**RQ3. What are security countermeasures in autonomous vehicles?**

All the found risks need to be dealt with. For that, countermeasures for all the risks were found from the literature. The countermeasures are defined in Chapter 3.5 and 3.6, more description and some estimations on implementing them in the case study can be found in Chapter 4.4. Every risk also has a section for countermeasures in the OCTAVE sheet which can be found in Appendix IV.

## 6.3 Conclusion

Autonomous vehicles have many security risks and having a clear method to present them is crucial. In this work some well-known methods were discussed. From those, SRM was chosen to define assets and risks, with OCTAVE Allegro to evaluate the risk scores and measure their impact.

All the risks, assets and countermeasures are based on the findings from the literature. The combination of SRM and OCTAVE Allegro is used to present them in a meaningful way. The same security risk management process is then carried out in a case study. The case study used here is a mutual research agreement between University of Tartu and Bolt to develop a road legal autonomous driving vehicle, which could be used as a taxi service for Bolt customers. With the case study, the findings from the literature could be analysed in a real life implementation. The impact for each risk from the literature can be defined and measured in the case study context.

The validation of the security risk management process for autonomous vehicles is done by interviewing multiple experts in the field. During the validation, the new method of using SRM and Octave Allegro was approved and some suggestions to further improve the process was presented.

Security risk management is an iterative activity. There is no endpoint in finding risks as new vulnerabilities are continually being discovered. Having the support to analyse security risks iteratively is vital for any security risk management method. In this thesis, only one iteration of the proposed method is done: discovering the vulnerabilities, assessing the security risks and defining countermeasures. Although continuous management of risk illustrated by more than one iteration of the proposed method is out of the scope, it is possible. The defined countermeasures implemented within the first iteration would become assets in the system. These assets with their vulnerabilities need additional security analysis, and as such, new risks can be discovered. Security risks from the second iteration will require further mitigating actions, forming a loop that continues until the system is discontinued and does not need more support. Only then, can security risk management can come to an end for the system.

## 6.4 Future Work

During the research in this thesis, some proposals for future works were defined. The proposals could further improve the research done in this thesis and open up new research opportunities to be discovered.

The way of using SRM for security risk management with combination of using OCTAVE Allegro to measure the impact is new. Further research on this topic is possible. The outcome of the research could provide a new standard for security risk management.

As the scope was on architecture in this thesis, adding support for process present in autonomous vehicles in security risk management can be done. The risks found in the processes and dealing with them will improve the overall security in the system.

In this thesis, one iteration of the security risk management was done. With each additional iteration new risks, vulnerabilities and countermeasures can be defined. Continuing the process will greatly improve the overall security in the system.

# 7 References


[1] C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles: Contactless Attacks Against Sensors of Self-Driving Vehicle.," *DEFCON,* no. 24, 2016.

[2] C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello, "A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis," *Applied Sciences,* vol. 9, no. 23, p. 5101, 2019.

[3] V. L. Thing and J. Wu, "Autonomous Vehicle Security: A taxonomy of Attacks and Defences.," *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* pp. 164-170, 2016.

[4] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 16, no. 2, pp. 546-556, 2014.

[5] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and Lidar.," *Black Hat Europe,* no. 11, 2015.

[6] S. J. F. Caralli R. A., Young L. R., Wilson W. R, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst., 2007.

[7] R. Matulevičius, *Fundamentals of Secure System Modelling*. Cham: Springer, 2017.

[8] É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management," in *Intentional Perspectives on Information Systems Engineering.* Berlin: Springer, 2010, pp. 289-306.

[9] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019: IEEE, pp. 1-6.

[10] D. Firesmith, "Engineering Safety and Security Related Requirements for Software Intensive Systems," in *29th International Conference on Software Engineering*, 2007, p. 169.

[11] *ISO/IEC 27001:2013 - Information Technology – Security Techniques – Information Security Management Systems – Requirements*, International Organization for Standardization, Geneva, 2013.

[12] *ISO/IEC 27005:2018 - Information technology - Security techniques - Information Security Risk Management*, International Organization for Standardization, Geneva, 2018.

[13] *ISO/IEC 13335-1:2004 - Information technology - Security Techniques - Management of Information and Communications Technology Security - Part 1: Concepts and Models for Information and Communications Technology Security Management*, International Organization for Standardization, Geneva, 2004.

[14] Common Criteria. "Common Criteria for Information Technology Security Evaluation, CC v3.1." https://www.commoncriteriaportal.org/cc/ (accessed 09.05, 2020).

[15] National Institute of Standards and Technology. "SP 800-30 Rev. 1: Guide for Conducting Risk Assessments." https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed 09.05, 2020).

[16] J. Freud and J. Jones, *Measuring and Managing Information Risk: a FAIR approach*. Butterworth-Heinemann, 2014.

[17] G. Wangen, C. Hallstensen, and E. Snekkenes, "A Framework for Estimating Information Security Risk Assessment Method Completeness," *International Journal of Information Security,* vol. 17.6, pp. 681-699, 2018.

[18] J. Sengupta, S. Ruj, and S. D. Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications,* p. 102481, 2019.

[19] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of Threats? A Survey of Practical Security Vulnerabilities In Real IoT Devices.," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8182-8201, 2019.

[20] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8169-8181, 2019.

[21] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of Vehicular Ad-hoc Networks: A Comprehensive Survey," *Computers & Security,* p. 101664, 2019.

[22] S. Sharma and B. Kaushik, "A Survey on Internet of Vehicles: Applications, Security Issues & Solutions," *Vehicular Communications,* vol. 20, p. 100182, 2019.

[23] M. S. Sheikh, J. Liang, and W. Wang, "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors,* vol. 19, no. 16, p. 3589, 2019.

[24] X. Wang *et al.*, "Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 2, pp. 1314-1345, 2018.

[25] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and Autonomous Vehicles: A Cyber-Risk Classification Framework," *Transportation Research Part A: Policy and Practice,* vol. 124, pp. 523-536, 2019.

[26] D. Iberraken, L. Adouane, and D. Denis, "Reliable Risk Management for Autonomous Vehicles Based on Sequential Bayesian Decision Networks and Dynamic Inter-Vehicular Assessment," 2019 2019: IEEE, pp. 2344-2351.

[27] J.-Y. Lee, B.-J. Kim, and K.-S. Yi, "Integrated Risk Management for Automated Driving," 2014: IEEE, pp. 1452-1457.

[28] National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," *Report No. DOT HS,* vol. 812, p. 333, 2016.

[29] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles," *Ad Hoc Networks,* vol. 90, p. 101823, 2019.

[30] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk Assessment for Cooperative Automated Driving," 2016, pp. 47-58.

[31] K.-B. Sung, K.-W. Min, J.-W. Kim, and J.-D. Choi, "Autonomous Vehicle Guidance System with Infrastructure," 2013: IEEE, pp. 1-6.

[32] A. A. O. Affia, R. Matulevičius, and A. Nolte, "Security Risk Management in Cooperative.," in *On the Move to Meaningful Internet Systems: OTM 2019 Conferences.* Cham: Springer, 2019, pp. 282-300.

[33] Y.-D. Kim, G.-J. Son, C.-H. Song, and H.-K. Kim, "On the Deployment and Noise Filtering of Vehicular Radar Application for Detection Enhancement in Roads and Tunnels," *Sensors,* vol. 18, no. 3, p. 837, 2018.

[34] T. Haggerty, R. H. Visintainer, and P. Mascarenas, "Automated Driving Solution Gateway," ed: Google Patents, 2018.

[35] D. T.-Z. Lu, C. K. Johnson, and R.-R. Hubert, "Unlock and Authentication for Autonomous Vehicles," ed: Google Patents, 2015.

[36] B. Daniel. "The Best Hosted Endpoint Protection and Security Software for 2020." https://www.pcmag.com/picks/the-best-hosted-endpoint-protection-and-security-software (accessed 09.05, 2020).

[37] Novatel. "Enclosures PwrPak7." https://www.novatel.com/products/gnss-receivers/enclosures/pwrpak7/ (accessed 09.05, 2020).

[38] AutonomousStuff. "Lexus RX 450h." https://autonomoustuff.com/product/lexus-rx-450h/ (accessed 09.05, 2020).

[39] Velodyne. "VLP-32C User Manual." https://velodynelidar.com/products/ultra-puck/ (accessed 09.05, 2020).

[40] AlliedVision. "Mako G G-319." https://www.alliedvision.com/en/products/cameras/detail/Mako%20G/G-319/ (accessed 09.05, 2020).

[41] Sekonix. "Sekonix SF332X-10X " http://sekolab.com/products/camera/ (accessed 09.05, 2020).

[42] AutonomousStuff. "Delphi Electronically Scanning RADAR." https://autonomoustuff.com/product/delphi-esr-2-5-24v/ (accessed 09.05, 2020).

[43] Novatel. "SPAN IMU-IGM-S1." https://www.novatel.com/products/span-gnss-inertial-systems/span-imus/span-mems-imus/imu-igm-s1/ (accessed 09.05, 2020).

[44] Neousys. "Nuvo-6108GC Series User Manual." https://www.neousys-tech.com/en/product/application/edge-ai-gpu-computing/nuvo-6108gc-gpu-computing (accessed 09.05, 2020).

[45] AutonomousStuff. "PACMod 3.0." https://autonomoustuff.com/product/pacmod/ (accessed 09.05, 2020).

[46] MikroTik. "wAP ac LTE6 Kit Router User Manual." https://help.mikrotik.com/docs/display/UM/wAP+ac+kit-series (accessed 09.05, 2020).

# Appendix

## I. Detailed Risk Definitions

| | R1 - Jamming ultrasound sensors | R2 - Spoofing ultrasound sensors | R3 - Acoustic quieting | R4 - Jamming radar | R5 - Spoofing radar | R6 - Blinding attack on cameras |
|---|---|---|---|---|---|---|
| **Business asset** | ultrasonic sensors data | ultrasonic sensors data | ultrasonic sensors data | surrounding environment data, radar data | surrounding environment data, radar data | video and image data |
| **Security criteria** | integrity of measurement data | integrity of measurement data | integrity of measurement data | integrity of surrounding environment data | integrity of surrounding environment data | integrity of video and image data |
| **System asset** | ultrasonic ranging sensors | ultrasonic ranging sensors | ultrasonic ranging sensors | radars | radars | cameras |
| **Vulnerability** | Ultrasonic sensors are not jamming resistant. | Ultrasonic sensors are not spoofing resistant. | Ultrasonic sensors are not acoustic quieting resistant. | Radars are not jamming resistant. | Radars are not spoofing resistant. | Cameras are vulnerable to blinding attacks. |
| **Attack method** | An attacker uses their ultrasonic frequency emitter to emit frequencies used by the sensors to carry out a jamming attack. | An attacker uses their ultrasonic frequency emitter to emit frequencies used by the sensors to carry out a spoofing attack. | An attacker can cover objects with sound absorbing materials to make them hard to detect using ultrasound sensors. | An attacker uses their signal generator to emit frequencies used by the radar to carry out a jamming attack. | An attacker uses their signal generator to emit and manipulate the frequencies used by the radar to carry out a spoofing attack. | An attacker can disturb the cameras with malicious optical outputs to blind the cameras. |
| **Threat agent** | An attacker with some previous experience with ultrasound sensors. Has a DIY ultrasonic jammer. | An attacker with some previous experience with ultrasound sensors. Has a DIY ultrasonic emitter. | An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use. | An attacker with some previous experience with radars and has signal generator (+multiplier etc.). | An attacker with some previous experience with radars and has signal generator (+multiplier etc.). | An attacker with some previous experience and tools to send malicious optical inputs (laser etc.). |
| **Threat** | An attacker uses their knowledge and tools to carry out a jamming attack on ultrasonic ranging sensors by emitting frequencies used by the sensors and causing false information received by the sensor (40kHz in this). | An attacker uses their knowledge and tools to carry out a spoofing attack on ultrasonic ranging sensors by emitting carefully crafted frequencies and sequences causing false information received by the sensor. | An attacker uses their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes late detections . | An attacker uses their knowledge and tools to carry out a jamming attack on radar by emitting frequencies used by the sensors and causing false information (distance constantly changing) received (76-77GHz in the experiment). | An attacker uses their knowledge and tools to carry out a spoofing attack on radar by emitting frequencies used by the sensors and causing false information (no objects detected) received (76-77GHz in the experiment). | An attacker uses their knowledge and malicious optical emitters to send and blind cameras causing unwanted blindness on the cameras and possibly permanently damage the camera sensors. |
| **Impact** | Loss of integrity of Ultrasonic sensors measurement data. | Loss of integrity of Ultrasonic sensors measurement data. | Loss of integrity of Ultrasonic sensors measurement data. | Loss of integrity of surrounding environment data. | Loss of integrity of surrounding environment data. | Loss of integrity of video and image data. |
| **Risk** | An attacker uses ultrasonic frequency emitter to manipulate the data received by the sensors causing false blackout by the sensors and loss of integrity of measurement data. | An attacker uses ultrasonic frequency emitter with crafted pulse to manipulate the data received by the sensors causing false information received by the sensors and loss of integrity of measurement data. | An attacker uses sound absorbing materials to cover some objects to make them hard to detect by the sensors causing late detection (possible collisions) and loss of integrity of measurement data. | An attacker uses their tools to manipulate the data received by the radar causing false blackout on the radar and loss of integrity of surrounding environment data. | An attacker uses their tools to manipulate the data received by the radar causing constant changes in distance/velocity on the radar and loss of integrity of surrounding environment data. | An attacker uses their tools to send malicious optical data to the camera causing unwanted blindness, possible hardware damage and loss of integrity of video and image data. |

# I. Detailed risk definitions *(Continued)*

| | R7 - Confusing controls with attack on cameras | R8 - Relay attack on LIDAR | R9 - Spoofing LIDAR | R10 - Code modification | R11 - Code injection | R12 - Packet sniffing |
|---|---|---|---|---|---|---|
| **Business asset** | video and image data | surrounding environment data | surrounding environment data | system software | system software | communication data |
| **Security criteria** | integrity of video and image data | integrity of surrounding environment data | integrity of surrounding environment data | integrity of system software | integrity of system software | confidentiality of communication data |
| **System asset** | cameras | LIDAR | LIDAR | ECU, computing unit | ECU, computing unit | network |
| **Vulnerability** | Cameras are vulnerable to blinding attacks. | LIDAR's are not relay attack resistant. | LIDAR's are not spoofing resistant. | System software can be modified, no validation. | Harmful code can be injected into system software, no validation | Communication can be intercepted. |
| **Attack method** | An attacker can disturb the cameras with short malicious optical outputs and large contrasts to blind the cameras for short period of time after the attack ended. | An attacker can setup tools to confuse and disturb the work of LIDAR causing false information in the LIDAR data. | An attacker can use their tools to create false objects in the environment for the LIDAR. | An attacker uses their OBD-II scanner to compromise the system. | An attacker uses their OBD-II scanner to inject code into the system. | AN attacker can install a packet sniffer to intercept communication. |
| **Threat agent** | An attacker with some previous experience and tools to send malicious optical inputs (laser etc.), tools to further destabilize the input. | An attacker with some previous experience and tools to send light with specific (905nm) wavelengths, oscilloscope. | An attacker with some previous experience and tools to send light with specific (905nm) wavelengths, oscilloscope. | An attacker with some previous experience with car diagnostics and coding can use OBD-II scanner to modify the system code. | An attacker with some previous experience with car diagnostics and coding can use OBD-II scanner to inject harmful code into the system. | An attacker with a packet sniffer and some previous experience. |
| **Threat** | An attacker uses their knowledge and malicious optical emitters to send a short output and blind cameras causing unwanted blindness and confusion for longer period on the cameras and possibly permanently damage the camera sensors. | An attacker uses their knowledge and tools to carry out a relay attack confusing and manipulating the data received by the LIDAR causing unwanted errors. | An attacker uses their knowledge and tools to create objects for LIDAR in the environment, that are not there. | An attacker uses their knowledge and tools to modify code in the system causing unwanted changes and potential harm. | An attacker uses their knowledge and tools to inject code in the system causing unwanted changes and potential harm. | An attacker uses packet sniffer to intercept and collect data from communications in the system. |
| **Impact** | Loss of integrity of video and image data. | Loss of integrity of surrounding environment data. | Loss of integrity of surrounding environment data. | Loss of integrity of system software. | Loss of integrity of system software. | Loss of confidentiality of communication data. |
| **Risk** | An attacker uses their tools to send malicious optical short output and blind cameras causing unwanted blindness and confusion for longer period, possible hardware damage and loss of integrity of video and image data. | An attacker uses their tools to send a light wave and manipulating the information got by the LIDAR to carry out the relay attack causing confusion, errors and loss of integrity of surrounding environment data. | An attacker uses their knowledge and tools to create objects for LIDAR in the environment, that are not there and causing loss of integrity of surrounding environment data. | An attacker uses OBD-II scanner to modify the system code causing unwanted changes and potential harm with loss of integrity of system software. | An attacker uses OBD-II scanner to inject code the system code causing unwanted changes and potential harm with loss of integrity of system software. | An attacker uses packet sniffer to intercept and collect data from communications in the system causing loss of confidentiality in the communication data. |

# I. Detailed risk definitions *(Continued)*

| | R13 - Packet fuzzing | R14 - Eavesdropping CAN | R15 - Inject CAN messages | R16 - GPS jamming | R17 - EMP attack | R18 - Inject malware |
|---|---|---|---|---|---|---|
| **Business asset** | communication data | communication data | communication data | location data | autonomous driving | autonomous driving |
| **Security criteria** | integrity of communication data | confidentiality of communication data | integrity of communication data | integrity of location data | availability of autonomous driving | integrity of autonomous driving |
| **System asset** | network | controller area network | controller area network | GPS | sensors, computing unit, actuation unit, ECU | computing unit, network, ports |
| **Vulnerability** | System can't handle invalid data inputs. | CAN bus can be listened to by outsiders. | No authentication for CAN messages. | GPS in not jamming resistant. | Electronic components in AV can be affected with EMP. | Malware can be injected using physical ports or network. |
| **Attack method** | An attacker can send invalid data to the system and trigger error and fault clauses. | An attacker uses their tools and motivation to listen to CAN bus. | An attacker uses their tools to inject CAN messages. | An attacker can use their tools to send modified signals to jam the GPS. | An attacker uses EMP generator to shut down components in the AV. | An attacker uses physical ports or network to inject malware into the system. |
| **Threat agent** | An attacker with some experience working with data packages. | An attacker with tools and motivation to listen to CAN bus messages. | An attacker with tools to inject CAN messages. | An attacker with tools to send GPS signals. | An attacker with EMP generator. | An attacker with access to ports or network to inject malware. |
| **Threat** | An attacker uses their experience to send invalid data to the system causing unwanted errors and potentially exposing security loopholes. | An attacker uses their tools and motivation to listen to CAN bus gaining access to communication data. | An attacker uses their tools to inject CAN messages causing disturbances in the system and possible accidents. | An attacker can use their tools to send modified signals to jam the GPS, making the vehicle localization not possible. | An attacker uses EMP generator to shut down components in the AV, making autonomous driving impossible. | An attacker uses physical ports or network to inject malware into the system, causing errors, loss of data, accidents. |
| **Impact** | Loss of integrity of the communication data. | Loss of confidentiality of communication data. | Loss of integrity of communication data. | Loss of integrity of location data. | Loss of availability of autonomous driving. | Loss of integrity of autonomous driving. |
| **Risk** | An attacker sends invalid data to the system causing unwanted errors and potentially exposing loopholes in the security causing loss of integrity in the communication data. | An attacker uses their tools and motivation to listen to CAN bus, gaining access to communication data and causing the loss of confidentiality of communication data. | An attacker uses their tools to inject CAN messages causing disturbances in the system and possible accidents and causing the loss of integrity of communication data. | An attacker can use their tools to send modified signals to jam the GPS, making the vehicle localization not possible and causing the loss of integrity of location data. | An attacker uses EMP generator to shut down components in the AV, making autonomous driving impossible and causing the loss of availability of autonomous driving. | An attacker uses physical ports or network to inject malware into the system, causing errors, loss of data, accidents and loss of integrity of autonomous driving. |

# I. Detailed risk definitions *(Continued)*

| | R19 - Manipulate map data | R20 - Extract map data | R21 - Delete map data | R22 - Disable actuation module | R23 - Induce bad analysis |
|---|---|---|---|---|---|
| **Business asset** | map data | map data | map data | autonomous driving | decision maker, driving planner |
| **Security criteria** | integrity of map data | confidentiality of map data | availability of map data | availability of autonomous driving | integrity of decision maker and driving planner |
| **System asset** | internal storage | internal storage | internal storage | actuation module | computing unit |
| **Vulnerability** | Storage and map data are not authenticated. | Storage and map data are not authenticated. | Storage and map data are not authenticated. | Actuation module is not theft proof. | Software in computing unit is not protected. |
| **Attack method** | An attacker uses their access to the maps to manipulate them. | An attacker uses their access to the maps to extract them. | An attacker uses their access to the maps to delete them. | An attacker uses malware to disable actuation module. | An attacker uses their knowledge to create fake output of the software. |
| **Threat agent** | An attacker with access to the storage and maps. | An attacker with access to the storage and maps. | An attacker with access to the storage and maps. | An attacker who can install malware on the actuation module. | An attacker with knowledge on the used software. |
| **Threat** | An attacker uses their access to the maps to manipulate them, resulting in traffic disturbances and accidents. | An attacker uses their access to the maps to extract them, causing information leak. | An attacker uses their access to the maps to delete them, resulting in traffic disturbances and accidents. | An attacker installs malware on the actuation module, which can disable the functions of it. | An attacker uses their knowledge to create fake output of the software causing the car to follow attackers orders. |
| **Impact** | Loss of integrity of map data. | Loss of confidentiality of map data. | Loss of availability of map data. | Loss of availability of autonomous driving. | Loss of integrity of decision maker and driving planner. |
| **Risk** | An attacker uses their access to the maps to manipulate them, resulting in traffic disturbances and accidents and loss of integrity of map data. | An attacker uses their access to the maps to manipulate them, resulting in information leak and loss of confidentiality of map data. | An attacker uses their access to the maps to delete them, resulting in traffic disturbances and accidents and loss of availability of map data. | An attacker installs malware on the actuation module, which can disable the functions of it causing loss of availability of autonomous driving. | An attacker uses their knowledge to create fake output of the software causing the car to follow attackers orders and causing loss of integrity of decision maker and driving planner. |

## II. Empty OCTAVE Worksheet

| **Allegro – Worksheet 10** | | **Asset risk worksheet** | | | | | |
|---|---|---|---|---|---|---|---|
| **Threat** | **Business Asset** | | | | | | |
| | **Business Asset's Value** | | | | | | |
| | **Area of Concern** | | | | | | |
| | **Actor**<br>*Who would exploit the area of concern or threat?* | | | | | | |
| | **Means**<br>*How would the actor do it? What would they do?* | | | | | | |
| | **Motive**<br>*What is the actor's reason for doing it?* | | | | | | |
| | **Outcome** (choose one)<br>*What would be the resulting effect be?* | Disclosure: | | Destruction: | | | |
| | | Modification: | | Interruption: | | | |
| | **Security Requirements**<br>*How would the information asset's security requirements be breached?* | | | | | | |
| | **Likelihood** (choose one) | High: | | Medium: | | Low: | |

| **Consequences**<br>*What are the consequences to the organization as a result of the risk?* | **Severity**<br>*How severe are the consequences to the organization or asset owner by impact area?*<br>**3 for highest priority, 2 for medium and 1 for lowest* | | | |
|---|---|---|---|---|
| | Impact area | Priority* | Impact | Score |
| | Confidentiality | | | |
| | Availability | | | |
| | Integrity | | | |
| | **Relative risk score:** | | | |
| | **Total Risk Score** *(Rel x likelihood):* | | | |

| **Risk Mitigation** | **RiskID - Name** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Choose action to take.** | Accept: | | Defer: | | Mitigate: | | Transfer: | |
| For the risk, what actions and controls will be used: | | | | | | | | |
| **Layer where applied** | **Description of control or action** | | | | | **Estimated cost** | | |
| | | | | | | | | |

## III. Criteria Used in the OCTAVE Worksheets

| **Risk Measurement Criteria** | | | |
|---|---|---|---|
| **Impact area** | **Low** | **Medium** | **High** |
| Confidentiality | Confidentiality is not affected | Confidentiality is affected, but only on low priority data | High priority and classified data is breached |
| Availability | Component has minimal downtime and does not affect overall performance | Component cannot be used a small amount of time and can cause some performance problems | Component cannot be used for a long period of time and affects the whole system |
| Integrity | Components' and data's' integrity is not affected | Components' or data's' integrity is affected, but overall performance is not | Integrity is lost and affected sensors and data will cause problems in the performance of the system |

**Business Asset's Value**

The value of an asset is estimated based on the value it provides to the system. The main aspect taken into consideration is what will happen to the system when the data is lost or modified. All data is considered confidential and should not be available to public.

The business asset's value is:

- **Low** – System can continue working without the asset
- **Medium** – System can continue working, but with some performance issues
- **High** – System cannot continue working without the data

**Likelihood**

Chance of the attack happening is **Low** when:

- The tools required are very specific and their cost is high;
- The knowledge required to carry out the attack is high;
- Attack window is small and preparation time is high.

Chance of the attack happening is **Medium** when:

- The tools don't cost a lot but need some small tinkering to work;
- The attack can be carried out by a moderately experienced attacker;
- Attack window and preparation time is medium.

Chance of the attack happening is **High** when:

- No tools required or are easily obtainable;
- Very small amount of knowledge is required, can be done by a rookie;
- Attack window and preparation time is small.

## IV. Filled OCTAVE Worksheets

The filled OCTAVE worksheets can be found in the additional appendix file included with the thesis.

## V. Validated OCTAVE Worksheets

The validated OCTAVE worksheets can be found in the additional appendix file included with the thesis.

## License

**Non-exclusive licence to reproduce thesis and make thesis public**

I, **Rando Tõnisson**,

(*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,

   **Security Risk Management in Autonomous Driving Vehicles: Architecture Perspective**,
   (*title of thesis*)

   supervised by Raimundas Matulevičius and Abasi-Amefon O. Affia
   (*supervisors' names*)

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.

Rando Tõnisson

***15/05/2020***