DEGREE PROJECT

Information security risk review and analysis for the future autonomous vehicle

- Using GBM-OA to compare literature review findings with the Arrowhead framework

Felicia Persson

Information Security, master's level (120 credits)
2017

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

Abstract

The future autonomous vehicle (AV) is a field where great amounts of research are being made, but while there are many studies on various parts of the vehicle, there are not any recent overviews looking at information security. The aim for the thesis is to give an overview of the security needs we face with the future AVs because of the information exchange these cyber-physical systems will require to function. A literature review based upon recent studies is presented by themes found and summarized in a table for a clear view. Additionally, the found knowledge gap is presented from the literature review to show where future research is needed to complement the present. The Arrowhead Framework's security chapters are used as examples of security for cyber-physical systems (such as the AV), and discussed and compared to the findings of the literature review to show differences and highlight room for improvement. This thesis contains an introduction to the future AV, and the GBM-OA method as its concepts are used to identify information security concerns found in the literature review as well as in the framework.

Keywords: Autonomous vehicle, information security, theme-based literature review, Arrowhead Framework, GBM-OA, risk overview

Table of Contents

Table of Figures

Table of Tables

Abbreviations

AAA – Authentication, Authorization and Accounting

AV – Autonomous Vehicle

CAN – Controller Area Network

CIA (triad) – Confidentiality, Integrity and Availability

CPS – Cyber-physical system

ECU – Electronic Control Unit

GBM – Genre Based Method

HTTP – Hypertext Transfer Protocol

IoT – Internet of Things

IS – Information Systems

V2V – Vehicle to vehicle

V2X – Vehicle to everything

VANET – Vehicular ad hoc network

1 Introduction

With the fourth industrial revolution on its way, cyber-physical systems (CPSs), i.e. systems that interact with their surrounding environment in ways we have yet to experience today, will become more and more prevalent in the society in general. CPSs will come in many different shapes and forms: in industrial environments, taking on and streamlining many tasks performed by humans today; in healthcare, taking care of the many physically tolling tasks today's nurse's and other personnel handle today; all in all, automating many jobs in an intelligent and human interactive manner.

On a more technical level, these systems will take in data through sensors combined with receiving other data through the IoT (Internet of Things) constantly connected devices and systems that will provide the systems with external data. Making predictions from the large amounts of data that will be gathered, coupled with the way these systems will interact based upon these predictions with their physical environment, is what makes us call these systems cyber-physical. IoT plays its part into these systems as well by the connectivity we are looking at today and which will only increase with time.

Expectations are that the number of devices that are connected – transferring and receiving data globally – will soon grow faster than they ever have before (Lasi, Fettke, Kemper, Feld & Hoffman, 2014; Vogel-Heuser & Hess, 2016; Lee, Ardakani, Yang & Bagheri, 2015). One huge leap forward for CPSs will be automated vehicles, not only public transportation vehicles but also private ones such as cars. The research and development of autonomous vehicles are taking big steps forward every day (De-J, Santos & Tudon-Martinez, 2017). Most of us have heard of self-driving cars and other smart technology of the future. We are already seeing these types of vehicles being tested on the streets of the United States, but they are not ready yet for the market (Mascareñas, Stull, & Farrar, 2017). Autonomous vehicles will change the entire market of vehicles and how we use transportation, of course depending on the degree of autonomy. There will most likely be a transitioning period, for how long is uncertain, and depending on the local and governmental laws there may be differences across the world in how these vehicles are implemented.

The benefits are many when it comes to the future's vehicles, no longer will we have to depend upon strangers' ability to react quickly, or that everyone on the road is sober and not distracted or tired – the vehicle will solve those problems. There will also be a huge reduction in costs, considering less crashes will cost the society less, and environmental effects will come as well. More fuel-efficient cars that based upon certain variables and sensors can lower their fuel usage is something that the future will bring us as well. People who cannot drive on their own will be able to have more reliable transportation and decide when to go out for rides in them, and when traveling people will be able to aim their attention towards whatever hobby or work they want.

Of course, this is speculation still since the autonomous vehicles are still in testing and prototype phases and laws regarding ownership and usage have not been fully formed. For now, there are many question marks regarding the autonomous vehicles, one of them being the security. The privacy of travellers is uncertain and the ways malicious entities could undermine the systems

and communication used by them are many (Fagnant & Kockelman, 2015; Schneider, Kohn, Klimke & Dannebaum, 2017).

1.1 Background (pre-literature review)

Below follows a summarized explanation and comparison of the autonomous vehicle today – undergoing heavy development – and the future AV according to current research. The AV in its form today is explained in the first part and the latter handle the future AV as scientists predict. By looking at what the AV looks like today we can get an understanding of where the future predictions partly come from. This sub-chapter functions as a further introduction and a background.

1.1.1 The autonomous vehicle today

Autonomous vehicles do exist today, albeit not fully in the way that the future autonomous vehicle may operate. When looking at AVs vs non-AVs, there are many levels of autonomy to consider. We already have cars today that have sensors and other types of technology on board to help the driver. The functions can range from help with parking such as cameras and sensors on the back of the car to more advanced solutions. They are usually referred to as vehicles with smart functions, but for this report, they will be referred to as semi-autonomous. Both semi- and fully autonomous vehicles have been and are being developed by several companies worldwide. Semi-autonomous vehicles are vehicles that by one or several functions use sensors and combines data to achieve intelligent driving aids. Examples of this are sensors detecting signs along the road as well as speeds of other vehicles on the road. These functions are then both used to warn the driver of dangers or simply that the speed has changed, but they can also function to slow down the vehicle or stop it completely if a danger is detected that the driver has yet to notice (Bangar, Pacharne, Kabade & RajaraPollu, 2016).

Other functions that make a vehicle semi-autonomous vary between speed holders – which have been around for a longer time – to different settings that affect the vehicle's performance and ways of driving. For example, settings can vary between "sports" and "economic", making the driver able to pick between which setting they prefer depending on their way of driving and what their daily traveling looks like – in this example the former would utilize functions to make the vehicle quick and performance oriented while the latter would enhance cheaper and more environment friendly driving (Bangar et al., 2016). In addition, functions for weather detection to ensure that the driver is aware of the risks that could occur driving for longer distances such as slippery roads depending on weather changes are not uncommon. Using eye detection to support the safety is another function in some semi-autonomous vehicles, and is used to detect a sleepy driver or someone who is not in the best position to drive safely. Since human senses cannot compare, these functions come in many new vehicles being produced today to enhance the safety for drivers and their passengers, although they are still expensive. Fully autonomous vehicles have yet to be released to the public and are still in various stages of being tested and developed.

In several countries, producers have tested the vehicles on larger roads and highways, using the tests to further develop the vehicles. The data they gather from these tests, such as how the

vehicles can interact with the rest of the traffic and how long they can drive without any problems arising is analysed and used to continue improving the technology.

1.1.2 The future autonomous vehicle

While it seems that the fully autonomous vehicle is very close, there are a lot of aspects that have yet to be explored, a big one being legalities and liabilities. It is important to establish laws and regulations for who will be responsible in case of accidents and other events including these vehicles. Normally, the driver would be the one in charge, but if the driver has no control, or very little, it is no longer as simple.

The idea for the subject came together from a previous course, along with many articles touching, but sometimes also diving into the subject of autonomous vehicles. The reasoning behind why this is an important subject is that there is a huge amount of research going on within this field, but there are many different approaches to autonomous vehicles. Many articles are about the systems and suggestions for algorithms and various in-depth methods for these autonomous vehicles to gather data and made predictions. Other articles are about specific types of security threats, or various obstacles that need to be overcome such as how to gather, store and make the most use out of Big Data. It is clearly a very current and new field of research which means that a contribution in the form of analysing the autonomous vehicle's overall risks can help give direction to further research. No other research such as this has been found in the smaller literature review made for this proposal, indicating that this thesis could fill a research gap.

Research already made about autonomous vehicle security solutions all have a wide variety of suggestions, ranging from architectural suggestions (Zaidi & Rajarajan, 2015) to specific security measures. Some mean that current protocols used in the semi-autonomous vehicles (vehicles with smart functions), are too vulnerable to be used in a fully autonomous vehicle and that it is therefore important to come up with a completely new security architecture (Dakroub, Shaout & Awajan, 2016). Not only the architecture is mentioned as being too poor today, the systems need to be more intelligent and have a higher level of trustworthiness per one researcher (Neumann, 2016). In his study, he concludes that because no system is ever perfect, it should be up to the consumer to decide whether they want to rely on autonomous vehicles for transportation – or perhaps if partly autonomous vehicles is the best way to go and is what will dominate the market when it comes to the future vehicles. The critique is sound and shows there are a great deal of aspects to consider, especially when it comes to human interaction with these cyber-physical systems.

Wooderson and Ward (2017), who in their study argue the importance of testing and validation when it comes to cybersecurity in vehicles, and especially cybersecurity in the future vehicles with their complex systems underline that although there is no international standard yet when it comes to cybersecurity for vehicles. Further, they bring up the various risks facing connected vehicles, in form of deliberate or accidental abuse, that need to be prepared for as far as possible and necessary since there is no fully guaranteed security in the world that could fulfill every risk. The arguments are not grasped from thin air - the future of autonomous vehicles is being created today, which is why most researchers are providing predictions, suggestions and discussions.

Ilvonen, Jussila, Kärkkäinen and Päivärinta (2015) emphasize the need for being proactive when it comes to (knowledge) security risk management. In their paper, they discuss the importance of trying to maintain a multifaceted assessment because failing to address a risk can and may result in confidential information being shared or accessed. They bring up the example of social media and how many have neglected to include the risks of people communicating their knowledge and only focused on the upsides to sharing information. By performing a holistic analysis, we can achieve a more nuanced presentation of risks and give ideas for how research can be continued.

To summarize, the concept of the study is that the future of autonomous vehicles faces many obstacles when it comes to maintaining high security – to continue research already made in the field, this study aims to conceptualize the many different security risks that emerge from applying GBM concepts to the autonomous vehicle. This study will in form of a literature review give an overview of previous research, which then will be summarized and applied to an existing, and new, framework for CPSs. By studying research on the AV and its risks, we can draw conclusions that in many ways can be applied to AVs in general, despite differences in technology and structure of the vehicles there should be risks they all have in common. This thesis will assist in providing an overview – which has been explicitly sought for, and additionally applying that knowledge and the found gap onto an existing framework.

1.2 Knowledge gap

The identified knowledge gap of the pre-literature review is that an overview of the information security risks of the future AV using GBM-OA concepts does not exist. There is both an expressed need for this, but also an identified need from performing a literature review to find articles on this matter. A large majority of articles handle specific risks that are linked to certain software or hardware that is predicted to be used in AVs. To cover this knowledge gap, research questions have been formed that, when answered, should meet the sought for information need.

Additional findings will too be presented in the results chapter, i.e. the literature review chapter.

1.3 Research questions

The questions that have emerged from the pre-literature review are the following ones:

1. What are the information security risks of the autonomous vehicle expressed in current research?

2. What are the research gaps, where can future research on information security risks of the autonomous vehicle be focused?

3. How can the findings of the literature review be applied to a real case framework's security? What can be learned?

Because of identifying a knowledge gap that researchers expressed a need to cover, one of the questions, number 1, directly relates to this. The second and third questions were chosen to be answered in the literature review, to further respond to the identified knowledge gap as well as apply findings of the review to a cyber-physical system-framework's security. By answering these questions, the current state of risks for the future AV can be presented, as well as future needs.

1.4 Expected contribution and limitations of the study

This study will contribute with an overview of previous research in the subject of AV and its information security risks. By summarizing research, predictions in this paper pursue to give indications to future researchers where studies should be performed. By searching for and presenting previous research in a theme based manner and applying GBM concepts, the overview can be used as a map for further research to fill gaps. While literature reviews as studies are limited regarding new findings since they rely solely upon previous research, they can contribute with a summary of what has happened up until now. Gathering information in this manner can save the next researcher time when it comes to mapping the previous research.

Regarding further risks and limitations with this study. There is a risk that the overview presented in this report does not represent all risks that exist, and that the portion of articles read and used for the study in its size is not enough to deem the outcome final in that there could be no other outcome. However, an argument against that is the impossibility to include hundreds of studies or even more – there is a great amount of work being done, articles are added continuously and for a literature review on master thesis level to cover everything is not possible. Risks presented along with other findings in the literature review will be based upon the references presented in the end of the study, if the studies used have failed to identify certain risks that I do not notice or know about, then those risks will be left out.

With literature reviews, it is not just about the literature chosen, but also about interpretations and how the literature combined is used. With the literature review method being open ended, since not just a single concept is searched for, the result will reflect what the studies contain – by theme. The work is ambitious in that it tries to create an overview of existing research, but even a portion of research can create a picture of what has been studied, and what needs more studying. By including the predictions and suggestions, as well as future research proposals of the authors of the studies, this literature review does not only reflect my identified knowledge gaps.

To ensure that these limitations and risks are being minimized and avoided, I have used several databases provided by LTU as well as Google Scholar, and have not limited research to a single country, or continent, and have included more technical articles as well as articles about predictions. This is to get a varied overview that does not focus on singular parts of the future AVs information security, but instead the holistic perspective. Furthermore, a literature review can only reflect its sources, and has a purpose of doing so – of course with the author's decisions of what to include and not. Many articles were not included because of them only having information security as an afterthought or a small including in the discussion.

2 Autonomous vehicle technical overview and information security concepts

In this chapter, a description of the autonomous vehicle will be presented to explain concepts that will reappear in the literature review. The connectivity and technologies of the vehicle will be explained. Furthermore, information security concepts will be presented to later, as well, reappear in the literature review. Introducing these will assist in understanding the technologies and risks being brought up in the later chapters.

2.1 Connectivity and communication

The connectivity of the AV will be vital to its existence and for it to properly perform its functions, this applies to the entire AV but also for information security involved (Zheng, Zheng, Yang, Zhao, Hou, Chatzimisios, 2015). The communications need to be reliable and contain a large quantity of data for the cyber-physical system that is the AV. Zheng et al. (2015) propose, in their study, a vehicular network to be used instead of currently existing ones to tackle the need for this. Theirs is one of many suggested developmental solutions to ensure the future AV's communications capabilities. Amongst several suggestions, they bring up how data can be intermittently broadcasted and transferred to keep it efficient and congestion-free.

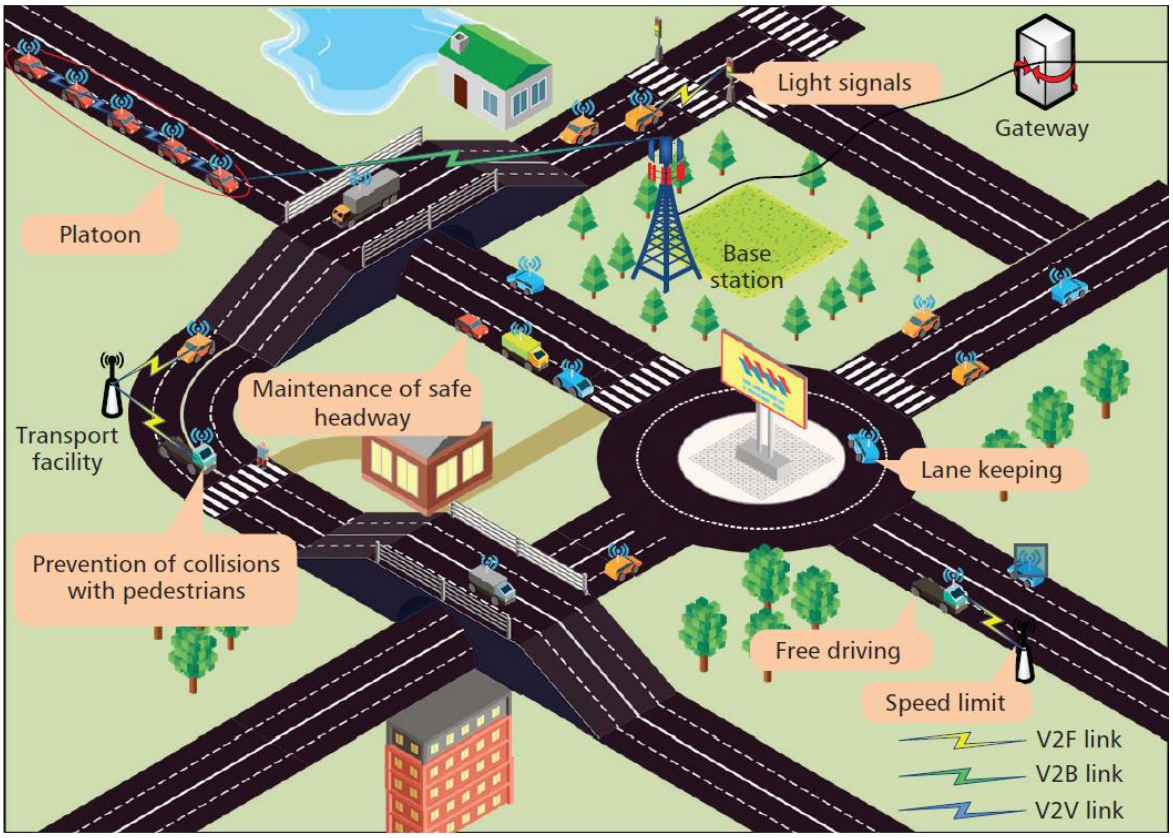

Figure 1. (Zheng et al. 2015)

They are far from the only scientists to come with suggestions for how the communications are going to be handled in the best way, but their study adds to the many expressing the importance of unhindered communications that can convey the information needed for the AVs to operate. In the above figure, the communications presented in their study are illustrated. The different links all represent different types of communications they propose AVs should use. The figure is a good example of a vision of how AVs will be connected on varying levels.

2.1.1 IoT

To explain what connectivity means in the context of the AV, we can begin with IoT. Internet of Things is the concept most devices today being connected on a global level, through the Internet. Using various ways of connecting to the Internet, whether it be WiFi, 3G, 4G etc. these devices rely on information sharing and communication to perform its functions. A big part of the communication is people talking to people via various social medias, or by using texting applications, but the communication also consists of devices communicating with servers for software updates of various applications. With the different functions most people use, the devices are connected 24/7. With research going toward all things technological being connected – such as for example the coffee maker or the electric scale – more and more devices are being added making this network and its communicated data extreme in its size.

2.1.2 Clouds

Now, all connections do not have to mean a connection to the Internet. Your scale may just be connected via Bluetooth to your phone application to store your most recent weight and then if you have a profile you want to carry with you through various devices for exercise tracking purposes, the information is stored on a remote server belonging to the website you use. An alternative to a remote server is having a local server storing data, or a local/private cloud (Prowse, 2015) – it may also continuously transfer this data to a remote server for longer storage.

Below is a figure showing what the cloud services can look like for the future AV (Zaidi & Rajarajan, 2015) – it can be viewed in multiple layer, each cloud storing specific data. Weather data is something that all vehicles on the grid can share across vehicles and across communications, but vehicle specific data that may contain highly sensitive information if shared boundlessly, can be stored in the private cloud.

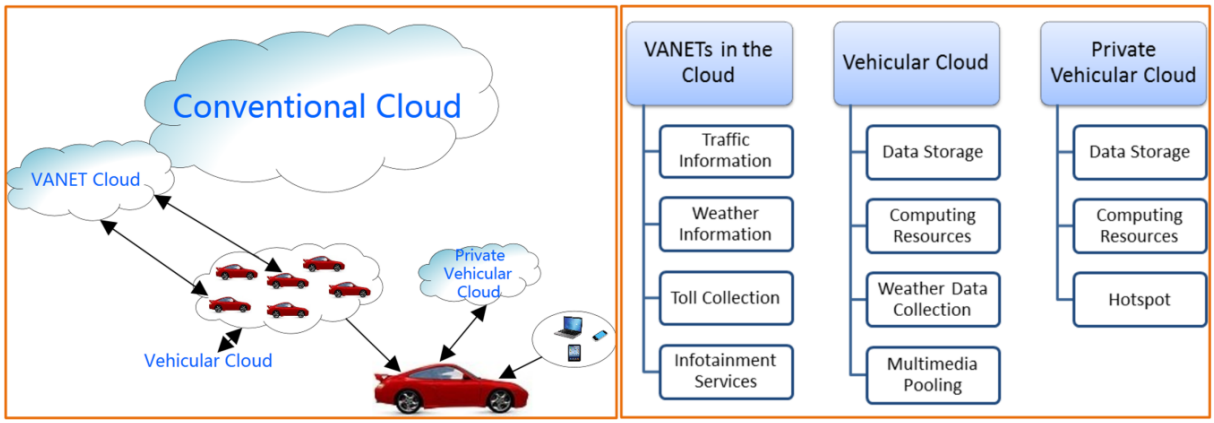

Figure 2. "VANETs and cloud (left), cloud applications (right)" (Zaidi & Rajarajan, 2015).

The main point with this is that not only will AVs require the types of security standards applicated to devices connected to the Internet today, and especially so since an attack can mean serious injury for people inside and outside the vehicle, but there are several other communications going on from the AV.

2.1.3 Communication

As for the AV, communication and being connected refers to the constant communication with the other vehicles on the road, the grid and, authorities and other third parties (Bagloee, Tavana, Asadi & Oliver, 2016). These different types of communications are going to be responsible for the AVs ability to know about the upcoming conditions of the road and the traffic in general. They also allow for the third parties decided upon, for example insurance companies, to be able to access data surrounding an incident. The safety and security will be heavily reliant on the communication of the vehicles altogether on the roads and the ability for their combined detection of immediate threats in their surroundings – such as for example a pedestrian trying to cross the road. It can be argued that everything that is being communicated is at risk when it comes to the autonomous vehicle. Information communicated inside the vehicle or outside, can all be compromised. While this study handles security mainly, safety can be mentioned because of its need for communication - but also because of the direct relation between the need for communication for safety implementations to function.

In the AV, various solutions will result in either the vehicle storing large amounts of data locally for longer or shorter time periods. The data stored will come from various sensors and information systems along with the hardware of the vehicle. All data gathered will make up large amounts, which in turn will be used but first stored.

2.1.4 CAN

The Controller Area Network, or the CAN bus, is a network used in many vehicles today as it was standardized. It has been around a long time, and handles the internal communications between electronic control units (Natale, 2012). The CAN protocol has features such as being able to detect errors in the communication, or transmission, between ECUs. It also contains guaranteed maximum latencies and other such features made for a functional network for controlling a vehicle – although CAN has also been applied to other systems. It is message-based

and has been widely used by car manufacturers to allow for implementing features into the vehicle with the development of them. By allowing the ECUs to communicate, we can get automated features, such as the airbags 'knowing' that someone is seated by the input from the seat-belt. This is merely an example of one of the functions the ECUs, through communication, carry out constantly throughout the usage of a vehicle. Like any other network, CAN has issues, specifically typology, timing and message ones, making the CAN bus vulnerable to an overflow of communication at times for example (Natale, 2012).

The vulnerabilities and capabilities of CAN has lead scientists in present time (Hopper et al., 2011; Zou et al., 2017) express the need for a new network for the internal communications of vehicles, especially so when it comes to AVs. One of the main reasons to this is that CAN was not created for communications reaching outside the vehicle, i.e. to the Internet and vehicle-to-vehicle amongst other types, and information security implementations are therefore complicated. Therefore, information security concerns like DoS attacks are a big argument against the CAN for AVs. CAN and information security concerns will be brought up later and further developed in this study.

2.2 Technologies

The AV will host a variety of information systems and hardware, but the most important ones to consider here, and without going into too much detail, sensors and ECUs are the ones that will be prone to attacks and therefore in need for security measures. They will each be presented below with their own chapter describing their functionalities as an introduction before the literature review. By considering how these parts work, and what they communicate with, the understanding for their role in planning high information security for the future AV is important when explaining the AV in its entirety.

2.2.1 Sensors

Sensors will provide data of various environmental aspects surrounding the vehicle as well as input from within the vehicle. Combinedly, this data is used for predictions of the vehicle and helps the system perform its functions. Much like the ECU, in the next chapter, it is a critical point of information exchange inside the AV as sensors provide useful information to the control system of the vehicle. The data input from sensors can be used for all types of calculations and prediction type systems.

One type of sensor is a radar or a camera, which can be used for parking help for the driver in vehicles today, showing any type of object that might be in the way, or even a human that could be in immediate danger should the driver move its vehicle in that direction. Sensors for temperature and weather conditions outside can help the steering of the vehicle and ensuring that the speed can be kept at a safe number (Natale, 2012). The various types of functions that can be carried out with the input from a sensor are endless. For the future AV, the sensors will provide the control system with information that a human could not compute in the same amount of time, which is a big reason to why self-driving vehicles can be safer.

Sensor data is prioritized depending on what has been decided in the CAN bus. Critical data will be prioritized while other sensor data might take longer to arrive. It is important that the sensor data that is important reaches its recipient in time for the control system to operate in full function (Natale, 2012).

2.2.2 ECU

Electronic control unit, or nodes as they are also called, used throughout the autonomous vehicle for various purposes when it comes to controlling the vehicle in general (Natale, 2012). These units are manipulated to perform their function for the vehicle to accelerate, slow down, stop, steer etc. Therefore, these units are used for airbags, audio, and doors for example. Each electronic control unit corresponds to something within the vehicle that needs to be controlled, to put it simple. As mentioned in the previous subchapter for CAN, ECUs communicate through CAN. For this study, all possible ECUs will not be listed for the AV, but it is important to note that there can be a large amount of them in a single vehicle.

The importance of keeping the ECUs secure from tampering with is very high, both from physical access and remote access. To further explain the ECU's role – actuators are what the ECU controls. In the future AV, an actuator plays the same role as an actuator in any type of vehicle – it performs an action, such as steering. They are controlled by the ECUs and carry out functions that they are designed to do. Actuators, just like ECUs, play a critical role to the vehicle being able to perform its functions and they come in a large amount for just a single vehicle. Actuators in themselves do not communicate with each other or other parts of the CPS, they are more an extension of the ECU.

Edwards, J., and Kashani, A. (2017) discuss ECUs in an automotive context in their study, underlining the importance of quality when it comes to this type of ECU. This is because of how the smallest issues with them can be very critical - the ECUs in an AV must perform their functions continuously with no downtime. The ECU, while having been basic in their build have because of newer technologies become more complex with time. This has caused more security concerns – more features, more criticality to the overall system. As each ECU is added to the internal network of the AV, each ECU has its own need for security, as does the network.

2.3 Information security risks

First, we must define risks to information security of the autonomous vehicle. To use already established frameworks used in information security, the CIA triad (Prowse, 2015) and AAA framework will be used to explain what we usually consider to be the most important goals to holding information secure. CIA stands for Confidentiality, Integrity and Availability. That something is confidential means that it is access-limited, has integrity means that it is accurate and is available means that it is accessible by those who should have access to it. AAA stands for Authentication, Authorization and Accounting (Decugis, 2009). Authentication means that those who should have access can be identified in their role, authorization is the next step and stands for the ability to give access to the authenticated entity, and accounting is when activity is logged and analysed to ensure security to put it simple. From these frameworks, threats are usually categorized in to what they represent a security risk within.

It is important to note that safety and security are differentiated in this study. Vehicle safety handles safety concerns for risks that do not include information security: such as crashes not dependent on communication but rather a malfunction of a sensor for example. While there is a fine line, safety in that regard has not been brought up or sought out in the literature review since it does not correspond with information security.

2.4 Information and data in relation to the autonomous vehicle and its communications

Information and data in relation to the future autonomous vehicle and its communication is the concept that they are all connected. The information and data in focus in this study is that being communicated within, to and from the vehicle. The nature of this information will vary, from personal information about the driver or the different users of the vehicle and their saved information to information regarding the various software and hardware and their statuses to information that is critical to the performance and safety of the vehicle. This means that information that both needs to have high confidentiality, integrity and availability will be communicated, stored and used by the vehicle.

Information that contains history of the vehicle's travels and communication between the vehicle and the grid or other vehicles could become subject to not only eavesdropping but also unauthorized alteration pose serious threats to the information security level of autonomous vehicles.

The AV relies on data from sensors to be communicated to the ECUs and controlling systems. The information of the vehicle, everything that is gathered, used and stored, is communicated in some way, either to another storage, or to third parties and governmental agencies. To understand the AV, one must understand its relationship with information and communication. Securing the information and the communications is key to ensuring high information security for the AV and its users.

3 Method

This chapter contains the used methodologies for the literature search and review, while the literature review method has been fully applied – concepts have been used from the GBM as it firstly is a risk assessment methodology. However, by applying methods, or concepts of them, to subjects outside their meant application, we can gain a new perspective.

After the methods have been described, the chapter also contains the planning and work progress, including a time schedule, of the study.

3.1 GBM (Genre-based method)

By considering people as knowledge assets, GBM gives more opportunities for identifying potential risks on a broader level (Päivärinta, Halttunen, & Tyrväinen, 2000).

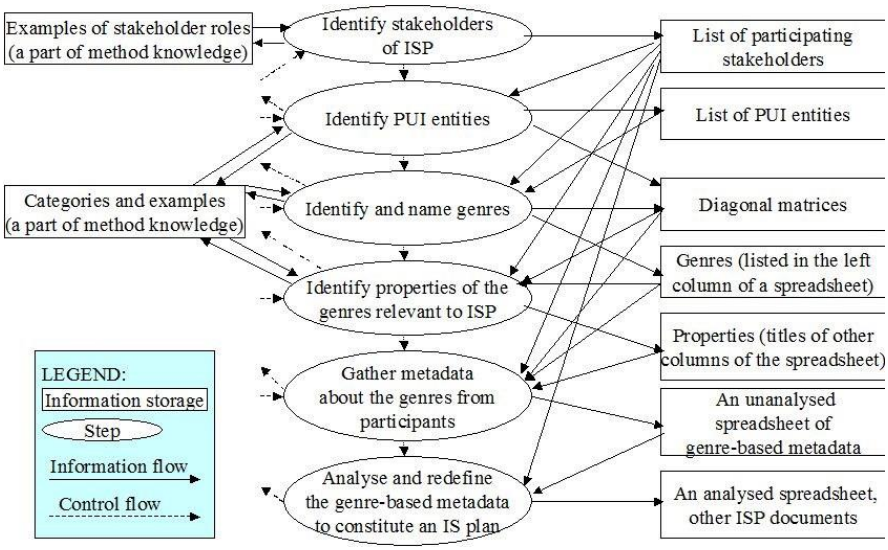

Figure 3. (Päivärinta, Halttunen & Tyrväinen, 2000).

The Genre-based method, shown in the above image, is a method that focuses on identifying knowledge or information within an organization by identifying the genres. Genres could be explained as the holders of certain types of assets – information assets. The GBM emphasizes people as entities that holds and uses knowledge in an organization. This means that only 'securing' physical and electronic type assets, could lead to a risk assessment falling short. Suggested for usage with another method called OCTAVE Allegro, this method applies another perspective when looking at risks of the information security kind.

Genres hold information that is being communicated through various channels, whichever technology or protocol being used. The information being communicated in the autonomous vehicles can be viewed in genres that are specific for this subject. A genre, or a communication flow, could for example be the data sent from a sensor on the vehicle to a server. In the vehicle however, there would be several genres that could look like this, and therefore when grouping them up into containers, they can be considered as one item instead of each sensor being assessed as they essentially will perform the same kinds of functions.

While this study does not contain any risk assessment, certain concepts of this method – such as humans being considered for risks, and grouping assets together when looking at communication to deem where risks can be found, I have tried to apply to the literature review.

3.2 OCTAVE Allegro

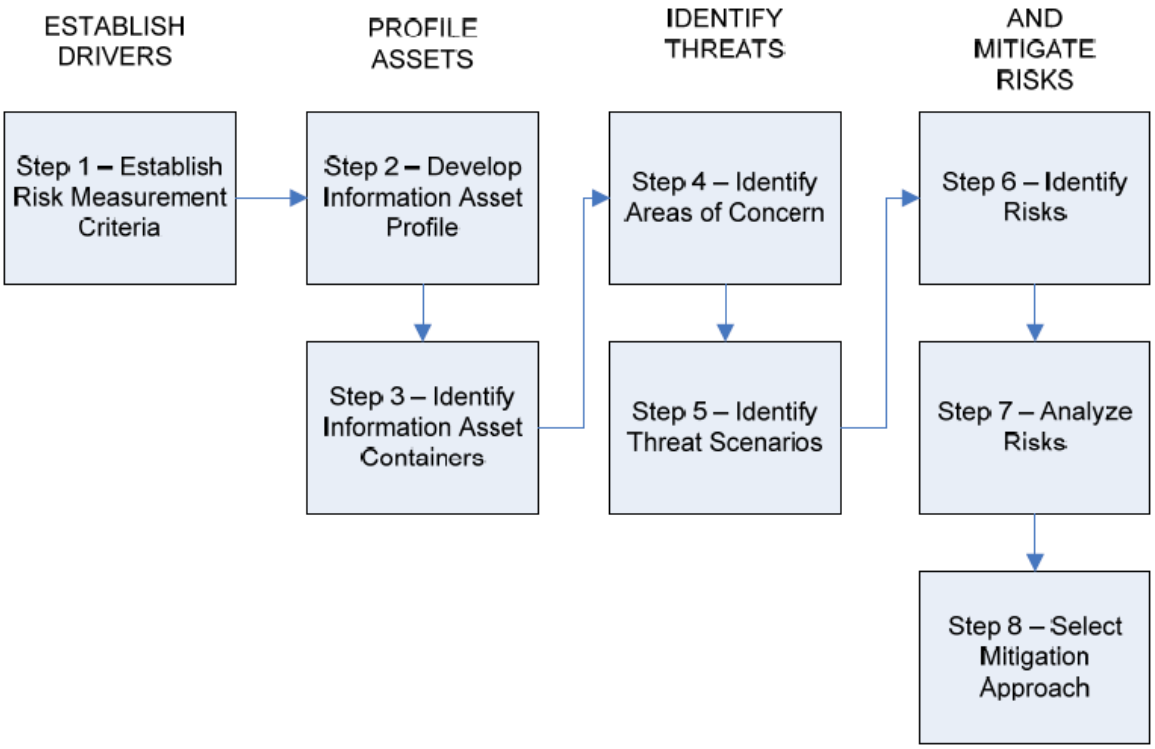

Image 1: OCTAVE Allegro Roadmap (Caralli, Stevens, Young & Wilson, 2007)

The above figure, outlines the eight steps of the method and what each of them represent. When using the OCTAVE Allegro method, the first step is to establish the criteria for risk, meaning what do we mean by risk in this case and what type of impact would certain types of risks result in. Depending on what is being assessed, certain risks score lower or higher on a scale of what is required for the unit that is being assessed to operate and function correctly. Certain impact areas will be more critical than others when it comes to the autonomous vehicle.

Next, the assets must be described in detail by going through all information assets than come into play in the vehicle, this step is where the literature review will provide valuable information. The development of this step is to identify containers that hold these assets, some containers will hold many assets and others only a few. The containers are identified looking at where the assets are stored and used. This requires extensive work because in this step it is important to as accurately as possible to identify containers to not miss out on possible security requirements (Caralli, Stevens, Young & Wilson, 2007).

Worksheets for the steps presented above have been created for OCTAVE Allegro, and these are used to standardize tasks such as impact area prioritization, to make sure that the method is being used as intended – and to produce outcomes of consistent quality (Caralli, Stevens, Young & Wilson, 2007).

Next is identify the threats, which is done in two steps. First, areas of concern are identified and described. Brainstorming is a good first approach to finding the areas in which threats to the security may lie. These are unique to each case, completely dependent on what is being assessed. This step does not dive as deep into details as the previous, because the next step will delve further into possible scenarios in which threats can exist. By listing most of the different types of threats and dividing them into categories, each type of threat can be gone through and described.

In step six, the previous step comes into practice as risks are to be identified. This is when the threats previously presented are gone through respectively by possible impacts. Here, realizations like 'A disruption of X can result in a negative impact of Y and Z' are conceptualized to fully capture what risk scenarios can lead to. Further steps include analysing risks and selecting mitigation approaches for these risks. To analyse the captured risks, is to decide the importance of prioritizing certain risks above others to have a functioning security for the information assets. After this step, mitigations are developed for the risks that require security measures. These mitigations respond to the risk score of information assets and their requirements to maintain a high level of security. Furthermore, the whole environment of the assets is considered when suggesting mitigations, in this case meaning that the whole vehicle and how and where it will operate should be considered (Caralli, Stevens, Young & Wilson, 2007).

3.3 GBM-OA

When merging the Genre-Based Method with Octave Allegro (GBM-OA), the methods become intertwined. What GBM is lacking can be found in OA, and the other way around, which is why these methods together can enrichen security analysis.

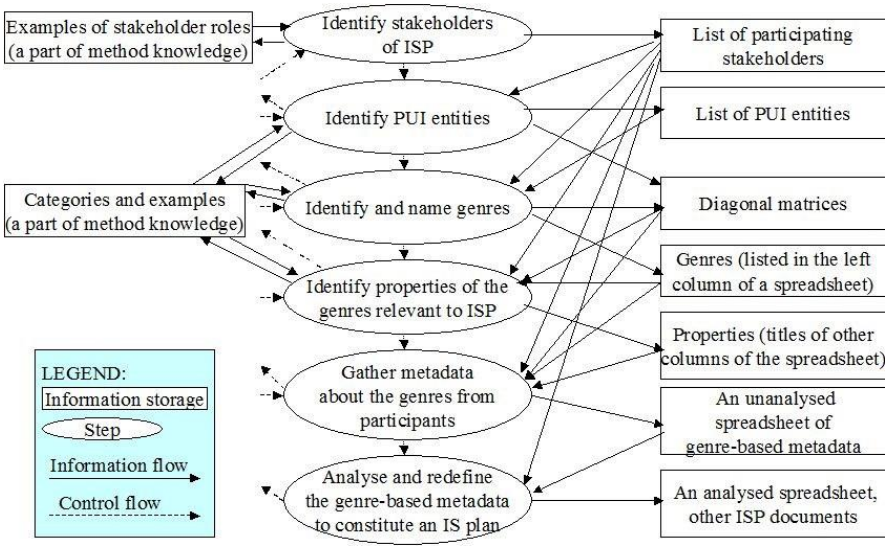

Image 2: Päivärinta, T., Halttunen, V., & Tyrväinen, P. (2000).

The Genre-based method, shown in the above image, is a method that focuses on identifying knowledge or information within an organization by identifying the genres. Genres could be explained as the holders of certain types of assets – information assets. These genres share PUI entities (producers and users), which are identified in the step after stakeholders. By using this

method on top of OCTAVE Allegro, a more detailed information asset mapping can be completed.

Genres hold information that is being communicated through various channels, whichever technology or protocol being used. The information being communicated in the autonomous vehicles can be viewed in genres that are specific for this subject. A genre, or a communication flow, could for example be the data sent from a sensor on the vehicle to a server. In the vehicle however, there would be several genres that could look like this, and therefore when we group them up into containers, they can be assessed as one item instead of each sensor being assessed as they essentially will perform the same kinds of functions.

In this study, concepts of the GBM-OA will be used – specifically the genre and asset list along with the containers. Identifying these, will give information regarding what the literature, and what Arrowhead Framework, have focused on. The differences, if any, can shed light on what has been researched and what may be missing from both the review and the framework. By applying these concepts, a discussion regarding differences will be easier to show in overview.

3.4 Data gathering and literature review method

As for the article search for the literature review, peer-reviewed articles and technical papers have been used. The chosen articles have been used because of their focus on information security risks and concerns for the future autonomous vehicle on various parts of the future AV, its connectivity and communications. They were found by searching the LTU database and SAE Mobilus (technical papers through access by LTU library) for the following terms: "Information security autonomous vehicle", "Autonomous vehicle risk" and "Autonomous vehicle communication". Google Scholar database was in several cases used to find articles when I reviewed the references used in articles chosen from the former two databases – some articles could not be found in them. In the LTU article database, the searches were defined to only show hits on peer-reviewed academic articles, and peer-reviewed conference materials, that were published in the last 5 years, 2012-2017, (all of 2017 had not passed at the start of the thesis so including 2012 was included). the articles presented were chosen for being the newest and most relevant articles on the subject. English was chosen as the language of the articles and the abstract was viewed for a larger number of articles before those relevant were picked out from the rest.

Below, the number of articles found, viewed/read, chosen and disregarded will be shown for each search term. The subjects chosen in the LTU search will be listed below each table. The reason behind choosing subjects in the search that are predefined by the database is to be able to precise how the articles were found, as well as ensure that the search result contains as many relevant articles as possible.

"Information security autonomous vehicle"				
Database	***Found (in search)***	***Viewed/read***	***Chosen***	***Disregarded***
LTU	97	~50	5	92
SAE Mobilus	62	~25	5	57

Table 1. Search term "Information security autonomous vehicle"

In the LTU database, this search was defined to the following subjects: *vehicles, roads, security, vehicular ad hoc networks, automotive electronics, robotic and control systems, intelligent vehicles, automotive engineering, communication, networking, mobile communication and component, circuits and devices.*

In the SAE Mobilus database, the sector chosen for the articles was *automotive*, and the topic chosen was *autonomous vehicles*.

"Autonomous vehicle risk"				
Database	***Found (in search)***	***Viewed/read***	***Chosen***	***Disregarded***
LTU	82	~ 30	8	74
SAE Mobilus	62	~ 25	3	59

Table 2. Search term "Autonomous vehicle risk"

In the LTU database, the topics chosen were: *autonomous vehicles, remotely piloted vehicles, fully autonomous automobiles, cyber-physical systems, vehicles and risk.*

In the SAE Mobilus database, the sector chosen for the articles was *automotive*, and the topic chosen was *autonomous vehicles*.

"Autonomous vehicle communication"				
Database	***Found (in search)***	***Viewed/read***	***Chosen***	***Disregarded***
LTU	128	~ 50	7	121
SAE Mobilus	62	~ 25	3	59

Table 3. Search term "Autonomous vehicle communication"

In the LTU database, the topics chosen were: *autonomous vehicles, communication networking and broadcast technologies, intelligent vehicles and fully autonomous vehicles.*

In the SAE Mobilus database, the sector chosen for the articles was *automotive*, and the topic chosen was *autonomous vehicles.*

Summary search terms, articles				
Database	Found (in search)	Viewed/read	Chosen	Disregarded
LTU	307	130	20	287
SAE Mobilus	62	~ 25	11	51
Other (When going through article references)	5		5	

Table 4. Articles – found, chosen and disregarded.

For SAE Mobilus, each search phrase resulted in the same articles being showed, therefore the combined number still ends up as 62. Articles chosen were picked through different rounds of search terms, therefore the results are different for each search term.

The table shows the combined articles found from the search terms used. Because of the natural step to go through references of articles, more articles were found, and therefore not all are from the past 5 years. Some were published before then. Some articles were also found viewing the journals they were published in, since often an issue has a specific theme. A problem when searching for articles for this study was determining what articles were usable from the title alone, before taking them to the next step of reading the abstract. There are many articles broaching the subject, however, a majority focus on purely specific technical problems or suggestions for the future AV that handle a very small part of the vehicle – such as sensor technology. While somewhat relevant, the topic would be too broad if all articles merely mentioning AV had been used.

Webster and Watson (2002) is the chosen method for literature review as it is theme based and fitting to the subject of information systems and information security. In their article, they underline the need for conceptual structuring when it comes to reviewing already produced material. Furthermore, the method presented clearly emphasizes the steps, from beginning to end, of a thorough literature review:

Beginning → identifying literature → structuring the review → tone → tense → theoretical development → evaluating theory → discussion and conclusion, and finally, → the reviewing and revision process.

The beginning steps include deciding and presenting which level of analysis one chooses, the scope for the study as well as who can benefit from the results of the review. Identifying literature is the next step of which the relevant, and current, articles are searched for. The articles should be of varied sources, meaning preferable not just from one place geographically as well as of high quality. High quality sources of literature can be leading journals, conference proceedings and databases with peer-reviewed articles.

The structure of the review should take on a concept-centric approach rather than an author-centric one, according to the authors, this ensures that the literature presented is synthesized and logical. Below is a table from their method article, showing what a concept-, versus an author-centric approach looks like.

Table 1. Approaches to Literature Reviews

Concept-centric	Author-centric
Concept X … [author A, author B, …] Concept Y … [author A, author C, …]	Author A … concept X, concept Y, … Author B … concept X, concept W, …

Figure 4. "Approaches to Literature Reviews" (Webster & Watson, 2002)

By creating a concept matrix, the literature search is made simpler and each article can be fitted into a certain (or several) categories depending on its content. The X marks a concept's existence in an article, giving a clear view of what can be found and where. This is to ensure that the review has relevant literature as well as findings that correspond to the aim of the search for research.

Table 2. Concept Matrix

Articles	Concepts				
	A	B	C	D	…
1		✖	✖		✖
2	✖	✖			
…			✖	✖	

Figure 5. "Concept Matrix" (Webster & Watson, 2002)

Tone and tense refers to how article findings are discussed. Giving too much criticism to an article from the past is not beneficial to anyone, and does not add much value. Differentiating between a past statement and current concepts gathered from literature is important for the readability of the text, present tense is easier to read while past tense is used when presenting ideas from someone else – they may have changed. Theoretical development includes finding knowledge gaps and through that motivate filling this gap with knowledge. To do that, the review needs to point the direction of future research. By pinpointing what needs to be done in terms of future research, the field can be brought forward. Additionally, the authors bring up the importance to demonstrate not only the contribution but also the impact, logic and thoroughness

of the paper (Webster & Watson, 2002). By using this method when performing the literature review, this study will provide a concept-centric view of already existing research.

3.5 Planning

First setting out to be a security analysis in shape of a case study with Volvo, the study was going to use GBM-OA to perform a risk analysis of the information security the company applied to their future autonomous vehicles. The study was going to be performed with one or several specialists from the company to ensure there was a stakeholder – as an analysis of that calibre cannot be performed without certain information directly from the source. When they pulled out of the project, out of concern for information being at risk to be accessed by their competitors, the work had to go in a different direction. Time wise, this made the study start out at a disadvantage. This is how the Arrowhead project came into question, as my main contact through which my communication with Volvo was going, was in this project and was willing to present their prototype to me. The planning has therefore looked drastically different throughout the changes that were made.

This work was divided into different phases to separate the parts of the study. Each phase had a main objective. The literature review is an iterative process where phases will go into each other and overlap.

Phase 1 will be performing a pre-literature review to create the introduction and to establish the need for a literature review on the subject. This will be done by searching the databases accessed through the university and Google Scholar. The gathering will be to create the research questions and describe the concepts of the study – they need to be introduced before the literature review.

Phase 2 will be the phase in which the actual literature review takes place, alongside writing the report and the method chapter. The bigger literature review is done to answer the research questions – to create an overview of previous research and its findings on information security risks of the autonomous vehicle. The literature review will be performed by searching for peer-reviewed articles and technical articles published. Using the literature review method presented in the method chapter, the literature is presented in different categories according to the themes found - some articles have content corresponding to more than one category. The literature review will be an iterative process where more articles are found by going through references of articles found. The Arrowhead Framework book (Delsing, 2017) is gone through to find the chapters regarding information security, and these are reviewed in a chapter after the literature review.

Phase 3 will function as the discussion phase where the entire report will be gone through, each chapter being finalized before lastly finishing the discussion and future research chapters. A reflection on the study will be included as well as a method discussion. The literature review/result may be added to during this phase as well because of the nature of the study, but most of the literature review will be finished in this phase. Comparing the literature review to the Arrowhead Framework's security will continue in this phase.

Throughout these phases the report will be a continuous task to work on as every step of the method will need documentation. The method chapter will also be built alongside the steps being performed, to in a detailed manner describe the process. The outcome and discussion will be built alongside the results being created, these parts are heavy in the report and therefore they will take up a lot of time.

3.6 Work approach and progress

By building onto the initial proposal, the report was created and has been an ever-developing work through the literature review especially. The first step that went on well into the discussion was searching for literature in the subject and analysing peer-reviewed articles and technical articles. This was the most taxing part of the work as it requires a lot of reading and time spent finding the articles containing the most relevant information to the study. The approach was to gather enough information to be able to create an information security risk overview of the future vehicle – that does not yet exist. By gathering information, and in a planned and methodological manner combine it to make predictions is how we can prepare for the future. In this case, the future is the autonomous vehicle and its information security risk that can pose problems for the stakeholders, producers and users. The method for the literature review is discussed in the method chapter. With GBM concepts in mind, the literature review also brings up human interaction as a source of risk to consider as humans, just like other information assets, communicate and interact with each other and the cyber-physical systems they are to use.

Because of changes made along the way, including a company in the field pulling out of participating in the study, the study naturally took another shape. Using the extended literature, this study could become an overview of previous, and very current, research. Comparing the findings to a new framework sheds light on differences that can be useful on both ends.

3.7 Time Schedule

The preliminary time schedule is provided to show how the project of the thesis will be performed week to week. This time schedule changed as the work continued. The reason for including this is to get a clearer view of what was performed and when. Each step corresponds to a part of the report, or a part of writing it - as the writing of it will be intertwined with the literature review itself and the surrounding chapters.

Step	*Start (week)*	*Finish (week)*	*Duration (weeks)*
Literature search	1	15	15
Literature review	2	29	27
Framework review	14	29	15
Report template	1	1	1
Introduction	2	9	6
Method chapter	3	13	10
Concepts	4	16	12
Discussion	17	29	12
Conclusion	19	29	10
Future research	17	29	12
Finishing the report	18	29	11
Proof-reading	18	29	11

Table 5. Time schedule

As the study was postponed from June until August, an extra two months were added to the schedule, which is why the duration is longer than 20 weeks. Some steps were put on hold during the process of altering and adding onto the study.

During my visit in Luleå, I was shown a prototype and got a presentation of the technologies within it. Testing the prototype and viewing the documentation for the project convinced me I could use the security of Arrowhead to enrich the literature review with a real case security based on future CPSs.

4 Literature review

The literature below will be presented by the four larger concepts that were found in the articles. Information security and attacks was a theme found in many articles ranging from being the focus, to being considerations for future research. Since many articles who mentioned one, would mention the other, it was appropriate to group them together. Articles mentioning the AV almost exclusively also bring up attacks as well as information security, relating those concepts directly to the AV. Therefore, I decided to group the AV concept up with information security and attacks. The next concept found was Internet of Things, network, connectivity and communication – both internal and external. Connectivity and communication were rarely mentioned without using both, and many would bring up IoT with other vehicle connectivity (vehicle to vehicle for example) and networks used. Communication was linked to both connectivity and networks. Since it is hard to discuss IoT without the latter two, this too was deemed an appropriate match.

As the focus is information security, certain security risks were excluded as they involved pure software efficiency solutions for the integrated systems in the autonomous vehicle. The third concept is Suggestions, mitigations and risk management, which came from the literature review after comparing articles and finding that many that bring up various information security risks and attack scenarios, suggest for ways of mitigating and managing these. This is an excellent indicator for where more research may be needed, or to find out where efforts currently are being put. This theme directly corresponds with some concerns expressed by scientists, while also bringing the possible solutions or at least beginnings to them for the overview – effectively shining light onto future possibilities.

The last finding, knowledge gaps, had a larger presence in some articles while being almost non-existent in others, showing that the focus varies between researchers. This sub-chapter gathers the expressed knowledge gaps as well as presents those identified through performing the literature review. A table gathers the themes of these knowledge gaps for summary purposes as they are not presented in the concept matrix. This is because the nature of the research gaps differs from being explicitly mentioned to being picked up because of how researchers suggest future studies should be performed and where.

First, I will start out by presenting the concept matrix as per Webster and Watson's (2002) method for literature reviews. This shows each big concept found, which are latter grouped up into each sub-chapter.

4.1 Concept matrix

Below is the matrix showing the concepts found in each article used from the literature search. The concepts are presented in the top row, and the articles are presented in the far-left column. An X will represent finding(s) of a concept in an article. These concepts are then grouped up for each sub-chapter of the literature review findings to be presented in text form.

Information security as a concept is directly or indirectly expressed in literature, in articles presented below security is used for network security, communication security and other such

concepts that are included inside the term information security – they all relate to the same thing. Some use information security as a term, while others refer to it as simply security, as it is to be assumed what they mean considering the context of the article. Risks related to information security are presented in a column to the right of it.

Attacks and threats were grouped up since many articles handled them in a similar fashion, using attacks and/or threats to describe what security risks could suggest or lead to.

Mitigation and suggestion were however not grouped up because mitigation refers to articles explicitly describing ways of minimizing threats or risks, meaning they have developed methods or software/technology for handling them. Suggestion refer to authors describing what they would like to see more of, what they suggest others should do or something they have identified that needs further developing.

Connectivity and communication are so closely linked that they also were grouped up because of how they are used in articles. Connectivity, referring to connected vehicles, servers, devices, grids etc. and communication referring to the exchange of communication between these.

Safety and security are, too, linked, but not because of dependency. Safety refers to the safety of users of the future AV, and sometimes the safety of the software in the AV. Security refers to the information security, which, if failing, can have an impact on the user of the vehicle's safety, but not necessarily.

Table of concepts per article

Article	*AV*	*Safety*	*IoT*	*Attacks/threats*	*(Information) Security*	*Risk(s) related to ← + managing them*	*Mitigation*	*Suggestion*	*Connectivity/communication*	*Network*
Amoozadeh et al. (2015)	X	X	X	X	X	X	X	X	X	X
Bagloee et al. (2016)	X	X		X	X		X	X	X	X
Bangar et al. (2016)	X	X						X	X	
Bloomfield et al. (2013)		X		X	X	X			X	X
Checkoway et al. (2011)	X	X		X	X	X	X	X	X	X
Dakroub et al (2016)	X	X	X	X	X		X		X	X
De-J et al. (2017)	X								X	X
Decugis (2009)					X		X	X	X	X
Delsing (2017)	X	X	X	X	X	X	X		X	X
Edwards et al. (2017)	X	X	X	X	X	X	X		X	X

Article *CONT.*	*AV*	*Safety*	*IoT*	*Attacks/threats*	*(Information) Security*	*Risk(s) related to ← + managing them*	*Mitigation*	*Suggestion*	*Connectivity/communication*	*Network*
Fagnant et al. (2015)	X	X		X	X	X	X	X	X	X
Hoppe et al. (2011)	X	X		X	X	X	X	X	X	X
Kang et al. (2016)	X	X		X	X				X	X
Koscher et al. (2010)	X	X		X	X	X	X		X	X
Lasi et al. (2014)									X	X
Lee et al. (2015)			X						X	X
Li et al. (2017)	X	X	X	X	X	X	X		X	X
Macher et al. (2017)	X	X		X	X	X	X	X	X	X
Mascareñas et al. (2017)	X	X		X	X	X	X			X
Natale (2012)				X		X	X		X	X
Neumann (2016)	X	X	X	X	X	X	X	X	X	X

Article *CONT.*	*AV*	*Safety*	*IoT*	*Attacks/threats*	*(Information) Security*	*Risk(s) related to ← + managing them*	*Mitigation*	*Suggestion*	*Connectivity/communication*	*Network*
Niklas et al. (2016)	X	X			X				X	X
Paar et al. (2010)		X		X	X	X		X	X	X
Parkinson et al (2017)	X	X		X	X	X	X		X	X
Pesé et al. (2017)	X	X		X	X		X	X	X	X
Petit et al. (2015)	X	X		X	X	X	X	X	X	X
Schneider et al. (2017)	X	X		X	X	X	X	X	X	X
Shields et al. (2017)	X	X	X	X	X	X	X		X	X
Sullivan et al. (2017)		X		X	X	X	X		X	X
Thing et al. (2016)	X	X		X	X	X	X	X	X	X
Vogel-Heuser et al. (2016)			X						X	X
Woodderson et al. (2017)	X	X		X	X	X	X		X	X

Article *CONT.*	*AV*	*Safety*	*IoT*	*Attacks/threats*	*(Information) Security*	*Risk(s) related to ← + managing them*	*Mitigation*	*Suggestion*	*Connectivity/communication*	*Network*
Yagdereli et al. (2015)	X	X		X	X	X	X	X	X	X
Zaidi et al. (2015)	X	X		X	X	X	X		X	X
Zheng et al. (2015)	X	X							X	X
Zou et al. (2017)		X		X	X	X	X		X	X
Summary (number of articles bringing up each concept): ***/36 Articles***	***27***	***30***	***9***	***28***	***29***	***24***	***26***	***15***	***35***	***35***

Table 6. Table of concepts per article

As can be viewed above, concepts such as AV, Safety, Attacks/threats, Information security, Connectivity and Network were found in most articles while IoT and Suggestions were not found in as many. Safety, not being a concept that was anticipated, will be brought up later in this chapter as an interesting finding. Safety being linked to Security is not a given, but many articles made the connection of having to consider Safety closely linked to Security in many cases as the future AV will have to not only keep people secure, but also safe.

Communicated information is the biggest risk for autonomous vehicles. Because of the connectivity of AVs, and the nature of the data that is stored, used and communicated (sent and received), mitigation techniques for risks related to the security need high prioritization. To show the findings by concepts from GBM-OA, assets and genres, as well as containers, identified in the literature are presented in a table below and will be compared to the Arrowhead Framework. All items listed are from the articles in the above matrix (excluding Arrowhead Framework literature).

4.2 Literature findings by GBM-OA concepts

Literature findings, GBM-OA		
Genre	**Asset**	**Container**
Speed input	ECU/actuator	Control system
Steering input	ECU/actuator	Control System
Sensor data being stored and used, sending, receiving and storing information in the AV and to/from websites, servers through Internet connection	Internal network/local cloud	Internal communication
Communicated vehicle status, location, speed, destination	External network (VANET, ad-hoc, Internet, V2V, V2X)	External communication
Vehicle functions system input	Vehicle control	Control system
Human-interface interaction	Safe practices	People

Table 7. Literature findings, by GBM-OA concepts

The containers show what the critical areas to protect are, and how they can be separated by what assets and genres they handle. This way of categorizing communication and the users of it can help when going further in analysing security threats and needs to ensure high security.

The identified containers are: Control system, Internal communication, External communication and People.

4.3 The Autonomous vehicle and information security + attacks

Because of the nature of these future vehicles, not only dangers such as life-threatening ones are a reality – but also privacy concerns. Macher et al. (2017) discuss the concerns for security of CPSs, and indirectly the AV, as stemming from dependency. The dependency for these systems to be reliable and have all necessary security implementations is high. In their article, they mean that information security now must be implemented at an earlier stage of development – it needs to be there from the beginning and be a priority when developing systems that not only have to be functional, but also have high security. They express the need to focus on the entire vehicle, and treat it as one complex system rather than a combination of sub-systems. Another study (Bloomfield, Netkachova & Stroud, 2013) brings up dependability in these CPSs when discussing security and safety in their combined form. They mean that more are realizing how close the two are and how one cannot exist, or be considered without the other. Historically, they have not been closely connected before, but with the future systems complexity, they should be. In their study, they conclude that methods applied for safety share a lot of similarity with security controls, and call for a methodology that handle security and safety combinedly.

4.3.1 Types of attacks - large scale to individual

Challenges can be divided in two categories, first there must be expertise for the individual technologies inside the CPS, but secondly, there must be a merging of these aspects into one, for the entire product (Macher et al., 2017). Furthermore, it is not just a matter of singular attacks targeting one vehicle at a time. Terrorists could, with access to a grid of vehicles, control large masses of them and disrupt the infrastructure of a big area. The types of attacks here could be as 'simple' as overcharging batteries simply to destroy, or they could be as harmful as trying to injure or possible kill the driver of the vehicle (Peer et al., 2010). Of course, attacks, until they happen, can only be speculated around – but that is the strength of planning for information security, trying to be one step ahead.

There is also the threat of malicious hackers gaining access to the communication channels used (Yag, Dereli, Gemci & Aktas, 2015). While eavesdropping attacks initially are not as critical as attacks to gain control over an AV, unauthorized users gaining access to information that is not meant for them could lead to great economic losses and security issues further down the road. Zaidi and Raharajan (2015) mean that attacks of the remote-control kind must be the most prioritized security threat to consider, as it by far is the most dangerous type of attack for the individual(s) in the AV. It could also very likely injure people in surrounding vehicles if one vehicle suddenly makes a very swift turn on a highway for example. Eavesdropping however is still a valid concern for individuals that may be communicating personal information – the communication channels should be of high integrity and confidentiality. In found research it has been expressed that while there are plenty of studies done on safety, meaning the vehicle's capability of driving safely, there is a need for further studies done on security. There is a need for standards and regulations to ensure that autonomous vehicles, regardless of manufacturer, have countermeasures in place for attacks (Bagloee, Tavana, Asadi & Oliver, 2016; Petit & Shladover, 2015; Neumann, 2016).

4.3.2 Personal and sensitive information as targets for attacks

Focusing on the information security aspect when it comes to personal data, Fagnant and Kockelman (2015) express concern regarding the sheer amount of data that will be logged and possibly accessed by government employees or those who gain access to such information unauthorized. The CIA triad is as relevant now as it has been with securing communications for other systems in the past. While tracking of movement has been around for a long time today, the sensors that will be acting with the infrastructure grid as well as the previous technology, will bring the ability to track peoples' movements to another level that we have yet to experience (Li, Ma, Medjahed, Wang, Kim and Mitra, 2017).

There is a lot of information that can be extracted from gaining knowledge about how a person moves around in their day to day life. Financial status and habits may seem harmless at first to some, but paired with the rest of the information that can be tracked a detailed profile could be created to be used by malicious entities. Phishing and scam attacks are on the rise, and privacy as a topic is growing in discussion in media, both on the level of how much data governments should possess but also how much personal data that is stored and can be accessed by anyone. Li et al., (2017) bring up privacy in their study about mechanisms for preserving privacy data. They

want to achieve a balance when it comes to how much information is used and stored and how privacy can be kept. In their study, they suggest a framework for storing data in clouds with high security implementation to ensure user privacy while data collected can still be used - without risking serious leaks of personal information.

Depending on whether data is gathered and stored, for how long, and who will be able to access it (government employees only, car company, insurance company etc.) measures must be taken to ensure the integrity and confidentiality of said information. It is important to notice that although a person may be the owner of a vehicle, the information that vehicle holds will not be made available to access by the owner. This has many reasons, for example if the vehicle has been involved with an accident and there is an investigation the owner cannot access the information – to ensure the integrity of it. From the manufacturer side, there is also a need for the software to not be tampered with, because then they cannot ensure the quality and functions of the vehicle any longer and it may become a hazard on the streets. The complexity of this matter is yet another of the many reasons as to why information security plays a big role in the development of the future AV.

4.3.3 Attacks targeting the control system and functions of the AV

What all the research points to is that there is a lot more work to be done, leaving many gaps to be filled by future research. The various security concerns expressed by researchers paint a good picture of where those developing the technology for the future autonomous vehicles should be turning their attention. Hopper, Kiltz and Dittmann (2011) categorize their concerns for the CAN by the CIA triad as well as authenticity and non-repudiation, underlining that CAN has major security issues that must be addressed. Attacks and exploits that CAN is prone to range from DoS, faking messages, spoofing and the fact that CAN does not have any authenticity controls. The authors mean that out of all security concerns, confidentiality is the least worrisome one, as a breach of confidential information would not directly result in outcomes as bad as the other attacks can result in. To explain further, a successful DoS attack would render any communication during it impossible and could lead to dangerous situations. Availability is always a critical factor when considering information systems, because an information handling system that needs to be accessed by its users, often depending on it, often operates on a 24/7 basis. If information cannot be reached, it could lead to systems malfunctioning and security may be low momentarily, the time depending on how long availability is blocked.

To build onto the potential threats that arise when looking at the AVs technologies and the information that it handles, there is a human aspect to consider (Parkinson, Ward, Wilson & Miller, 2017). While not mentioned by many as a security aspect, it is important to consider. While the vehicle in its manufacturing stage is only used and accessed by people with experience of the technology and the knowledge to operate the AV's various systems – the average driver may not be as technically inclined. This of course leads to information security risks of the nature that is harder to mitigate, as it requires the person who owns the vehicle to be aware and knowledgeable enough to avoid phishing attacks. Victims of such attacks are often those who cannot tell the difference between known sources and malicious ones. It is also possible to be targeted and miss that you are being attacked until it is too late. The knowledge of people using

the vehicles could be a vulnerability that needs to be addressed. How this is going to be done is yet to be explored, but for many complex systems people interact with in their line of work, they need to take classes and certificates to ensure safety and security.

Parkinson et al. (2017) bring up the human as more passive in its role when it comes to the future AVs, of course depending on the route manufacturers will take. If the vehicle has more autonomy, the human will most likely have less and the other way around – both cannot coexist. Their point is that manufacturers may decide to make humans observers and passengers rather than the driver – this however begs for many questions regarding what level of autonomy the user of the vehicle may gain in case of a malfunction of the vehicle's information based functions. Another rather unexplored part of the equation that is information security for the future AVs.

Functions and usages of various applications come from a wide range of security possibilities, for example there are secure communication suggestions developed (Shields, Huser & Gell, 2017). Suggestions are also made for how vehicles should communicate with each other in a secure manner as well as how internal communication should be encrypted within the vehicle (between ECUs), and not only for external communication purposes. With the software used in the vehicles, and the vast amount of coding that goes in to them, Edwards and Kashani (2017), present the first existing method for finding bugs efficiently in automotive systems. According to the researchers, flaws in these vehicles can and will be exploited by those with malicious intentions. Source code is brought up as a main security concern for ECUs now and in the future as AVs continue their development. Edwards et al. (2017) mean that an attack on one vehicle can quickly hit many vehicles if successful, since manufacturers will use similar control systems for their AVs. The challenge for the code is to be flawless when the production has been finalized, however this is a difficult goal to reach since problems may arise in late development and go by undetected.

Furthermore, in modern vehicle analyses of vulnerabilities and attacks on vehicle software, research shows several bugs and exploits that can be used (Checkoway, McCoy, Kantor, Anderson, Shacham, Savage, Koscher, Czekis, Roesner, & Kohno, 2011). Authors show an external overview of modern vehicle attack possibilities including the interface within the vehicle with the conclusion that it is more likely than not that further vulnerabilities are unknown. While not done with the future autonomous vehicle in focus, the study gives greater insight to how many doorways there are to consider when securing a vehicle. While vulnerabilities are addressed continuously, more will arise with new technology. Implementing ways of detecting these security flaws, both in the development of software as well as during the life cycle of it, is vital to address these threats.

4.4 IoT, network, connectivity and communication

To maintain confidentiality, integrity and availability for the autonomous vehicle is vital to its security (Schneider, Kohn, Klimke & Dannebaum, 2017), and not only because of the communication between the vehicle and its surroundings, but also because of the overall connectivity that is and will be expected of the user. Having direct access to the Internet and being able to use various applications through personal devices connected to the vehicle while

traveling brings up a wide range of potential security risks and threats. And yet we have not covered all communication to and from the vehicle, V2X.

IoT has already brought us hyper-connectivity between our devices and applications and the ability to always stay connected, when we are able to access a network – so it is only natural that the autonomous vehicle will provide us with a further enhanced experience than vehicles today offer (Li, Ma, Medjahed, Wang, Kim & Mitra, 2017). It is more common than not for new vehicles today to have the option for the user to connect its phone to be navigated through via a display in the front of the vehicle. Some offer a brand unique UI while others offer the UI of the phone to be directly accessible through said display. Now, the connection may not always be there while traveling today, but in the future, we can expect every car to be connected. Connecting, and allowing your vehicle to store all your phone's information, and at the same time being able to control your vehicle through said phone, creates a reality in which yet another point of – unauthorized – access can be made available. This has however not been a priority thus far when developing these vehicles since, after all, their main function is not to provide an entertainment center for their users with constant connectivity for social media and other personal communication and browsing.

4.4.1 AV dependability

While AVs will depend on communication and availability, there is also a larger perspective to consider when discussing security concerns for the future of transportation. Paar, Rupp, Schramm, Weimerskirch and Wolf (2010) propose a big concern to consider when discussing information security for the future AV, since the prognosis is that it will be run on batteries rather than gasoline. In their study, they bring up the economic and delivery issues that could arise with an even larger use of electricity. It is yet another aspect that needs to be considered as the world has witnessed attacks on larger grids recently with Ukraine (Sullivan & Kamensky, 2017) for example, when the capital's power grid was put out by attackers.

The information security for the AV will not be limited to the vehicle or its communications, one must think about the ability to slow the infrastructure down to a halt by limiting electricity – the average electric car today does not run for many miles before it needs charging. Of course, the duration of the batteries is constantly being extended with the development of these vehicles. While power grids are not the focus here, the big picture is what needs to be considered to ensure high security. There could be disastrous consequences if the power outage following an attack to the power grid would be lengthy, because of the reliance on electricity for implementing security measures (Peer at al., 2010). Given the power outage is widespread and possibly influencing availability of information needed to safely operate the vehicle, there must be security measures implemented to handle such incidents. Without electricity in the scenario in which AVs are all run on electricity, there will be yet another large part of society that is reliant on the power grids continuous functioning.

Zaidi and Raharajan (2015) studied vehicular internet and autonomous vehicles and concluded that there are notable challenges that need be dealt with, when it comes to security and privacy, before the autonomous vehicle is released. In their article, they have studied vehicular ad hoc networks, or VANETs. A VANET is a vehicle to vehicle (V2V) connection that means the

vehicles use a wireless network created between them to communicate with one another. It is the same concept as mobile ad hoc networks, a spontaneous connection ensuring an information exchange, but this vehicle version supports applications for certain vehicle-only features that are useful to broadcast to several vehicles nearby for security and efficiency purposes.

Together, vehicles using VANETs can create a combined cloud storage of information they all need and can receive – sensor data about weather for example, or in case of an emergency specific information can be requested by emergency services through the same cloud. In their study, Zaidi and Raharajan (2015) discuss how security for VANETs is needed and how it can be implemented. Certain information, like location, will be requested to be sent from each vehicle continuously, but location, unlike weather data, is personal information and can be tracked by others than governmental figures in case of the security not being high enough. The vehicle to everything (V2X) communication (Paar et al., 2010) is visualized in the figure below, showing what a mapping of it may look like.

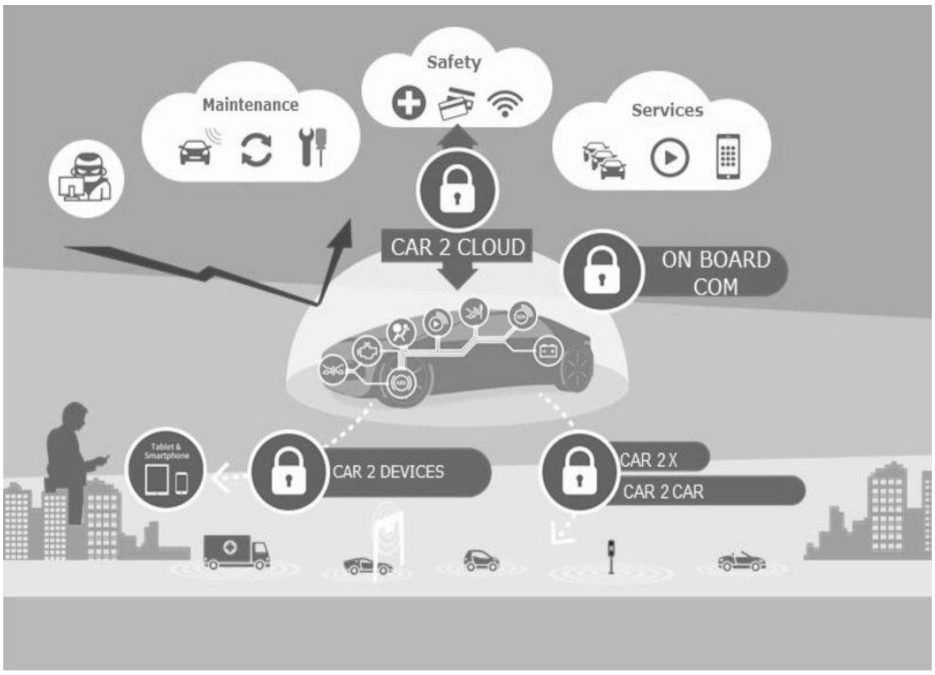

Figure 6. "Connected car and the need for security" (Schneider et. al., 2017)

4.4.2 Internal or external communication

The different type of threats that will expose the vehicle to adversaries can be categorized in two groups, internal and external ones. Devices; mobile phones, computers etc., and communications; sending and receiving data to various servers storing and analyzing the vehicle's information, are examples of internal versus external threats (Edwards & Kashani, 2017). By separating internal from external threats, we can develop counter measures to possible attacks and vulnerabilities that these two groups may suffer from. Information security is and will be a

big obstacle before we can rely on autonomous vehicles for transportation. There are many components in autonomous vehicles, many more than in the vehicles on the roads today – many of which will be communicating not only with each other but with external sources. Research on the communication between vehicles, which is vital for the vehicles to be able to safely interact with each other on the roads, show that there is a need for countermeasures to different attacks that will target these V2X communications (Amoozadeh, Raghuramu, Chuah, Ghosal, Zhang, Rowe & Levitt, 2015). Furthermore, the researchers express that because of these types of vehicles' need for instant exchange of information between them, they are prone to eavesdropping attacks and other such attempts to intercept the communication methods. Various ways of ensuring privacy and anonymity is therefore something that should be implemented: such as encryption, short-term certificates and group signatures.

Other methods for ensuring security for the communication is to use automotive firewalls (Pesé, Schmidt & Zweck, 2017). Since the vehicle will be just as prone to remote attacks as any other device connected to the Internet, and perhaps even more so since the vehicle may be the target for both malicious users trying to take control over it either for stealing it, eavesdropping or stealing information, or simply to cause damage – firewalls and intruder detection software will be the minimum security required. Parkinson et al. (2017) mean that privacy needs to take priority among other concerns when considering communications of the future AVs. While privacy is not a new concern when it comes to V2X communication, there are many new risks that will need to be resolved and mitigated. In their study, they have many suggestions for how to battle these risks, which will be mentioned in the next sub-chapter.

4.4.3 CAN security concerns

With the connectivity level of the AVs, there will be a lot of traffic passing through and to be able to block out malicious types this will be critical. These are just a few ways of which the security can be held high for the information these vehicles will handle. This will all be vital to the vehicle's functions and the need for securing it is high. If an unauthorized user, for example, could see the communication or alter it somehow, we could be looking at disastrous "accidents" where malicious hackers have taken control over vehicles. To avoid this, further research needs to be done regarding ways of securing the autonomous vehicles of the future. Naturally, there are many other types of attacks that will be used to target autonomous vehicles, such as, eavesdropping, Denial of Service or various types of disruptions of the basic functions of the vehicle. Features of the Controller Area Network, or CAN – a network developed for and widely used by vehicles – that according to Zou, Chan, Gui, Chen, Scheibert, Heidt and Seow (2017) that are vulnerable consist of the following: Lack of device authentication, segmentation, data encryption measures and broadcasting.

Hoppe et al. (2011) also discuss CAN in their study with the outlook that the network is not very efficient and secure, but that it possibly could be with certain implementations (these will be brought up in the next sub-chapter). However, the availability of CAN is not great. The network is easy to overflow with messages and because of the way messages are sent to each node within the network, it is not overly complicated to insert messages – CAN does not require addresses of the senders. Despite the somewhat hopeful suggestions by Hoppe et al. (2011), they

give large criticism to the CAN bus and how it does not meet basic requirements for information security. With their analysis of the network readers can conclude that there is a lot of work to be done before one can deem CAN a secure enough network for future AVs. Koscher et al. (2010) list the various vulnerabilities of the CAN network and include the overflooding, for example a DoS attack, how there are no authentication for packets sent within CAN and how it would be easy to not only listen to messages but also intercept and inject packets. Yagdereli et al. (2015), too, express their low trust in the CAN bus used today since according to them, CAN is simply not equipped to handle security risks arising from the connectivity the future AV will need.

4.5 Suggestions, mitigations and risk management

While many studies bring up security risks and concerns for the future AV regarding connectivity and the systems that will be used inside the vehicle, there are also a considerable amount of suggestions and mitigation approaches to handling some of these expressed risks. Some suggestions are brought up and studied more than others. Those who were found in the literature review will be presented in this chapter.

Privacy is a huge concern for the future AV, not only are scientists expressing how the position tracking along with personal information may make it easy to find out a great deal about a person's habits and daily lives – there is also the concern for how this information will be accessed and then used. Parkinson et al. (2017) predict that information about people collected anonymously may be used for commercial purposes when sold. But it is a fine line to draw, deciding what information is fair game and what information should be kept private to logically possible extents. Suggestions for how to combat this information security concern are many, for example cryptography is one of them. Cryptography can be used in various ways – applied to communication to ensure that confidentiality and privacy are kept highly secure, to ensure authorization functioning properly. One suggestion is for it to be used for CAN messages to ensure high integrity (Hoppe et al., 2011), especially as CAN today has no way of doing so. Zaidi and Raharajan (2015) discussed VANETs and security of information sent from vehicles about location and how eavesdropping is possible without proper security. Therefore, the authors suggest authentication and traceability to ensure integrity and non-repudiation of these messages.

A suggestion expressed in a study (Paar et al., 2010) for security implementations bring up malicious intent and how there is a need to have methods for stopping inside or outside attacks from happening when there is a conflict of parties involved with the systems inside the AV. Kang and Kang (2016) studied intrusion detection for the internal network of the vehicle. Concluding that a specific method for training the IDS (intrusion detection system) to recognize a wide range of packets, trusted and malicious ones, had the result of a high rate of catching malicious entities from entering the internal network, or in-vehicular network as they call it. Speculations regarding such human factor are necessary since we can to great lengths control the information systems as assets, but human assets are harder as their intent is often unknown. In their study, Thing and Wu (2016) present an informative map of AV defences as they call them – security measures of varying nature, for example both preventive and passive defences. In the figure

below, which serves as a good map for defending against certain security attacks, they have traced what kind of defences can be implemented in the future AV. Below is the map.

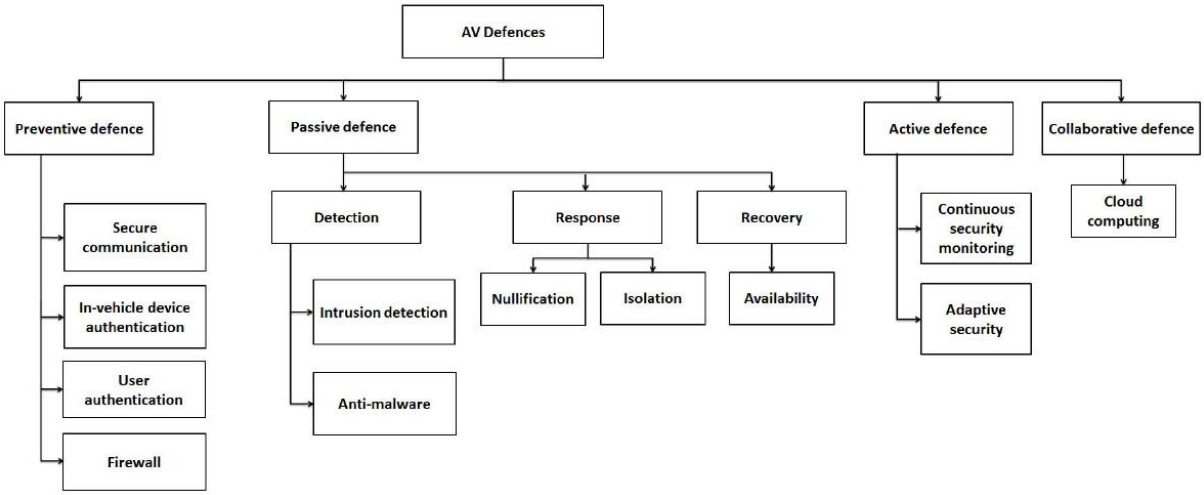

Figure 7. "Autonomous Vehicle Defence Taxonomy" (Thing & Wu, 2016)

Many of these can be found in devices today, although of course, the security will need to be adapted to vehicles. Hoppe et al. (2011) bring this up in their study – how while regular software security implementations for desktops are a good start for AVs, there needs to be a consideration and development for securing the hardware. This is because of how the attacks scientists see potential for happening not only serve a threat to information and privacy, but also to the hardware in the vehicle. Manipulating the sensors and the nodes in the vehicle would have consequences beyond law-bound fees and a hurt reputation.

4.5.1 Standardizing and integrating security

Methods and architectural standards are going to be needed for the further development of AVs (Macher, Messnarz, Armengaud, Riel, Brenner & Kreiner, 2017). One study suggests that many security issues could be solved by standardization when it comes to architecture and developing the systems within the AV. They (Macher et al., 2017) mean that they could find useful approaches using combined standards that already exist as a base for integrating security measures (and safety ones). In their study, they mean that safety and security must be intertwined as they are part of the same implementations and considerations – and because a security threat made reality is a direct threat to safety, in terms of attacks targeting nodes and control systems. An attack carried out to nodes responsible for carrying out functions critical to the vehicle's steering or otherwise basic controls, could be fatal to the users of the vehicle.

Edwards and Kashani (2017) also suggest a standard for developing the software used in AVs to find security issues in the early process. AUTOSAR, or Automotive Open Source Architecture, a worldwide attempt at creating standardizations for the automotive industry development is a partnership between many huge manufacturers of vehicles (Niklas & Rathgeber, 2016). With the development of the future autonomous vehicle, they present software architecture that can

be used across different manufacturers for more efficient communication. By standardizing architecture for autonomous vehicles, security mitigations could be more efficiently developed and implemented, since the vehicles would operate on the same standard in many ways.

Schneider et al. (2017) conclude that their stance on future security for AVs is that the holistic view is the way to go – instead of focusing on individual parts. And when they say holistic they mean all the way from start to finish, development to maintenance. They do however not suggest any way of implementing this view, but do suggest specific solutions, like many others.

Not all suggestions brought up directly correspond with an information security risk, there were also some suggestions regarding how the communication from vehicle to vehicle could be used for safety purposes. Zheng et al. (2015) suggest in their study how vehicles could send out, for anyone nearby to hear, messages about the weather status where they currently are driving. This could be a way to make information that is sensitive the only information that is put under information security measures.

4.6 Summary

Summary of findings in the sub-chapters above in form of answers to the research questions.

1. Many security risks brought up in the studies regarding future AVs are risks we can find in modern vehicles today, albeit the same technology may be more critical in the future since vehicles today are not controlled by software – they are manually controlled by the person driving it. The most critical risks are those where attacks can mean remote control or disruption/control of nodes or ECUs within the vehicle's internal network. Communication and connectivity were the two greatest areas where research has focused their security concerns and suggestions. These two are highly critical to the AV as it will depend on them 24/7. The internal network is critical to keep guarded from unauthorized outside access of any kind. Architectural weaknesses include there being no standards, meaning solutions take longer to be developed, and that adequate efforts are still not being made to ensure that (information) security is implemented at the early stages of system development.

2. Implications of these security risks vary from personal information being accessed by unauthorized entities, to the more critical kinds where injury to owners and users of the AV is likely in terms of an attack. Attacks are expressed to range between singular vehicle attacks to full grid ones across a geographical area, the size cannot be speculated around as it will depend on technologies and how far VANETs and communications reach based on location for vehicles. Confidentiality, integrity and availability are all critical to securing the future AV as listening to, changing or interrupting messages – both externally and internally, may cause malicious entities to be able to target vehicles and perform disruptive actions to them. Mitigations today are scattered and less prevalent than expressed risks and concerns. There is a lot of question marks when it comes to how certain security risks will be solved, and a lot of criticism to current systems and the CAN used in the automotive industry. There are indications new

networks might become the next standard, but a lot of the information security solutions will partly be up to the manufacturers' ability to agree on standards for developing these vehicles. The most occurring mitigations suggested by scientists are: standardization for development methods and risk assessments, full-picture considerations for security where security has an early role and priority in development. Specific mitigations found in the literature review will be presented in the table below.

3. See summary of chapter 5: 5.7 Summary page 56.

4.6.1 Table – summary of risks

Below follows a table of most occurring findings.

Summary of risks		Summary
AV and information security + attacks	**IoT, network, connectivity and communication**	**Suggestions, mitigations and risk management**
Vulnerabilities of the CAN network when it comes to integrity, authentication and availability.	CAN – No authentication for packets/messages, no availability, low capability	Accepting privacy concerns as risk management, as security of the AV functions should be prioritized over the integrity of the human using the AV.
Privacy (integrity) concerns	DoS and other kinds of attacks on availability of system or network, injecting malicious packets, eavesdropping, remote control of ECUs.	Standardization of architecture for better security/attack mitigation between manufacturers.
Physical access to AV, injecting malicious code, trying to gain access to (personal) information residing in AV.	VANET security when sharing – sometimes confidential - information regarding AV in a cloud for other vehicles as well as emergency services to access	Implementing security at an early stage of developing the future AV.
User safety, an attack could result in immediate physical danger of the person using/driving the vehicle	Remote control of vehicle functions through attacks, malicious large- or small-scale access to vehicles	Standardization of communication between manufacturers.
User knowledge – human tampering with vehicle or non-secure behaviour	Ensuring confidentiality of personal information that is communicated to various servers and clouds	Separating personal information from information that can be used to track people's movements
	Integrity of sensor readings can give wrong input to control system	

Table 8. Summary of findings

The table above shows a summarized version of the findings for a better visual and overview of the literature review. Each column represents a sub-chapter of the literature review, but each line is not connected.

4.7 Knowledge gaps

In this sub-chapter, each knowledge gap identified will be presented, how it was identified will be explained and in the end of this sub-chapter, a table for all knowledge gaps will be shown for a clear view of what the gaps are. Implications for each knowledge gap will also be brought up, to be further discussed in the next chapter: Discussion.

The knowledge gaps that have been expressed by literature will be presented in this sub-chapter to shine light on the combined efforts of studies. While some have called their observations knowledge gaps, some have also referred to them as suggestions for future research or simply discussion points for their studies and how there is more knowledge that needs to be mapped regarding found and possible security risks.

4.7.1 List of knowledge gaps and articles

List of knowledge gaps including articles:

- Concern regarding whether cryptographic responses to security be enough with the development we are currently seeing in computing. (Parkinson et al., 2017).

- Lack of studies about responses to attacks on the AV, how to inform the driver on such an attack being ongoing and how to disengage if possible. (Parkinson et al., 2017).

- Ownership of data, who would be ultimately responsible for security of said data and what kind of data will be stored. (Parkinson et al., 2017; Bagloee et al., 2016; Fagnant et al., 2015).

- V2V communication can be used to falsify messages to vehicles nearby, putting vehicle users in danger, lack of knowledge about this. (Bagloee et al., 2016; Parkinson et al., 2017).

- Vehicle responsibility in terms of ultimate control, who is responsible in case of an accident? (Bagloee et al., 2016; Fagnant et al., 2015)

- Lack of standardization (Bloomfield et al. 2013; Edwards et al., 2017; Macher et al., 2017; Parkinson et al., 2017; Wooderson et al., 2017)

- Lack of knowledge about ECU, sensor, GPS vulnerabilities (Parkinson et al., 2017; Koscher et al., 2010; Neumann, 2016; Paar et al., 2010; Parkinson et al., 2017; Schneider et al., 2017)

- Lack of knowledge on communication vulnerabilities (Checkoway et al., 2011, Fagnant et al., 2015)

- Lack of knowledge on privacy concerns, who can access information, legalities (Fagnant et al., 2015; Parkinson et al., 2017)

- Lack of research and suggestions for whether manufacturers should report their found vulnerabilities or not (Parkinson et al., 2017), Checkoway et al., 2011; Fagnant et al., 2015; Parkinson et al., 2017),

- CAN security concerns (Hoppe et al. 2011; Koscher et al., 2010; Yagdereli et al., 2015; …)

- VANET security is still far from secure enough to handle AV communicated information (Amoozadeh et al., 2015; Zaidi et al., 2015).

Parkinson et al. (2017), Koscher et al. (2010), MORE all express open-ended questions regarding safe state of the vehicle, a sort of mode that one can revert to or start, in case of systems being attacked within the AV. The functionalities of such a state is unclear but could include the driver being warned about having to take control over the vehicle and allowing the vehicle to turn off specific systems to ensure the vital functionalities of the vehicle, but denying others.

Zaidi and Raharajan (2015) bring up a very interesting perspective to what the future may hold for AVs and the handling of information. They pose the scenario in which location history could be beneficial to the individual to share with their insurance company to, possibly, gain a lower premium if the locations are considered safe. They raise thoughts about how information could be used in a positive way, granted the individual feel like their privacy is worth a lower premium in the case of the insurance company. Another, certainly negative, thought to consider that they bring up is how it could be turned around as well – speeding in your AV could mean an instant report to the authorities responsible for giving you a ticket. What the future holds in those cases however is yet to be seen.

4.7.2 Knowledge gap – possible impact/risk table

Knowledge gap	*Possible impact/risk*
Lack of knowledge of specific systems, detailed reports	Partly unexplored risks, the possibility of attacks on the AV to take control of nodes and hinder vital parts from functioning. Attacks on both the internal and external communication of the AV
Lack of standardization	It is unclear to researchers, developers, and ultimately manufacturers how to most efficiently combine their efforts to finding risks and ensuring high security by their research when there is no general accepted standard for the future AV security
Ownership of data	Legislation is behind, the uncertainty needs to be cleared before manufacturers can implement certain security measures to ensure data is only accessed by those who own/need it
Lack of knowledge about ECU, sensor and GPS vulnerabilities	Security measures that are implemented do not cover the vulnerabilities unless these areas are explored further, this will result in successful attacks and vehicle users in possible danger
CAN – lack of knowledge on security concerns	The internal network of the vehicle may be incapable of handling all communication it needs to and the vehicle may suffer problems when it comes to control system and functions
How to inform driver about an attack	Each manufacturer may take it upon themselves to implement various ways of handling an ongoing attack, without standardization it may be hard for users to understand what to do in case of an attack
Lack of knowledge about responses to attacks	Without knowledge about attack responses that are appropriate, manufacturers may not have implemented mitigations to handle attacks that have not been accounted for – or are new – an automatic stop to external communications and leaving control to the user of the vehicle may be an appropriate response depending on the nature of the attack

Privacy of vehicle usage, regarding laws and regulations – speed limit example	What information is to be sent to authorities, insurance companies etc. and when. Can there be a privacy of speed and other information or will speeding instantaneously result in a ticket being sent to the owner of the vehicle or will the user be able to decide on the privacy of such information.
Privacy of personal information	User information regarding location and other identifying information can be accessed by unauthorized users – not necessarily critical to safety but a possibility. Will user privacy regarding habits and daily life be a concern for manufacturers or will security directly responding to user safety be prioritized?
Lack of knowledge about VANET security	An attacker can intercept communication or falsify communication locally to other vehicles to physically harm them or to interrupt traffic
Will cryptography today be enough to ensure security	Concern that future computing will be able to access communication information despite cryptography

Table 9. Summary of knowledge gaps and their impacts and risks

In the table above – as a continuation from the knowledge gap list - the knowledge gaps identified as well as their possible impact and risks have been listed to give a clear view of what their implications could be. This also serves as explanation as to why these knowledge gaps are important to fill.

5 Arrowhead Framework

The Arrowhead Framework documentation by Delsing (2017) describes the security approach and solutions that are a part of the framework. There are two chapters focusing on security, chapter 6 "Engineering of IoT automation systems" as well as chapter 10 "Application system design – High security". These are the chapters I have used to apply GBM-OA concepts to present and analyse the information security of the framework.

From my visit in Luleå at LTU and meeting with scientists and engineers from the Arrowhead project I got to view the prototype they had built and I also received an informal presentation of the vehicle prototype and its functions. From the documentation, I decided to perform a comparison between the application system design security, a standalone chapter of the Arrowhead documentation (Aldrian, Priller, Schmittner, Plosz, Wagner, Hein, Ebner, Maritsch, Ruprechter & Lesjak, 2017), as well as the Engineering of IoT automation systems chapter (Carlsson, Vera, Arceredillo, Tauber, Ahmad, Schmittner, Plosz, Ruprechter, Aldrian and Delsing (2017). Using GBM concepts and the information security risks, suggestions and gaps found in the literature review, the Arrowhead framework's security will be presented and compared. Findings will be summarized by the end of this sub-chapter, and discussed in the next chapter.

5.1 Summary of Arrowhead Framework: Application System Design – High Security

Aldrian et al. (2017) have in their chapter considered how equipment has not been designed for connecting to the Internet in the automotive industry. Because of this IoT perspective, they have concluded certain features that should be included. Authentication, certification, and reliability, as well as means for continuous assessments against security threats that may arise in the future. The requirements for the Arrowhead Framework's method were defined as following: Using the ISO/IEC 20922 protocol because of it being "firewall friendly" (Aldrian et al., 2017, p. 319), as well as an authentication service for machines, and requiring architecture to be "…evaluated according to security and safety methods" (Aldrian et al., 2017, p. 319).

With the use of a mediator that connects to the internal network and the Internet, the main function of it is that it does not have any routing functions to deny entry from external sources to the internal network without total input validation. The mediator stands for the security of a device, stopping unauthorized users from externally being able to connect to the internal network. The historian is another application that logs every event of the system, ensuring that nothing goes unseen and therefore every alteration can be tracked.

- How to ensure that only non-critical data documentation is stored on the mediator?
- How to ensure only the owners can access the definitions of what can be sent through the mediator?

These have been considered and separated:

1. trusted internal network
2. the internet

The mediator, as it does not support routing, oversees all communication in terms of the role as a firewall where predetermined communication is the only accepted form. According to Carlsson et al. (2017) the security function is separation – by separating the end target from the outside source, higher security can be ensured. The mediator separates the target device from both the Internet and the internal/local network. To ensure that nearby ("inside") devices that need to communicate with each other can, NFC is used for short-range communication. This to ensure that remote access is not possible without the usage of secure VPN access.

- If the mediator is maliciously accessed, how is it ensured to not be altered so as to access the devices it separates the external network from? If an outside actor can reach the mediator, but not further, could malicious code inserted be spread to devices given that the actor would know how he mediator communicates with the devices?

The transport layer security relies upon Public Key Infrastructure, meaning a trusted part signs keys to ensure their identity. Certificates are to be revoked in case someone unauthorized gains access.

5.2 Summary of Arrowhead Framework: Engineering of IoT automation systems

This chapter goes further into detail than the overview security chapter about how security measures have been taken as well as how risks have been taken into consideration for the Arrowhead Framework.

Carlsson et al. (2017) explains how information security threats, specifically cybersecurity threats, could cause problems for the safety of the automation system. They mean that security has not been a big consideration before in the history of the field. Safety and security is grouped up here since the systems the framework is made for are to operate very closely to people. The approach they have taken when overlooking the security of the framework has been to first identify assets that are of interest to the ones operating the system. Secondly, they have identified threats and vulnerabilities and lastly, they have ranked these threats and vulnerabilities through risk assessment. According to Carlsson et al. (2017) the security analysis has to be performed during the development stages, in parallel to them, so that security can be implemented at all levels. This has all been done using the ISO 27005 standard. Additionally, the STRIDE method, from Microsoft, as well as interviewing experts, has been used to identify threats that could potentially harm the security of the system. The DREAD methodology has been used in addition to STRIDE, to decide what possible impact a threat could have. Threats are scaled on how much an attack would affect, e.g. a single node or more than that. They are also scaled on how easily detected they are.

Confidentiality, integrity, availability, authentication, authorization and nonrepudiation are objectives that have been considered for security. This is according to the standard of CIA and AAA, but instead of accounting they have used nonrepudiation, which is similar in that an action cannot be hidden since it will be linked to a unique user and therefore each action will be answered for. Accounting is otherwise implemented to log actions made by all users to ensure that actions can be tracked in case of an anomaly. Attacks are categorized into four different types, Interception, Manipulation, Repudiation and Denial of service (Carlsson et al., 2017). Interception meaning that an attack could have the aim to just listen to communication, and manipulation meaning an attack could have the aim to alter or delete information. By repudiation they mean someone who denies participation in a communication and by Denial of service they mean someone stopping the availability of information. FMEA (Failure Mode Effect Analysis) and FMECA (Failure Mode Effect, and Criticality Analysis) has been applied to find potential failures.

5.3 Risk comparison, applied suggestions and knowledge gaps

The Arrowhead Framework has put a great deal of work into security and creating an internal network that is separated from external communications without meeting certain criteria.

> "Autonomous vehicles or smart assets requiring localisation within mines each hosts an Arrowhead Framework local cloud. Operating the autonomous local cloud in this way allows the asset to run as many local services as required, without connectivity to the Internet and head office. When connectivity has been reestablished, the local cloud is accessible through global service discovery. Head office systems or other authorised stakeholders such as maintenance or accounting systems are able to query for relevant information above and beyond current location." (Delsing, 2017, p. 350.).

As shown in the quote from Delsing (2017) above, the local cloud and its functionality is explained. The internal network and the internet, completely separated by using no routing capabilities on the mediator – requiring complete input validation. Though unauthorized users may not be able to enter the internal network remotely, the information that will pass through the mediator for Internet access will be subject to external threats.

- Will the internal network be penetrable if the vehicle is accessed, or if a user connects, for example, a USB device that contains malicious code?

These are threats that today are used to gain internal access to companies, by placing out USB storages nearby entrances or parking. Out of good will or curiosity, people may then try to access the USB through their PC, effectively injecting malicious code to the internal network.

- How does Arrowhead protect the system from these types of attacks?

The Arrowhead framework security chapter discusses the consideration of several models when creating a high security application system design. Security experts and frameworks for continuous threat profiles being added builds good possibilities for keeping the communication secure on a high level. Using the GBM (Genre Based Method) one can however notice the lack of mention of human factors and the possibility of people using smart devices to gain access to

the cyber-physical systems in question – in this case automotive ones. To add another perspective to security, the genre based methodology considers all information flows with its genres and producers and users of information. By viewing the implemented security by Arrowhead through the GBM glasses, I would like to add how information and policies regarding the usage of devices and controls of the automotive systems can ensure further security. It is positive that the framework has considered that new threats are discovered every day, and with their implementation of accessing vulnerability catalogues that are continuously updated, they cover many threats that have yet to be explored. However, many threats come from internal usage, and therefore logging is something that should be applied to mediators and any passage for information to ensure that user activity is saved for future use, in case of an incident, which has been implemented with the Historian. Has the internal network been considered for possible attacks from the inside, such as privilege escalation in modification rights etc.? Because of the sensitivity of the information stored, used and transferred, there is always the off-chance for someone to become motivated through financial gains or other reasons one could misuse their position to give away, destroy or modify information.

5.4 Findings

Table of concepts per chapter										
Article	***AV***	***Safety***	***IoT***	***Attacks/ threats***	***(Information) Security***	***Risk(s) related to ← + managing them***	***Mitigation***	***Suggestion***	***Connectivity/communication***	***Network***
Aldrian et al. (2017)		X	X	X	X	X	X		X	X
Carlsson et al. (2017)		X	X	X	X	X	X		X	X

Table 10. Table of concepts per chapter

While both chapters bring up the same concepts, they handle them very differently. Chapter 10, Aldrian et al. (2017), is more of an overlook, describing what type of security measures have been taken in a broader perspective. Chapter 6, Carlsson et al. (2017), instead focuses on going more in to depth with what has been chosen, how it works and why.

5.5 Genre list, assets and containers

Within this subchapter, the identified genres and assets from both chapters will be presented, along with the containers corresponding with the assets.

Assets	Genres	Container
Sensors	Communicating for usage, and storing, sensor readings	Internal communication
Internal network	Communicating data and information regarding all functions of the CPS/vehicle internally between devices and software	Internal communication
Mediator	Information, data, exchange regarding the status of the CPS and its operations	Internal communication/External communication
Historian	Software for logging all events	Internal communication
Mechanical components (e.g. steering actuator etc.)	Information about steering, speed etc.	Control system
Electronic components (e.g. PLCs etc.)	Information about steering, speed etc.	Control system
Software components (e.g. local cloud etc.)	Information about steering, speed etc.	Control system

Table 11. Assets and Genres, Arrowhead Framework

The identified containers are Internal communication, External communication and Control system.

5.6 Table of suggestions

Using the previously presented overview of current information security risks (see Table 8. Summary of findings), along with aspects of the GBM, the following table contains my suggestions for additions and future considerations within the high security application system design for the Arrowhead Framework. Suggestions are based upon findings from the literature review in comparison to this framework – differences that could be of interest to the framework.

Suggestion	*Application*	*Reason*
Consider the human aspect	Ensure that inside threats can be managed and educate people who are to use the systems on security	A lot of security risks stem from people not knowing what they can and cannot do, such as inserting a found USB into the control panel
Availability	Ensure full availability of the system so that an AV can communicate with other vehicles and authorities always	Security and safety reasons – V2V and V2X communication ensures full operability of the vehicle, road conditions ahead can be known to the vehicle before it reaches there
Risk management	Accepting certain risks for full operability, connected to availability	Research suggests that certain risks regarding user privacy may have to come second-hand to safety, allowing passage to devices inside the mediator might be necessary to for example an AV

Table 12. Table of suggestions

5.7 Summary

The mediator provides the only way in for external users to access and communicate with the device(s) the mediator protects. A DoS attack would, because of the inability to route communication through the mediator (input validation and serial interface communication between mediator and the device(s)), would only stop the mediator from operating. In the scenario of the CPS being an AV, this would be potentially problematic because of the need for the AV to have continuous communication of the type V2V. Other types of communication, such as vehicle-to-grid, would also be impossible in the case of the mediator being "down". Would the mediator be enough for an AV? As in, would a local cloud be enough to store

information and data for the AV to operate. While many functions will be operable without the connection to external sources, the operability of the AV is to a large part dependent on being able to get instant information from other vehicles on the same road. Information about the weather ahead of the vehicle on its path, and information about possible road blocks and other things that can be a threat to the secure operation of the AV.

5.8 Comparing Arrowhead Framework's security to literature review findings

As opposed to the literature review findings when it comes to genres, assets and containers. No assets could be identified as human when it comes to those handling information as security was viewed purely from a cyber-security perspective, meaning only technology was reviewed in the framework's security. This could pose a problem when it comes to identifying risks that we take when humans interact with systems and devices. There is not always enough knowledge on the human's part when it comes to what is considered safe practices.

6 Discussion

Regarding the expressed gaps of knowledge when it comes to scientists within the field of studying AVs and the future possibilities of connectivity, data storage and usages and the integration of multiple systems in the AV – some knowledge gaps expressed in the literature review can be criticized. Gaps brought up in its individual chapter in the results, do not all concern those developing security measures – it could be a matter of governments and law making. Ownership and responsibility are not always clear in the world today, which is why there needs to be laws and regulations implemented to ensure that there are as few question marks as possible for these cyber-physical systems. The concerns brought up are all valid and should be part of the larger discussion about AVs information security, but it should not be up to a single entity to take all responsibility upon themselves. This is because security can never reach its full potential, it will never be 100% efficient and work in every possible scenario. Now, that is not to say that there should be a separation of duties, if you will. Security is about ensuring that every step of the way, mitigations and risk managements have been applied within the means of the responsible actor. There are cost, time and effort factors that always play their roles into decision-making of this nature.

What I am trying to convey with this is that there is no one to ultimately deem whether security measures are correct or incorrect, especially when there are many manufacturers and no global forum for everyone to reuse technology or system design that may be subject to financial fees on the creators' will. This type of transparency between manufacturers and their used models would however require some level of 'goodwill' from the owners of such information, as economy will continue to play a large role for information security and especially combined efforts to ensure high levels of it. Cyber-physical systems are under no perspective simple – they are complex and consisting of many different components, each with their own vulnerabilities and strengths.

Perhaps it is not only in the specific technologies we need to look, but in the demands for security and how standards can be updated to correspond with the risks. If scientists with their studies give governments their forecast, manufacturers could potentially be forced to work together for security measures and the sharing of vulnerabilities to ensure that large scale attacks are harder to perform. The multiple sources bringing up the CAN had a lot of criticism to give regarding its very basic security, something that is concerning but also begs the need for perhaps entirely new networks to take its place. Preferably one that manufacturers can agree upon being made a standard, just like the CAN has been.

Attacks are mostly considered to be of economical purposes, direct damage or otherwise scouring for information of predetermined targets, however there was a lack of concern expressed for terrorist attacks with the aim of simply blocking off transportation for an area with no other purpose than to cause disruption for any other reason.

In this study, the concepts security and safety were considered further away from each other than literature otherwise has expressed in the literature review. This finding was presented in results, and if more apply this way of not separating the two, we could be looking at methods in the

future that consider safety and security more closely linked and dependent in at least one direction.

6.1 Literature review discussion

The literature review approach is a rather simple one – gather articles and find what they have in common or what is often expressed. The overview shows where current efforts are being made in the field of information security for the future AVs. Most articles are from the past five years while a portion are older, but not considerably so. The articles were picked as they corresponded with the research questions and brought in to the study because of their ability to answer to these.

While not a criterion in the search for literature, suggestions, measures and management to and of the risks was something that several studies brought up in their analyses of information security. Risks were complemented by needs and their concern for what the future may hold and what needs to be done before we can consider AVs part of the not so distant future. This shows that there is a lot of good ideas out there from different directions trying to take on the problems that many express they are concerned about. It is unfortunate that security on the manufacturer's side most likely will be driven by expressed demands from governments and insurance companies rather than something that takes a priority. Of course, this highly depends on the manufacturer – and their ability to see information security issues as potential pitfalls. Which in all well-meaning they should, not only with the new directives in the European Union but also as a protection against having customers fall victim to large scale attacks, which not only would be tragic but very costly.

In the case of insurance companies and perhaps in the future sharing location history to provide proof that the car only moves in what could be considered safe locations and manners, other similar questions may arise, like: Will AVs be able to go over the local speed limit? Perhaps they will be limited to the regulations of the road and regardless of whether the owner of the vehicle is in control of it, i.e. driving it themselves, the vehicle will stop accelerating once it has reached the current speed limit. And will this be considered owner-control or simply semi-autonomy where the individual drives the vehicle but cannot leave the lane until it is safe to do so, or stop in the middle of a highway. Exactly what the user will be able to access and not is related to information security – manipulation of settings inside the AV should be very limited to the owner of the vehicle except for when it comes to comfort settings.

The expected outcome and the actual outcome of this study differed – themes that were not expected were found in the articles reviewed. I decided to include these additional findings because they made the study richer, and gave an indication that there is a need for mobilization of studies in the information security risk subject for future AVs. Perhaps it is as simple as there being a need for more frequent overviews of recent studies, to inform of what is lacking and what is covered in terms of knowledge.

6.2 Arrowhead Framework security chapters discussion

As several similarities were found between Arrowhead Framework's security and the findings of the literature review, there were certain concerns that stood out in comparison.

The human aspect of security is not brought up in the framework book, perhaps because of the focus on cyber-security rather than a holistic view. This we can see in the table listing assets – genres – containers. The container People was not brought up in the framework. For example, the mediator can store information input, but it is not specified how that information is ensured to be of a type that is non-critical. What I mean by that is that information stored in the mediator should have certain regulations, a user should not be able to save and store a file that an external and possible malicious user can view. It is also not specified how the mediator's functions can be upheld with various sources of communication between the vehicle and other vehicles, the vehicle and servers, the vehicle and the grid it travels within. If all information is to be predetermined, how can availability of the vehicle be ensured to its surroundings. Another concern is the possibility of DoS attacks on the mediator, since it is the single point of all communication to go through, how does it ensure availability to all services within the vehicle. Granted, the framework was not created with only autonomous vehicles in mind, it was created for cyber-physical systems in general. But regardless, it can benefit from the findings in this study for future purposes.

6.3 Method

The literature review method was a good choice for this study as it can be considered rather open ended in terms of what the aim is. Finding themes in articles and presenting them accordingly, instead of by author, makes for an easier read and a more thorough review. Other literature review methods were not considered since the aim for the study was to create an overview – and the way to create one is to find the concepts of several studies on the subject. By combining their findings, one can gain a view of what is most commonly expressed and what has been focused on. Since the aim however was to show what has been done in the subject of information security risks for future AVs, considered articles were focused on the future often, and speculations was a common find. But even so, when it comes to risks and knowledge gaps expressed in said literature, there were also findings that were unique to certain articles, which is why the knowledge gaps chapter listed expressed gaps with the authors mentioning them referenced to show how many brought them up.

Not only was the literature method a logical choice because of its capability of catching concepts expressed in multiple sources. It was also fitting to the future perspective of the review as it focuses on how we can learn about the future by considering the past, in this case the present past.

While several articles, and the framework, did not consider the human as a potential security risk, they did express their concern for the safety of the people inside AVs and those who can be effected by security breaches or attacks. However, few failed to recognize the full picture – or overview – which had already been concluded in the early stages of the literature review. Information security is about going past cyber security, which is what I with this literature tried

to convey. Only considering information assets that are either software or hardware, does not consider people using AVs to their benefit or maliciously gaining access/entry to a vehicle and injecting malicious code, for example.

6.4 Work process and planning

To review a project is a good way to reflect upon the positives and negatives. The work process has had its ups and downs since the aim of the study has changed with time. Planning has therefore been recreated with the new aim in mind, and certain weeks may not exactly correspond with the actual work. Something noteworthy of the time schedule is that many chapters of the report took considerably longer than planned for. A daunting process was writing the literature review itself and the discussion, at least in terms of the decided upon time it would take. They took a lot longer and demanded a lot of time, spread out over the course of the work.

7 Outcome and future research

This literature review presents an overview of the future AV's information security risks, but also suggestions and mitigations expressed within research focusing on risks. By collecting literature and summarizing where research is at today and what needs to be done, future researchers as well as people from the AV industry and the future users of these vehicles can gain knowledge. This work was written to be informative and fill an expressed need for overviews of information security risks as many had taken it upon themselves to analyse parts of the AV without putting them in to relation with each other and showing the big picture. It is important to show the connection of the risks and security of each software and hardware as well as the users of the AV – to see it from another perspective. We know that complex systems require elaborate information security thinking and planning. An attack on the availability of information systems within the AV could lead to varying degrees of danger to the user of the vehicle, the new era of vehicles being dependent on information rather than fuel – figuratively speaking – brings concerns that are yet to be responded to on many areas. By pointing out the gaps from several studies, part of the background work for future research has been completed with this report.

Future research should be based on the found knowledge gaps where research has fallen behind or is simply not present. By filling these gaps, we can gain a better understanding and a full picture of the security possibilities and limitations that comes with the future AV.

8 Acknowledgements

I would first and foremost like to thank my supervisor, Tero Päivärinta, for his input, help and critique through the process of writing my master thesis.

I would also like to thank Jan van Deventer and his team I met with at LTU and received a presentation from about the Arrowhead framework and prototype. Your help was appreciated. Jan also helped me and managed the contact with Volvo at the earlier stages of my thesis, of which I am grateful.

Lastly, I would like to thank my fellow classmates in the Information Security master program who participated in the seminars and gave me helpful input to each stage of my thesis report.

9 References

Aldrian, A., Priller, P., Schmittner, C., Plosz, S., Tauber, M., Wagner, C., Hein, D., Ebner, T., Maritsch, M., Ruprechter, T., & Lesjak, C. (2017). Application system design – High security. In Delsing, J. (Ed.) IoT Automation – Arrowhead Framework (e-book). pp. 317-329.

Amoozadeh, M., Raghuramu, A., Chuah, C., Ghosal, D., Zhang, H., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving*, IEEE Communications Magazine*, 53, 6, pp. 126-132. doi:10.1109/MCOM.2015.7120028

Bagloee, S., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: challenges, opportunities, and future implications for transportation policies', *Journal of Modern Transportation*, 24, 4, pp. 284-303. doi:10.1007/s40534-016-0117-3

Bangar, P. Y., Pacharne, S. B., Kabade, S. S., & Rajarapullo, P. R. (2016). Design and Implementation of Next Generation Smart Car. International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp 508-512. doi:10.1109/ICACDOT.2016.7877637

Bloomfield, R., Netkachova, K., & Stroud, R. (2013). Security-Informed Safety: If It's Not Secure, It's Not Safe. In Gorbenko, A., Romanovsky, A., & Kharchenko, V. (ed). Software Engineering for Resilient Systems. Vol: 8166. pp. 17-32. Spinger, Germany. doi:10.1007/978-3-642-40894-6_2

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute, Carniege Mellon University.

Carlsson, O., Vera, D., Arceredillo, E., Tauber, M. G., Ahmad, B., Schmittner, C., Plosz, S., Ruprechter, T., Aldrian, A., & Delsing, J. (2017). Engineering of IoT automation systems. In Delsing, J. (Ed.) IoT Automation - Arrowhead Framework (e-book). pp. 161-207.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czekis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *Proceedings of USENIX Security 2011.*

Dakroub, H., Shaout, A., & Awajan, A. (2016). Connected Car Architecture and Virtualization, *SAE International Journal Of Passenger Cars: Electronic & Electrical Systems*, 9, 1, pp. 153-159, Academic Search Index. doi:10.4271/2016-01-0081

De-J, J., Santos, L., & Tudon-Martinez, J. C. (2017). Towards a Supermileage Autonomous Vehicle, *SAE Technical Paper*, doi:10.4271/2017-01-0114.

Decugis, S. (2009). Towards a Global AAA Framework for Internet. *Ninth Annual International Symposium on Applications and the Internet, Applications and the Internet*. doi:10.1109/SAINT.2009.57

Delsing, J. IoT Automation – Arrowhead Framework (e-book).

Edwards, J., & Kashani, A. (2017). Identifying Security Vulnerabilities Early in the ECU Software Development Lifecycle, *SAE Technical Paper*. doi:10.4271/2017-01-1657

Fagnant, D., & Kockelman, K. (2015). Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations, *Transportation Research Part A*, 77, pp. 167-181. doi:10.1016/j.tra.2015.04.003

Hoppe, T., Kiltz, S., & Dittman, J. (2011). Security threats to automotive CAN networks – Practical examples and selected short-term countermeasures. *Reliability Engineering and System Safety*, vol. 96, pp 11-25. doi:

Ilvonen, I., Jussila, J., Kärkkäinen, H., & Päivärinta, T. (2015). Knowledge security risk management in contemporary companies – toward a proactive approach, *48th Hawaii International Conference on System Sciences*. pp 3941-3950. doi:10.1109/HICSS.2015.472

Kang, M., & Kang, J. (2016). Intrustion Detection System Using Deep Neutral Network for In-Vehicle Network Security. Plos ONE, vol: 11, issue: 6, pp 1-17. doi:10.1371/journal.pone.0155781

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., & Savage, S. (2010). Experimental Security Analysis of a Moden Automobile. 2010 Symposium on Security and Privacy. doi:10.1109/SP.2010.34

Lasi, H., Fettke, P., Kemper, H-G., Feld, T., & Hoffman M. (2014). *Industry 4.0. Business & Information Systems Engineering*. Vol: 6, issue: 4. pp. 239-242. doi:10.1007/s12599-014-0334-4

Lee, J., Ardakani, H. D., Yang, S., & Bagheri, B. (2015). Industrial Big Data Analytics and Cyber-Physical Systems for Future Maintenance & Service Innovation. *Procedia CIRP, 38 (Proceedings of the 4th International Conference on Through-life Engineering Services),* pp 3-7. doi:10.16/j.procir.2015.08.026

Li, H., Ma, D., Medjahed, B., Wang, Q., Kim, Y. S., & Mitra, P. (2017). Secure and Privacy-Preserving Data Collection Mechanisms for Connected Vehicles, *SAE Technical Paper*. doi:10.4271/2017-01-1660

Macher, G., Messnarz, R., Armengaud, E., Riel, A., Brenner, E., & Kreiner, C. (2017). Integrated Safety and Security Development in the Automotive Domain*, SAE Technical Paper*. doi:10.4271/2017-01-1661

Mascareñas, D., Stull, C., & Farrar, C. (2017). Autonomous execution of the Precision Immobilization Technique, *Mechanical Systems And Signal Processing*, 87, Part B, pp. 153-168. doi:10.1016/j.ymssp.2016.06.043

Natale, M. D. (2012). *Understanding and Using the Controller Area Network Communication Protocol*. Springer, United States of America.

Neumann, P. G. (2016). Risks of Automation: A Cautionary Total-System Perspective of Our Cyberfuture, *Communications of the ACM*, 59, 10, pp. 26-30. doi:10.1145/2988445

Niklas, M., & Rathgeber, S. (2016). AUTOSAR – A standard in the course of time. EUROFORUM *Automotive Software Development, Munich*.

Paar, C., Rupp, A., Schramm, K., Weimerskirch, A., & Wolf, M. (2010). Implementing Data Security and Privacy in Next-Generation Electric Vehicle Systems. *SAE Technical Paper*. doi:10.4271/2010-01-0743

Padyab, A.M., Päivärinta, T., & Harnesk, D. (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management*, vol: 10, issue: 2. pp. 13-28. doi:10.4018/ijkm.2014040102

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems, vol: pp, issue: 99. doi:10.1109/TITS.2017.2665968

Pesé, M. D., Schmidt, K., & Zweck, H. (2017). Hardware/Software Co-Design of an Automotive Embedded Firewall, *SAE Technical Paper*. doi:10.4261/2017-01-1659

Petit, J., & Shladover, S. (2015). Potential Cyberattacks on Automated Vehicles, *IEEE Transactions On Intelligent Transportation Systems*, 16, 2, pp. 546-566. doi:10.1109/TITS.2014.2342271

Prowse, D. L. (2015). *CompTIA Security+ SY0-401 Cert Guide*. 3rd edition. Pearson Education, United States of America.

Päivärinta, T., Halttunen, V., & Tyrväinen, P. (2000). A genre-based method for information systems planning. *Information Modeling in the New Millenium*, pp 70-93. doi: 10.4018/978-1-878289-77-3.ch005

Schneider, R., Kohn, A., Klimke, M., & Dannebaum, U. (2017). Cyber Security in the Automative Domain – An Overview, *SAE Technical Paper*. doi: 10.4271/2017-01-1652

Shields, J. B., Huser, J., & Gell, D. (2017). Autonomous Key Management (AKM) Security Architecture for Vehicle and IoT Applications, *SAE Technical Paper*. doi:10.4271/2017-01-1653

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal*, vol: 30, issue: 3, pp 30-35. doi:10.1016/j.tej.2017.02.006

Thing, V. L. L., & Wu, J. (2016). 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), doi:10.11.09/iThings-GreenCom-CPSCom-SmartData.2016.52

Vogel-Heuser, B., & Hess, D. (2016). Guest Editorial Industry 4.0–Prerequisites and Visions, *IEEE Transactions On Automation Science & Engineering*, 13, 2, pp. 411-413. doi:10.1109/TASE.2016.2523639

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, vol. 26, no. 2, pp. xiii-xxiii

Wooderson, P., & Ward, D. (2017). Cybersecurity Testing and Validation, *SAE Technical Paper*. doi:10.4271/2017-01-1655

Yagdereli, E., Gemci, C., & Aktas, A. (2015). A study on cyber-security of autonomous and unmanned vehicles, *Journal Of Defense Modeling & Simulation*, 12, 4, pp. 369-381. doi:10.1177/1548512915575803

Zaidi, K., & Rajarajan, M. (2015). Vehicular Internet: Security & Privacy Challenges and Opportunities. *Future Internet*, 7(3), pp 257-275. doi:10.3390/fi7030257

Zheng, K., Zheng, Q., Yang, H., Zhao, L., Hou, L., & Chatzimisios, P. (2015). Reliable and efficient autonomous driving: the need for heterogeneous vehicular networks. IEEE Communications Magazine, vol: 53, issue: 12. doi:10.1109/MCOM.2015.7355569

Zou, Q., Chan, W., Gui, K., Chen, Q., Scheibert, K., Heidt, L., & Seow, E. (2017). The Study of Secure CAN Communication for Automotive Applications, *SAE Technical Paper.* doi:10.4271/2017-01-1658