University of Twente

Master Thesis

Information Security Risks for Car Manufacturers based on the In-Vehicle Network

By:

Chris Blommendaal (s0177482)

c.blommendaal@student.utwente.nl

Deloitte:

Anouk Jessurun Msc RE

University of Twente:

Dr. Maya Daneva

Prof. dr. Jos van Hillegersberg

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science

at the

Faculty of Electrical Engineering, Mathematics and Computer Science

Deloitte.

UNIVERSITY OF TWENTE.

September 2015

Abstract

A new development within the Internet of Things is the development of connected cars. By incorporating a large amount of micro controllers and sensors in their products, modern vehicles are able to assist drivers in various ways. Over time these connected cars will become completely autonomous, it is expected that the first autonomous car will be on the road within 10 years. However, little attention is paid to security and privacy issues.

In order for these sensors and micro controllers to communicate with each other, a variety of networks is used within vehicles. This to reduce cabling costs, and to provide an easy manner to add new nodes to the network. However, these networks are not designed for the usage within cars, which poses risks. Thereby, adding external connectivity (for instance Wi-Fi, cellular, Bluetooth) to these networks poses threats to the information security within cars as well.

Within this thesis we investigate what information security risks result from the used in-vehicle network architecture. By combining scientific and empirical data an architectural model is constructed in ArchiMate$^{\text{TM}}$. Using this model we categorize vulnerabilities and identify the group that poses the biggest threat to the informations security within cars.

We find that most information security risks are due to the protocols used within cars and the interconnectedness of the various vehicular networks. In order to overcome these risk we suggest the development of new networking protocols that are secure by design. Furthermore, car manufacturers should prepare themselves better for potential crisis situations.

Acknowledgments

This thesis not only marks the end of my study but also the end of my life as a student at the University of Twente. Prior to my thesis I would like to take a moment to reflect on this period and thank some people.

Starting my student life at the age of 17, I was young and pretty naive. Always being a tech savvy kid resulted in me wanting to study ‘something’ with IT. I am happy that I stumbled upon the Business & IT program in Enschede. A study that integrates IT with industrial engineering and economics turned out to be great choice for me. I developed a great set of analytical skills and critical judgment over the years.

Next to being a student at the university I can reflect on an amazing period in my life in which I developed myself in numerous ways. Therefore, I would like to thank everyone that made my student life in Enschede a great success. And of course a big thanks to my parents who have given me the opportunity to study and having faith in me, even in moments when results were lacking.

Furthermore, I would like to thank Dave for having trust in me and giving me the opportunity to write my thesis at Deloitte. Besides, I appreciated the support Anouk provided to me and would like to thank her for introducing me to numerous people within Deloitte. They were all able to provide valuable feedback for my thesis.

Last but not least I would think Maya and Jos. Without your support it would not have been possible to write this thesis. During times I had troubles, you always gave me suggestions to push me in the right direction.

Regards,

Chris

Contents

List of Figures

List of Tables

Abbreviations

ABS	**A**nti-lock **B**raking **S**ystem
ADAS	**A**dvanced **D**river **A**ssistance **S**ystems
AI	**A**rtificial **I**ntelligence
CAN	**C**ontroller **A**rea **N**etwork
CPS	**C**yber **P**hsyical **S**ystem
CPA	**C**yber & **P**rivacy **A**dvisory
DbW	**D**rive-**b**y-**W**ire
DSRC	**D**edicated **S**hort **R**ange **C**ommunications
ECU	**E**lectronic **C**ontroller **U**nit
ESP	**E**lectronic **S**tability **P**rogram
ETC	**E**lectronic **T**hrottle **C**ontrol
FOTA	**F**irmware update **O**ver **T**he **A**ir
InfoSec	**Info**rmation **Sec**urity
IoT	**I**nternet **o**f **T**hings
ISSRM	**I**nformation **S**ystem **S**ecurity **R**isk **F**ramework
LIN	**L**ocal **I**nterconnect **N**etwork
MOST	**M**edia **O**riented **S**ystem **T**ransport
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
OBD	**O**n **B**oard **D**iagnostics
TCU	**T**ransmission **C**ontrol **U**nit
V2I	**V**ehicle to **I**nfrastructure
V2V	**V**ehicle to **V**ehicle
VANET	**V**ehicular **A**d hoc **Ne**twork

Chapter 1

Introduction

The digitalization of society continues. The amount of devices connected to the Internet reached the 15 billion mark and is expected to hit 50 billion by 2020 (Gartner, 2015). This immense growth of the Internet in terms of size and interconnectedness (referred to as the *Internet of Things (IoT)*) poses a vast range of opportunities as well as threats to individuals and society.

A recent development within this *Internet of Things* is the emergence of Connected Cars. These vehicles are equipped with many sensors to measure their surroundings as well as *Dedicated Short Range Communication equipment (DSRC)* that is used to share this information with surrounding vehicles. This in order to increase safety, improve traffic flow and reduce pollution. So far the development of these services is feature driven and little attention is paid to security and privacy (Telefonica, 2015).

While the first cars operated solely by the use of mechanics and hydraulics, modern cars are computers on wheels. Figure 1 shows how the amount of code inside a modern vehicle relates to other technological achievements. This relatively high amount of code is due to the hardware structure used in Connected Cars. Nearly every functionality within a car (for instance: wipers, claxon, brakes, park assist) has its own *Electronic Control Unit (ECU)* running on its dedicated embedded controller with its own software. As one can imagine, having such a large base of software inside a car increases the chance of bugs and implementation faults.

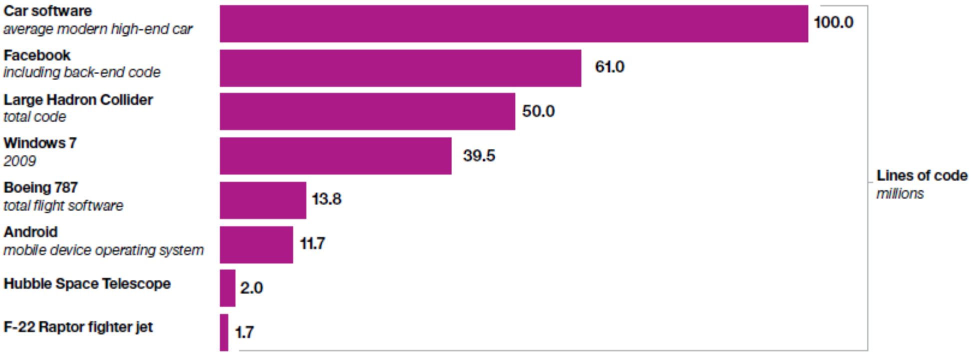


FIGURE 1: Source lines of code in vehicles. Image from (IBM, 2014).

Recently, researchers have shown that it is possible to hack vehicles, even remotely, and then control a variety of car actuators (Wired, 2015). This poses potential risks, especially since the development of Connected Cars has just started and little information is available regarding possible risks. Studies predict that the amount of Connected Cars on the road will increase vastly over the upcoming years. Predictions range from 150 million to 250 million Connected Cars by 2020 (Forbes, 2015, Gartner, 2015, GSM Association, 2013).

1.1 Research setting

This research is facilitated by Deloitte as a part of my graduation internship within the master Business Information Technology at the University of Twente. My internship took place at the Deloitte Risk Advisory department in Amsterdam. This department is a pillar within Deloitte Netherlands which itself is part of the worldwide Deloitte network as depicted in Figure 2. Risk Advisory has been advising clients on financial and reputation risks over the last 25 years. After the millennium Risk Advisory engaged in cyber advisory services labeled as *Cyber Risk Services*.

During my internship I was part of the *Cyber & Privacy Advisory (CPA)* team within Cyber Risk Services. This team serves Small and Medium Enterprises (SMEs) and multinationals on topics such as crisis management, digital strategy and security and privacy transformation programs. Within this team the attention for Connected Cars is rising, since the amount of privacy concerns is rising and the media frequently reports on flaws in car security. Furthermore, other teams within Cyber Risk Services such as Cyber Operations, which focuses on hacking, are also interested in the topic of automotive security.

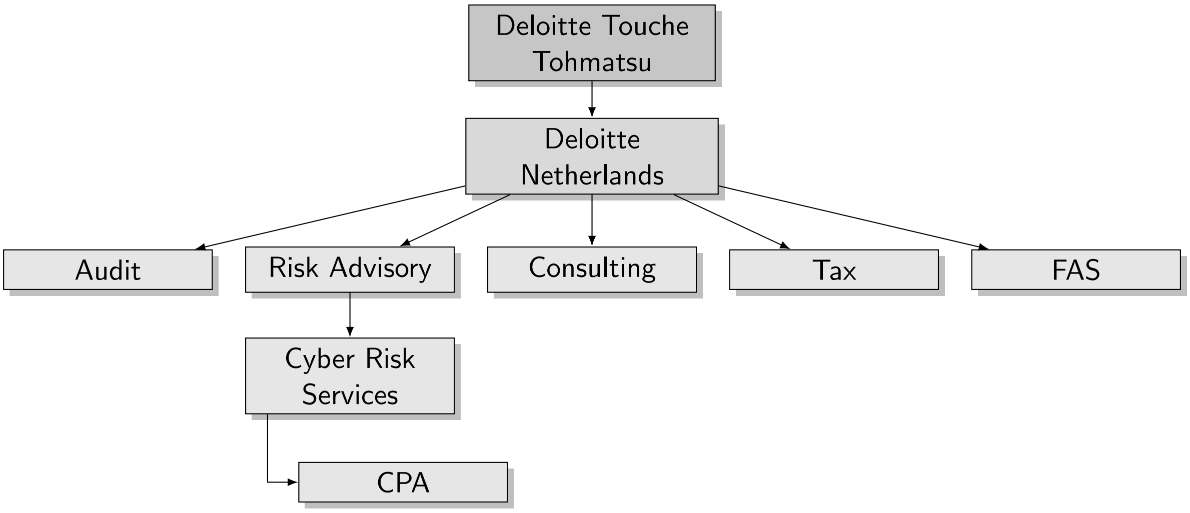


Figure 2: Cyber & Privacy Advisory within the Deloitte network.

1.2 Motivation

Deloitte aims to be "*the most innovative professional service supplier*" and is therefore continuously bringing new value propositions to the market (Deloitte, 2014). This is based on market demands but is also driven by internal innovation. One of the focus areas for innovation is the Connected Car field, because a variety of parties is involved in this field. Projects range from legal, regulatory & compliance to cyber security, logistics and information security.

In order to focus this innovation effort on the most critical parts within the Connected Car business, this project aims to identify the biggest risks to information security for car manufacturers. Deloitte already offers a wide ranging of cyber services to various clients, within this thesis we aim to identify opportunities to offer cyber services to clients within the automotive sector. Producing a comprehensive overview of risks and prioritizing them is expected to help to identify new business opportunities. This helps Deloitte in keeping its innovative character.

Within this study we use ArchiMate$^{\mathrm{TM}}$ to model the in-vehicle network structure and to model risks. We have chosen to use ArchiMate$^{\mathrm{TM}}$ because it is an established modeling tool (Jonkers et al., 2011). Furthermore, it is also used within Deloitte for various modeling purposes.

For the scientific community this study is relevant since it systematically investigates the risks in the Connected Car domain and searches for mitigation strategies for these risks. Mapping these vulnerabilities and risks onto an ArchiMate$^{\mathrm{TM}}$ model should yield a clear overview of the various vulnerabilities and risks.

Due to the rapid growth of Connected Cars a structured analysis of potential security risks is beneficial. AT&T announced that nearly 700 thousand new connected cars were added to its US network in the first quarter of 2015 (Dignan, 2015). This shows that the field of Connected Cars is expanding rapidly and should therefore receive attention from the scientific community.

Connected Cars are the predecessor of autonomous vehicles and should therefore be evaluated thoroughly while there are still humans in it who are paying attention to their surroundings (Orlikowski and Iacono, 2001). Although autonomous vehicles are not yet available for the consumer market, they are expected to become available within the next ten years. This gives this study social relevance as well.

1.3 Problem Statement

The increasing digitalization of society has opened up lots of opportunities; within the Internet of Things a multitude of devices is now able to communicate with each other in order to make life easier. This digitalization on a massive scale also has its adverse impacts. Recently smart objects such as *fridges* and *cars* have been hacked (Hacking et al., Wired, 2015) which resulted in data loss and dangerous situations on the road.

This persistent cyber security threat combined with the lingering issues on privacy and data protection puts pressure on newly developed products such as cars. Based on our exploratory literature study we observe that:

- A larger part of the vulnerabilities and risks result from the in vehicle network architecture.
- Vulnerabilities are treated on a individual basis and are not linked to the bigger picture.
- It is unclear how car manufacturers can mitigate the risks that are currently present.

Therefore, we aim to investigate what information security risks are present within Connected Cars. By examining vulnerabilities inside vehicular networks we will come up with risks for automotive manufacturers.

Based on the above the following problem statement has been proposed:

What are the key information security risks for car manufacturers resulting from the in-vehicle network architecture?

This should result in a comprehensive list of information security risks linked to risk mitigation strategies. Based on this we can recommend both the automotive sector and Deloitte, which sponsors this study.

1.4 Scope

This study focuses on the in-car network architecture and its vulnerabilities. Based on the vulnerabilities we identify corresponding risks for car manufacturers. The results of this study can be used by Deloitte to develop new business propositions in promising areas as the Connected Car field is moving fast and is gaining a lot of attention in the media these days (Kaspersky, 2015, Markey, 2015, Wired, 2015).

1.5 Objectives

The main objective of this study is to identify information security risks tailored to the Connected Car domain and result from the in-car network architecture. By conducting a systematic literature review in order to provide insight in the Connected Car domain that can be used by Deloitte to further develop services for the automotive industry.

Therefore the main objective (**MO**) of this study is:

To map and asses information security risks within Connected Cars in order to make recommendations for risk mitigation and business development.

In order to fulfill the main objective of the study the following sub-objectives are defined. With our first objective we aim to get insight into the in-vehicle network architecture. Secondly, we use ArchiMate^{TM} in order to model this architecture and map the identified information security risks. Thirdly, we want to find risk mitigation strategies for the identified information security risks. Our fourth objective is to measure to what extend ArchiMate^{TM} is feasible for modeling information security risks. Lastly, we investigate what areas are suitable for business development for Deloitte.

This yields the following sub-objectives:

SO1. Getting an overview of the architecture within a Connected Car.

SO2. Identifying the largest information security risks and map those onto the in-vehicle architecture using ArchiMate.^{TM}

SO3. Identifying risk mitigation strategies for the identified information security risks.

SO4. Measuring to what extent ArchiMate^{TM} is feasible for risk modeling.

SO5. Identifying promising areas for Deloitte for the development of new business propositions.

This last objective is due to the fact that within Deloitte Cyber Risk Services, Connected Cars get more and more attention. However, this subject is very broad and for Deloitte it is not clear yet on which areas to focus. Therefore, we aim to systematically review vulnerabilities and risks within Connected Cars and to come up with recommendations for Deloitte in terms of potential business development areas.

1.6 Research questions

Within this study we focus on translating architectural vulnerabilities to information security risks and linking those to risk mitigation strategies for car manufacturers. Thereby, we develop an architectural model by using ArchiMate^{TM} in order to be able to map vulnerabilities and risks onto this model. This aids in tracing risks to hardware components. Based on our problem statement in Section 1.3 we construct the following main research question:

> *What are the key information security risks within connected cars deriving from the in-vehicle network architecture and how can they be mitigated?*

In order to assess the information security within connected cars we first need to study the architecture of Connected Cars. Therefore, our first research question is focused on the architecture itself. We model this architecture using ArchiMate^{TM} which is later used for mapping purposes. Mapping these risks helps to identify business development opportunities in **RQ6**.

RQ. 1 What does the architecture of Connected Cars look like?

Based on the architecture studied in our first research question we investigate what vulnerabilities the scientific community has identified resulting from this network structure. Thereby, we construct an architectural model which is used for risk and vulnerability purposes.

RQ. 2 What architecture related information security risks are identified by the scientific community?

Furthermore, we engage in empirical research to validate the results of the previous research question and to identify any missing information security risks and/or mitigation strategies.

RQ. 3 What architecture related information security risks are identified by practitioners in the field of automotive security?

Based on our architectural model from **RQ1** and the risks identified in research questions **RQ2** and **RQ3**, we evaluate the use of ArchiMate^{TM} for risk modeling purposes.

RQ. 4 What is the benefit of using ArchiMate^{TM} with its extension to model information security risks?

Using the risks identified by the scientific community and the risks from subject matter experts we aim to identify mitigative strategies for car manufacturers.

RQ. 5 How can these risks be mitigated?

Based on the mapping and risk overview we identify business development possibilities for Deloitte.

RQ. 6 Which areas are suitable for business development purposes for Deloitte?

Table 1 shows how the various research questions above map onto the objectives identified in Section 1.5.

Table 1: Mapping of research questions onto objectives.

	SO1.	**SO2.**	**SO3.**	**SO4.**	**SO5.**
RQ. 1	✓				
RQ. 2		✓			
RQ. 3		✓			
RQ. 4	✓			✓	
RQ. 5			✓		
RQ. 6					✓

Based on these research questions we can answer our main research question and reach the objectives stated in Section 1.5.

1.7 Structure and reading guide

The structure of this thesis is as follows. First Chapter 2 will elaborate on the research method used, how the articles used were selected and how our focus group was structured. Subsequently Chapter 3 will explain in detail what Connected Cars are and how they function internally.

Chapter 4 elaborates on risk and contains the main results of our study. Chapter 5 discusses the mapping of risks onto our ArchiMate^{TM} model and implications for practice. Finally Chapter 6 ends this thesis with conclusions and recommendations. Figure 3 depicts how the *empirical*, *theoretical* and *research design* elements of this study interact.

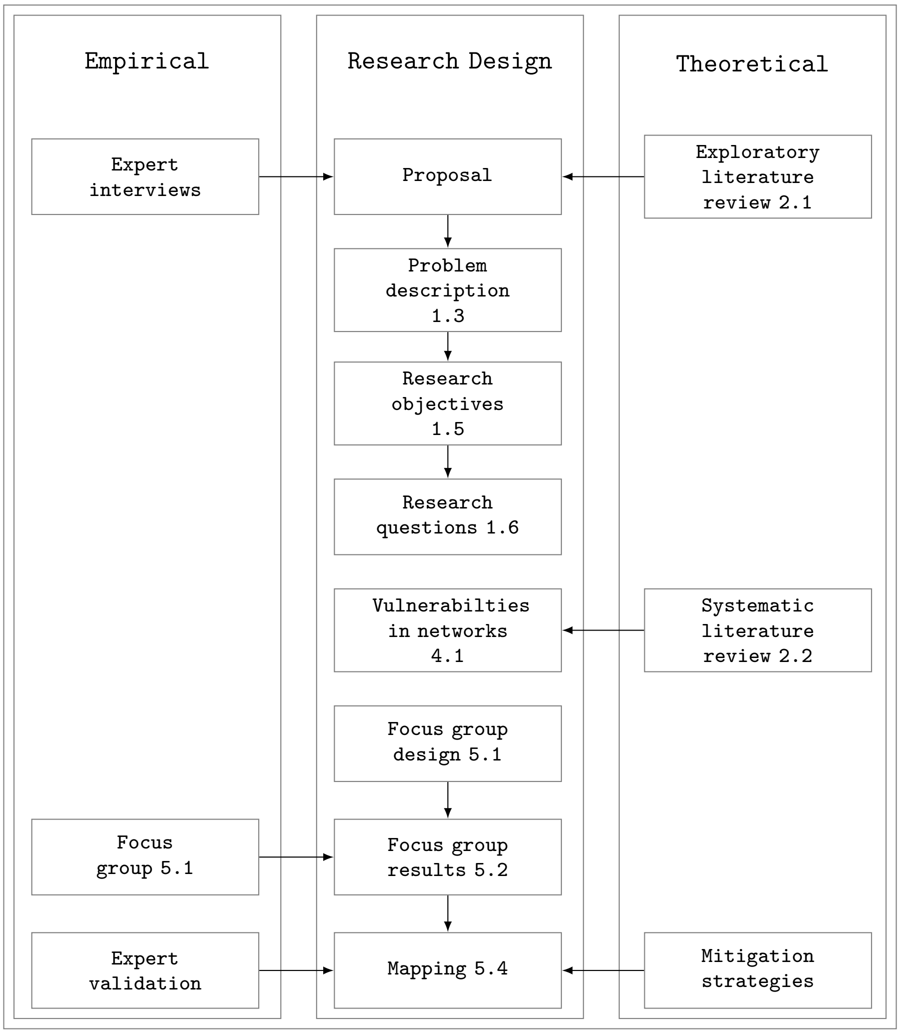


FIGURE 3: Overview of research design

Chapter 2

Research Methodology

According to the Merriam-Webster dictionary, a methodology is:"*a set of methods, rules, or ideas that are important in a science or art: a particular procedure or set of procedures*". Explicitly choosing a research methodology helps to guide and structure the research. Thereby, in order to conduct an effective research we need to scope the area where our research takes place. Verschuren and Doorewaard argue that within designing a study it is important to determine focus and scope. In order to do so we first conduct an exploratory literature review in Section 2.1 as advised by Verschuren and Doorewaard (Verschuren and Doorewaard, 2000).

Within this thesis a variety of research methods is used to collect data, this in order to overcome biases or narrow views of a single method. According to Creswell, this approach encourages the use of multiple worldviews or paradigms (Creswell, 1999). By first conducting an exploratory literature review and consulting subject matter experts, a preliminary view of the current state of the art was formed. Afterwards we engage in a systematic literature review in order to get a detailed overview of the information security risks within vehicular networking.

Based on the results from our systematic literature review we conduct a focus group in order to see if practitioners recognize the concepts identified by the scientific community. This focus group is useful both to validate our results, and to complement them if necessary.

2.1 Exploratory literature review

An exploratory literature review will be conducted to see where research is currently at. By using sources *Scopus* and *Google Scholar* we found several articles using the keywords: "*connected car*", "*autonomous car*", "*autonomous driving*" and "*smart car*". The goal of this exploratory literature review is to assess the current state of art within automotive security. Based on this exploratory literature review we conclude that:

- A larger part of the vulnerabilities and risks result from the in vehicle network architecture.
- Vulnerabilities are treated on a individual basis and are not linked to the bigger picture.
- It is unclear how car manufacturers can mitigate the risks that are currently present.

2.2 Systematic literature review

In order to get a proper understanding of the current state of literature we choose to engage in a systematic literature review. According to Kitchenham: "*A systematic literature review is a means of evaluating and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest. Systematic reviews aim to present a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology.*" (Kitchenham, 2007). Reviewing the available literature using an unbiased approach "*optimizes the chances for noting and pointing out aspects of the phenomenon under study in need of more data*" (Wolfswinkel et al., 2013). For our systematic literature review we choose the 5 step model as introduced by Wolfswinkel. We have chosen this model because it is based on Grounded Theory and is highly applicable within IS research (Webster and Watson, 2002, Wolfswinkel et al., 2013). The five steps in this model are: define, search, select, analyze and present as shown in Table 2.

Table 2: Five-stage literature review model by Wolfswinkel et al. 2013

1. Define
    1.1. Define the criteria for inclusion exclusion
    1.2. Identify the fields of research
    1.3. Define the appropriate sources
    1.4. Decide on the specific search terms
2. Search
    2.1. Search
3. Select
    3.1. Refine the sample
4. Analyze
    4.1. Open coding
    4.2. Axial coding
    4.3. Selective coding
5. Present
    5.1. Represent and structure the content
    5.2. Structure the article

2.2.1 Define

As outlined by Wolfswinkels approach we should first identify the criteria for inclusion and exclusion. Criteria for inclusion and exclusion are shown in Table 3 and Table 4, respectively. We select articles based on the criteria for inclusion and filter them on the stated exclusion criteria afterwards. Furthermore, we investigate neighboring disciplines such as the *Internet of Things (IoT)* and *mobile security*. These closely related areas might introduce new vulnerabilities.

Table 3: Overview of inclusion criteria

	Inclusion criteria	**Reason**
IC1	The article is regarding information security in connected cars	We want to investigate how information security within connected cars is addressed
IC2	The article is regarding information security in mobile or the Internet of Things	Neighboring application areas can help to identify risks

Table 4: Overview of exclusion criteria

	Exclusion criteria	**Reason**
EC1	The article is not in English	We only use articles written in English in this study
EC2	The article is not available to us	If articles are not available to us they cannot be incorporated in this study.

2.2.2 Search

Within our systematic literature review we used the search terms "*smart car*", "*connected car*" and "*autonomous vehicle*", since our exploratory literature review showed that these terms were frequently used within the scientific community. We started our search on the topic of connected cars but expanded it since the number of results was fairly low. This was to be expected on such a recent topic.

We used *Scopus* as main search provider. Furthermore *Google Scholar* was consulted to gain access to articles whenever possible. The exact search queries used can be found in Appendix A.

2.2.3 Select

Based on the previously mentioned inclusion and exclusion criteria articles are selected. Most of the in- and exclusion criteria are enforced automatically by search engines whilst some were handled manually. Furthermore, we add one additional article to the corpus that was frequently cited by other articles found but did not come up using our search terms.

Figure 4 depicts how the corpus of articles was constructed. Due to the lack of high quality scientific publications found on the topic we extended our search towards the references of the articles found and high quality publications from neighboring disciplines. This results in a total of *12 articles* used in the study. These articles are to be found in Appendix B.

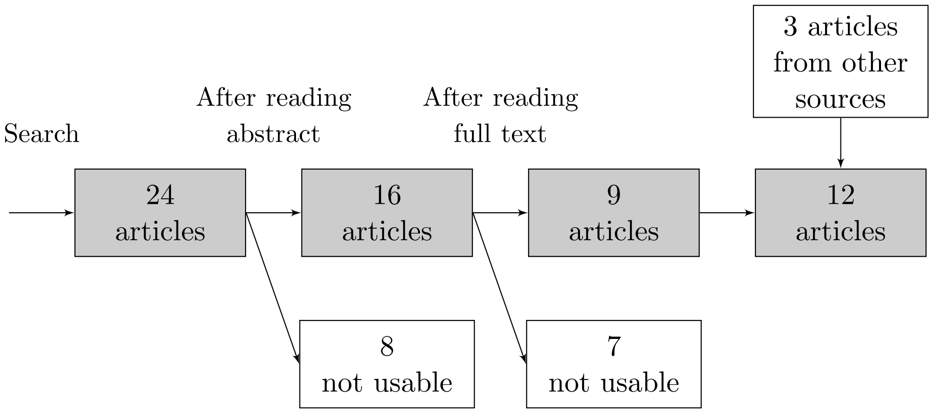


Figure 4: Graphical representation of article selection.

2.2.4 Analyze

By using open coding we translated relevant excerpts from the corpus of articles to concept in our structured literature review. According to Wolfswinkel et al., open coding means that "*researchers engage in conceptualizing and articulating the often hidden aspects of a set of excerpts that they noted earlier as relevant during their close reading of a set of single studies. This way each set of excerpts is incorporated into a set of concepts and insights.*" (Wolfswinkel et al., 2013).

2.2.5 Present

By using a traceability matrix, vulnerabilities found in the reviewed papers are shown. This matrix can be found in Section 4.1 on page 38. Based on the concepts found in the literature we propose a grouping method which is used throughout the remainder of this thesis. In order to validate our results and identify any missing vulnerabilities we conducted a focus group with subject matter experts. Details regarding the conducted focus group are discussed in Section 5.1 on page 49.

2.3 Relevance

Wieringa defines relevance as the "*suitability of an artifact or of knowledge to help achieving a goal*" (Wieringa, 2010). These goals can be of economical or theoretical nature. Within this section we distinguish between scientific, social and practical relevance of this thesis.

2.3.1 Scientific relevance

This study is relevant for the scientific community since it combines the vulnerabilities identified by several studies and maps them onto the in-vehicle network architecture. Using the vulnerabilities identified by literature we translate those towards risks for car manufacturers. Subsequently, risk mitigation strategies are discussed.

2.3.2 Social relevance

Finally this study is socially relevant since the number of connected cars is growing rapidly. It is expected that by 2020 a quarter billion cars will have automated driving capabilities (Gartner, 2015). Furthermore, we are currently in a transitioning phase, humans are still driving the cars but are assisted by a variety of sensors and systems. This development will continue over the next few years until the moment that cars are truly self-driving. In this situation it is important that there is full trust in the technology used. Therefore, attention should be paid to risks involving car hardware and software.

2.3.3 Practical relevance

In terms of practical relevance this study makes recommendations to both the automotive sector as well as Deloitte. It addresses dangerous situations that may arise due to the currently used networking structure. Furthermore, we advise Deloitte on which parts of the in-vehicle network account for for the largest amount of risks. These areas might be suitable for business development since demand will grow over the coming years.

As currently vehicles are only *connected* and not yet *autonomous*, currently, there is always ia driver behind the steering wheel. In case an unsafe event occurs, the driver is still able to intervene. However, over the next few years this will change (Gartner, 2015). In order to keep automotive transportation safe, risks regarding self-driving capacities should be addressed.

The practical relevance of this research can be summarized as follows:

- Systematically investigates the vulnerabilities within Connected Cars
- Creates insight in the threat landscape within the automotive
- Identifies promising business development areas for Deloitte

Chapter 3

Connected Cars

This section elaborates on Connected Cars in terms of definition, history and network topology. Based on this last elaboration, the various in-vehicle networks are mapped onto the OSI model for comparison purposes. Finally the ArchiMate$^{\text{TM}}$ modeling language and its risk modeling extensions are introduced.

3.1 Definition

Since there are many definitions found when searching for the terms "*connected car*" or "*smart car*" we first need to establish some common ground and define how this study interprets these terms. The term *smart car* was introduced when cars were given some form of *Artificial Intelligence (AI)*. However over the years cars not only got forms of AI but also means to communicate with other cars.

Therefore, Wikipedia defines a Connected Car as: "*a car that is equipped with Internet access, and usually also with a wireless local area network*" (Wikipedia, 2015). IT consulting firm Cognizant uses a more technical definition, namely: A Connected Car is defined "*as a vehicle using mechatronics, telematics and artificial intelligence technologies to interact with the environment to provide greater safety, comfort, entertainment and, importantly, a 'connected-life' experience.*" (Cognizant, 2012). Within this thesis we focus on Connected Cars, not on smart cars.

Based on these previous definitions we define a Connected Car as "*a vehicle that is equipped with sensors and internet access in order to interact with other vehicles and its surroundings*". Where a Connected Car is equipped with the means to communicate with cars and infrastructure, an autonomous vehicle is able to use this information to (partially) drive the vehicle without human intervention. This requires a great deal of extra technology. Since autonomous vehicles are still in a testing phase this study focuses on connected cars. However, since Connected Cars are a subset of autonomous vehicles, findings and recommendations are likely to be generalizable to the autonomous vehicle domain (See Figure 5).

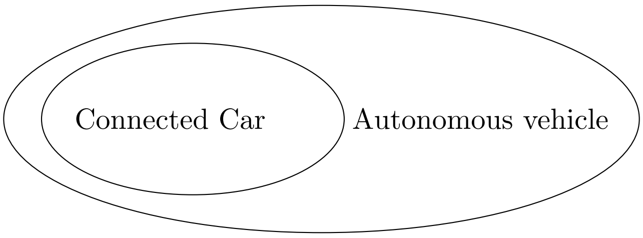


FIGURE 5: Connected car and autonomous vehicle.

In the United States the National Highway Traffic Safety Administration has proposed a taxonomy in order to formally classify cars based on their self-driving capabilities (Left Lane, 2015). This taxonomy is graphically represented in Figure 6. Vehicles that are currently available on the consumer market hover between Level 1 and Level 2. New features such as Adaptive Cruise Control[1] an Lane Assist[2] are typical examples of automated vehicle response or *Advanced Driver Assistance Systems (ADAS)*.

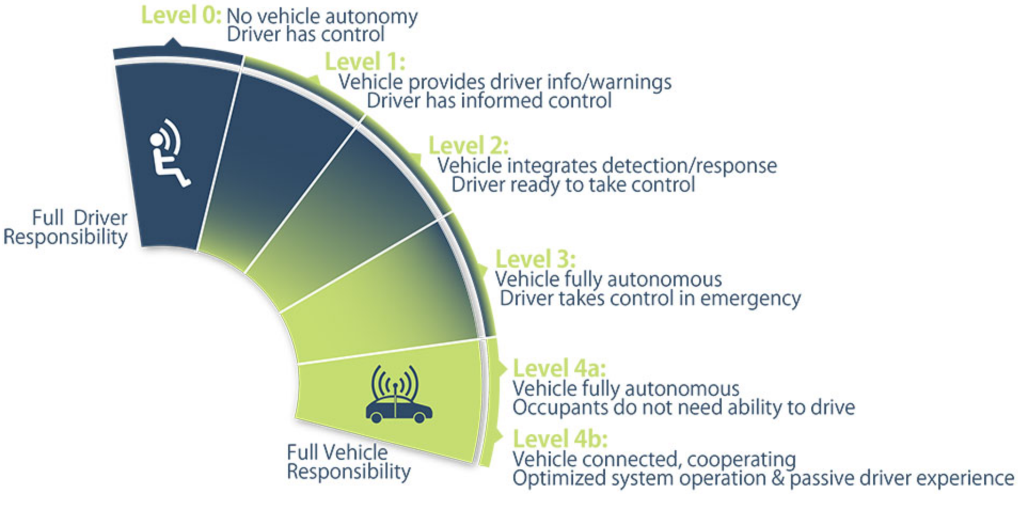

Level 0: No vehicle autonomy
Driver has control
Level 1:
Vehicle provides driver info/warnings
Driver has informed control
Level 2:
Vehicle integrates detection/response
Driver ready to take control
Level 3:
Vehicle fully autonomous
Driver takes control in emergency
Level 4a:
Vehicle fully autonomous
Occupants do not need ability to drive
Level 4b:
Vehicle connected, cooperating
Optimized system operation & passive driver experience
Full Driver Responsibility
Full Vehicle Responsibility

FIGURE 6: NHTSA classification system. Image from (Left Lane, 2015).

[1] Adaptive Cruise Control matches the speed of your predecessor

[2] Lane Assist corrects steering when you tend to wander out of your lane

3.2 History

Where the first cars produced relied on mechanics and hydraulics to operate properly, cars nowadays fully rely on electronics. This started with efforts to reduce the amount of air pollutants exhausted by cars. By automating the engine with parameters such as fuel injection, ignition timing and valve timing; exhaust efficiencies were gained. This Engine Control Unit was the first embedded system in a car.

Since the 70s the number of *Electronic Control Units (ECUs)* in cars has increased drastically (Navet et al., 2005). An ECU is an embedded system that controls one or multiple systems within a car. Systems such as *Anti-lock Braking System (ABS)*, *Electronic Stability Program (ESP)* and *Transmission Control Units (TCU)* are examples of ECUs.

As one can imagine most of these systems need to exchange data in order to work properly. In the early days when the number of ECU systems in a car was limited, this connectedness was achieved by hard-wiring each ECU to the relevant other systems. As technology progressed this approach was rendered unfeasible in large systems, this due to available space, costs and complexity.

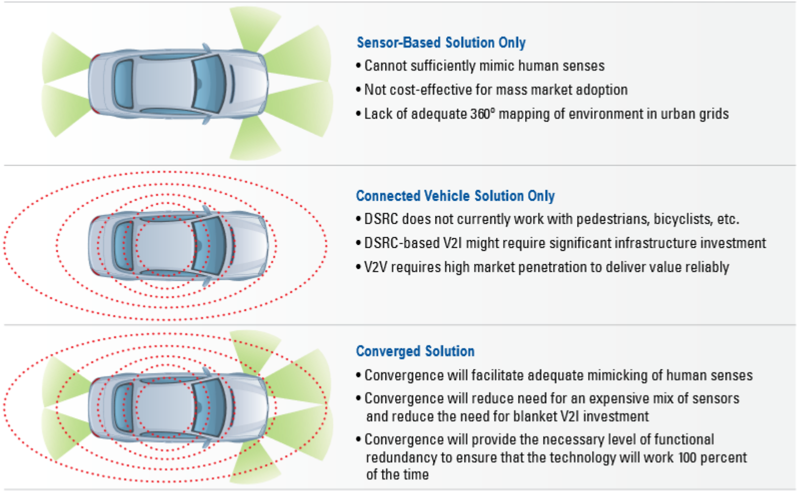
Figure 7: ECU's in a car. Image from (Delphi, 2012).

Therefore, car manufactures adopted in-car networks to provide for connectivity in a cost-effective and feasible manner (See Figure 7). The majority of cars nowadays has a *Controller Area Network (CAN)* since these are cost effective and easy to install. This CAN network can be accessed through the *On-Board Diagnostic version 2 port (OBD-II)* for maintenance purposes. This port is mandatory for all cars sold after 2008 in the United States (Koscher et al., 2010).

Using all this technology cars nowadays are so called *Cyber Physical Systems (CPS)*. Driving actuators such as throttle, gear and break are controlled digitally. When the driver pushes the gas pedal this is noticed by the *Electronic Throttle Control (ETC)*, which in turn will increase the air intake and fuel-injection into the motor. The usage of these electro-mechanical systems instead of mechanics and hydraulics is begin referred to as *Drive-by-Wire (DbW)*.

Next to these internal networks modern cars are equipped with a variety of sensors to measure their surroundings and transponders in order to communicate with it. This communication can either be of a *Vehicle-to-Vehicle (V2V)* or *Vehicle-to-Infrastructure (V2I)* nature. Examples of V2I communication are traffic lights, toll gates and parking garages.

In order for vehicles to become truly self-driving an accurate view of its surroundings is important. In order to achieve this the sensory information is combined with V2V communication. This approach is necessary because there will always be older vehicles without the newest technological advances. This principle is illustrated in Figure 8. Moreover, sensors provide a more accurate view of the surroundings when compared to V2V communication means.



Sensor-Based Solution Only

- Cannot sufficiently mimic human senses
- Not cost-effective for mass market adoption
- Lack of adequate 360° mapping of environment in urban grids

Connected Vehicle Solution Only

- DSRC does not currently work with pedestrians, bicyclists, etc.
- DSRC-based V2I might require significant infrastructure investment
- V2V requires high market penetration to deliver value reliably

Converged Solution

- Convergence will facilitate adequate mimicking of human senses
- Convergence will reduce need for an expensive mix of sensors and reduce the need for blanket V2I investment
- Convergence will provide the necessary level of functional redundancy to ensure that the technology will work 100 percent of the time

FIGURE 8: Converged sensing approach. Image from (Left Lane, 2015).

3.3 Networks

In order to provide communication between ECUs, several networks are in place within a modern vehicle. Commonly found networks are the *Controller Area Network (CAN)*, *FlexRay*, *Media Oriented Systems Transport (MOST)* and *Local Interconnect Network (LIN)* (Kleberger et al., 2011b, Koscher et al., 2010, Sagstetter et al., 2013, Wolf et al., 2004). This combination of networks used to cater for all different network requirements. Infotainment systems for instance call for a higher bandwidth, where other systems require fault tolerant networks. Therefore, a variety of network topologies is used within cars (Bosch, 2013) as shown in Figure 9.

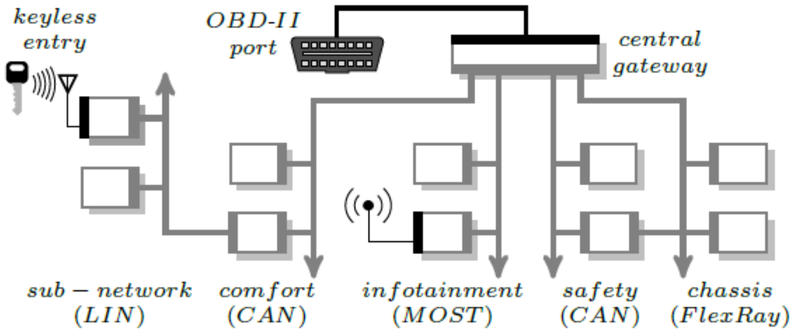


FIGURE 9: Schematic overview of various in-car networks.
Image from (Sagstetter et al., 2013).

3.3.1 CAN-bus

The **C**ontroller **A**rea **N**etwork is a *linear* bus-type network (See Figure 10). In such a network all nodes are connected to a single communication bus. Advantages of this type of network are that it is easy to connect new nodes to the network and that cabling costs are low. Thereby, the CAN network is used in cars since it is resilient against electro-magnetic interference. Major disadvantage is that it has a single point of failure, a broken bus results in (parts of) the network becoming unavailable.

However, the CAN standard only specifies the Physical and Data Link layer of the OSI model. Hence, networking principles like addressing and error checking are not implemented within the CAN standard (Bosch, 2013).

3.3.2 MOST

The **M**edia **O**riented **S**ystems **T**ransport is a higher speed communication network tailored for multimedia purposes. Instead of a linear topology the MOST-bus uses a ring based one (See Figure 10). Since the MOST bus is designed specifically for multimedia purposes its specification encompasses all 7 layers the OSI model.

3.3.3 FlexRay

As a result of further digitization within cars, the need arose for a high bandwidth, low latency network. Because of this shared problem major players in the automotive industry (BMW, Volkwagen, General Motors a.o.) teamed up as the *FlexRay Consortium* to develop the new FlexRay network. This new network had to be faster than the commonly used CAN network and more flexible in terms of topology.

This resulted in a new in-vehicle network that is capable to operate in a linear, ring or star topology (Fujitsu, 2006). Because of its baud rate of 10 *Mbps* it is used for the latest data consuming innovations such as *Adaptive Cruise Control (ACC)* and Lane Assist.

3.3.4 LIN

The **L**ocal **I**nterconnect **N**etwork serves as a simple, cost effective bus network used for non-complex tasks. Think of mirror-adjustment, window opening and lighting. Since other nodes on the CAN network are usually responsible for these tasks the LIN network is often used as a sub-network within a CAN network as depicted in Figure 9.

3.3.5 Gateway

In order for nodes on these networks to be able to communicate with each other one or more gateways are installed in cars. This because nodes on different networks need to be able to communicate with each other, for instance, the unit controlling the driver's display on the CAN network does need data from the Engine Control Unit which is a node in the FlexRay network.

Unfortunately there is little reliable data available on the precise implementation of these gateways. Some encompass all in-car networks while other might just connect a few. However, it is safe to assume that all networks are interconnected directly or indirectly (Bosch, 2013, Fujitsu, 2006, Koscher et al., 2010, Sagstetter et al., 2013).

3.3.6 Ethernet

A promising technology for in-car networks is Ethernet. It is widely used within the Internet and other applications but still has some issues before it can be applied within cars. It is expected that Ethernet will become the new standard over the next few years. Up until then experts state the following: "*Ethernet is an emerging technology for in-car applications. While domain-specific implementations for info- and entertainment are ready for deployment, a unified in-car Ethernet backbone is subject of ongoing research.*" (Steinbach et al., 2012).

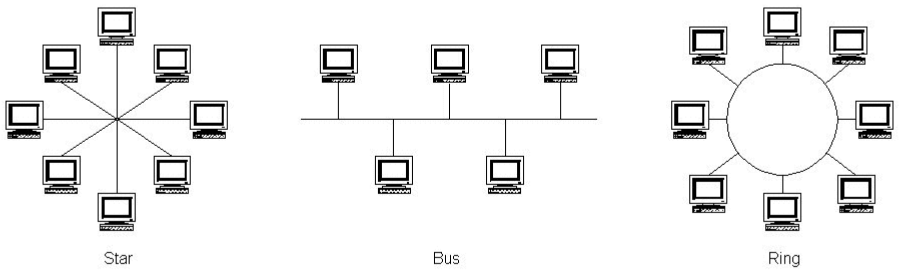


FIGURE 10: A star, bus and ring network topology. Image from (Bramer, 2003).

3.4 OSI Network stack

Based on the network descriptions in the previous section, we can compare how these networks fit into the OSI network stack and what vulnerabilities arise from the networks' specification (International Standards Organization, 1994). Within the OSI model various networking functions are abstracted into *7 layers*. By clearly separating concerns interoperability should be guaranteed.

Within automotive networking there is a variety of networks involved as discussed in Section 3.3. These networks not only differ in terms of topology but also in terms of OSI layers implemented. This results in inconsistent implementations regarding addressing, access control and encryption. The CAN, LIN and FlexRay network only specify OSI layer 1 and 2 in their definition. This results in only having a physical layer definition and a communication protocol (See the bottom two layers in Figure 12) (Bosch, 2013).

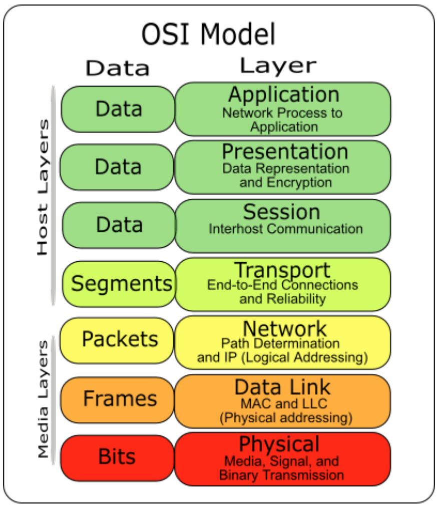

OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure 11: Layers in the OSI model. Image from (Hewitt, 2005).

Figure 12 depicts how the various in-vehicle networks map onto the OSI model. It shows clearly that the MOST bus implements all the layers of the OSI model, where others are limited to layer 1 and 2 only.

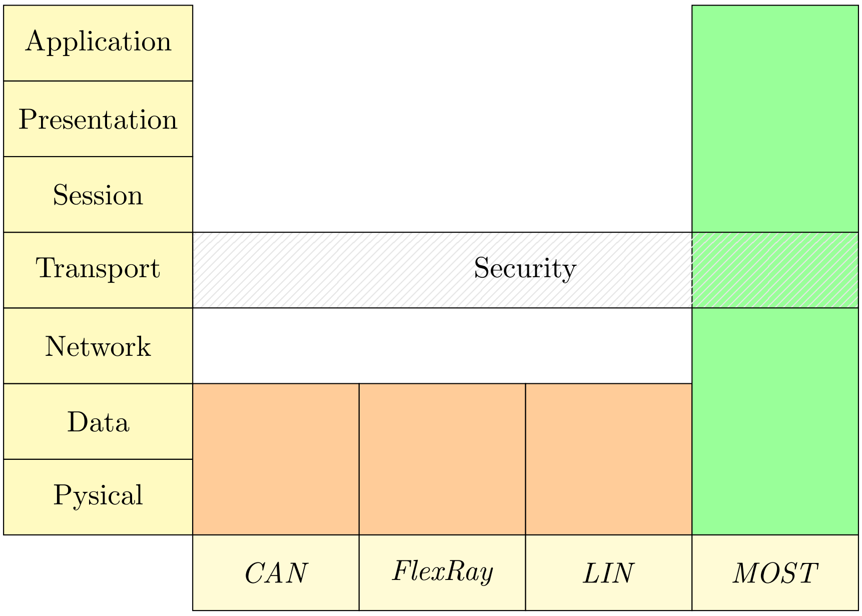


Figure 12: In-vehicle networks mapped on the OSI model.

The majority of network security mechanisms reside in the transport layer. It can be a deliberate choice to use networks that have not implemented security features. This can be the case when insensitive data is shared or when hosts on the network provide security features themselves.

3.5 ArchiMate^{TM}

ArchiMate^{TM} is a modeling language that is developed by *The Open Group* (The Open Group, 2015). According to its specification ArchiMate^{TM} is "*a visual design language with adequate concepts for specifying inter-related architectures*". We chose to use the ArchiMate^{TM} modeling language since it is an established modeling tool (Jonkers et al., 2011). By using ArchiMate^{TM} to model the in-car network a clear link between business, application and technology can be identified.

However, ArchiMate^{TM} does not specify means to model risks onto architectures. To overcome this deficiency *The Open Group* published a white paper in which existing modeling concepts are repurposed in order to be able to model risk (Band et al., 2015). Using this extension we aim to adequately model risks using ArchiMate^{TM} in order to see how information security risks are related to the vehicular network architecture. This risk extension of ArchiMate^{TM} will be treated in Section 3.6.

ArchiMate^{TM} uses a combination of *layers* and *aspects* to provide a structured framework for modeling. The following layers are defined by The Open Group (The Open Group, 2015):

1. The Business Layer offers products and services to external customers, which are realized in the organization by business processes performed by business actors.
2. The Application Layer supports the business layer with application services which are realized by (software) applications.
3. The Technology Layer offers infrastructure services (e.g., processing, storage, and communication services) needed to run applications, realized by computer and communication hardware and system software.

These layers have intersections with the following three *aspects* thus yielding a `3x3` matrix as depicted in Figure 13. ArchiMate^{TM} uses the following aspects:

1. The active structure aspect represents the structural concepts (the business actors, application components, and devices that display actual behavior; i.e., the ‘subjects’ of activity).
2. The behavior aspect represents the behavior (processes, functions, events, and services) performed by the actors. Behavioral concepts are assigned to structural concepts, to show who or what displays the behavior.
3. The passive structure aspect represents the objects on which behavior is performed. These are usually information objects in the business layer and data objects in the application layer, but they may also be used to represent physical objects.

Within these areas ArchiMate has defined specific elements to depict passive structure, behavior and active structure (See Figure 14). Note that in this image green items illustrate the technology layer, blue items resemble the application layer while yellow items depict the business layer.

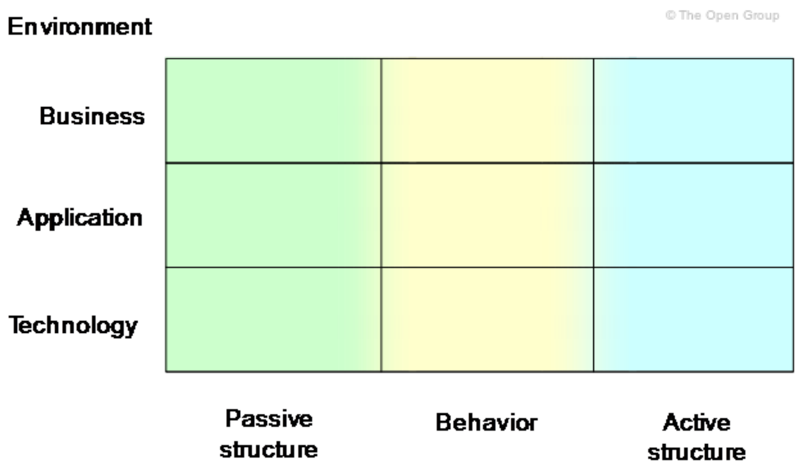


Figure 13: Passive structure, behavioral elements and active structure. Image from (The Open Group, 2015).

Figure 14 shows the meta model for the technology layers. This provides a clear overview of what elements are involved and how they interact. Furthermore this meta model standardizes positioning of elements in the model. All the elements from this meta model can be found in Figure 15 which shows all the ArchiMate modeling concepts.

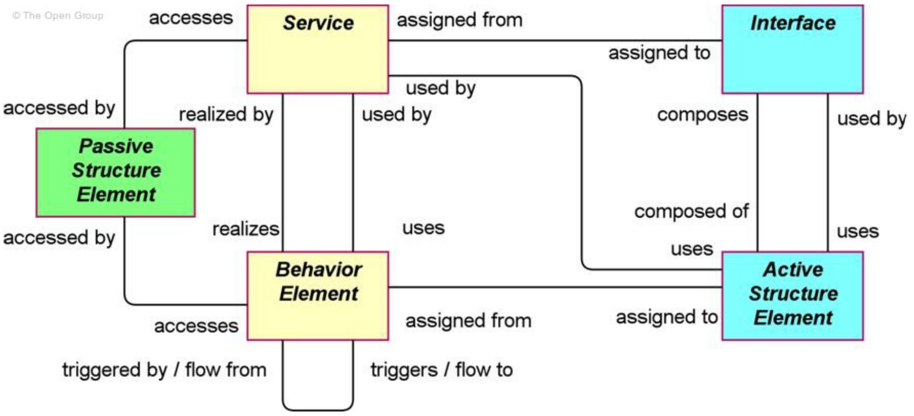


Figure 14: Meta model of the technology layer. Image from (The Open Group, 2015).

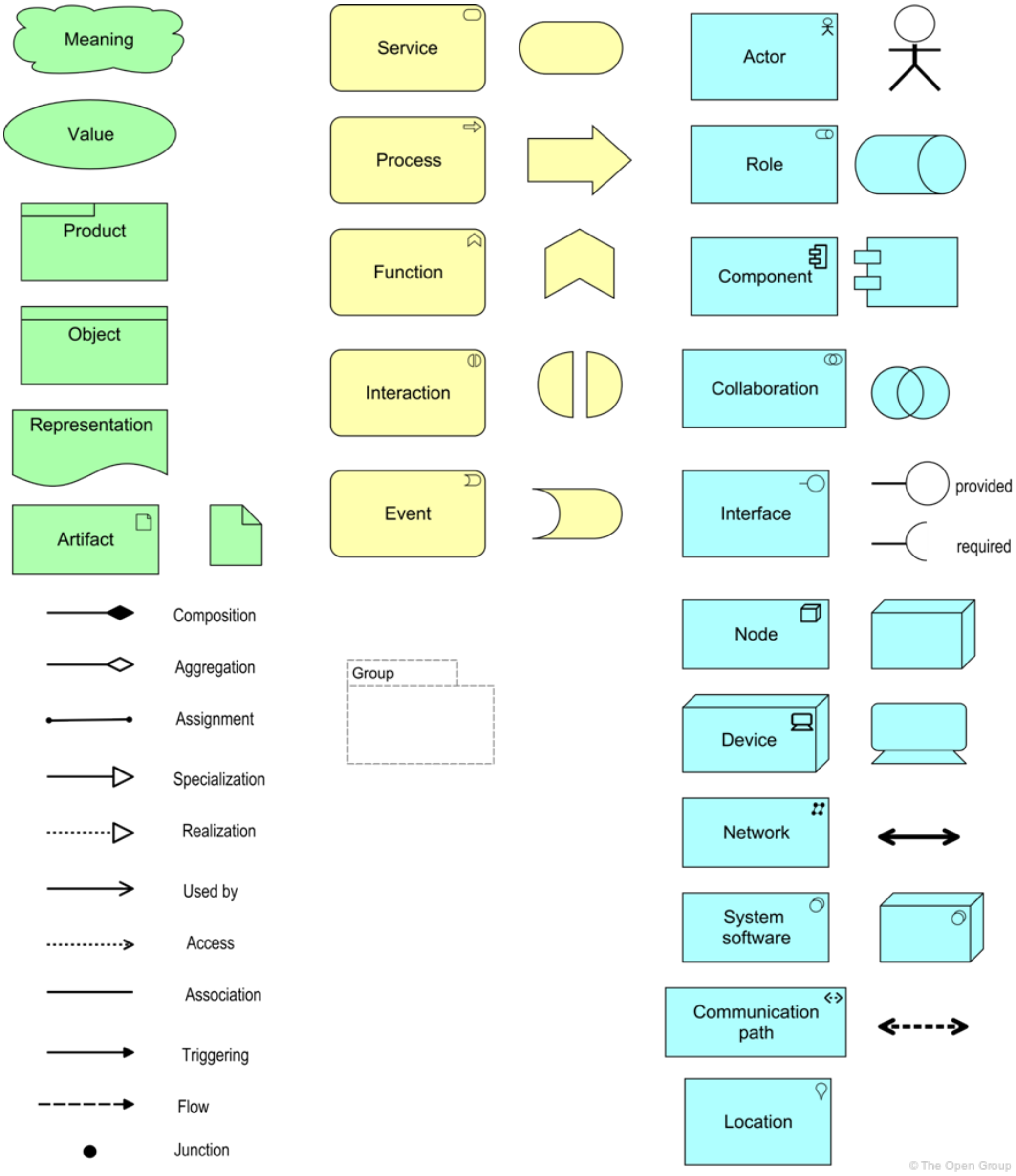


FIGURE 15: Concepts from the ArchiMate language.
Image from (The Open Group, 2015).

3.6 ArchiMate^{TM} Risk Modeling

Within the previous section ArchiMate^{TM} was introduced as a modeling tool. Within this section we will elaborate on how ArchiMate^{TM} can be used as a risk modeling tool.

ArchiMate^{TM} is developed in order to "*provide a graphical language for the representation of enterprise architectures over time (i.e., including transformation and migration planning), as well as their motivation and rationale*" (The Open Group, 2015). Clearly this description does not take the element of risk into consideration.

Information system risk management frameworks are widely available, i.e. (National Institute of Standards and Technology, 2012) but lack formal notation and representation according to Grandry et al. (Grandry et al., 2013). Therefore, he suggests an extension of the ArchiMate^{TM} language which was later adopted by *The Open Group* (Band et al., 2015, The Open Group, 2015). Currently no other method has been introduced for modeling risks in ArchiMate^{TM}.

This paper by Band et al. proposes a method of modeling risks within ArchiMate^{TM}(Band et al., 2015). By repurposing elements which are originally designed to model motivation, risks can be modeled using the ArchiMate^{TM} language. The mapping of these motivational elements for risk purposes is shown in Table 5.

Table 5: Risk concepts mapped onto the ArchiMate^{TM} language

Risk concept	**ArchiMate elements**
Threat agent	Business actor
Threat event	Business event
Risk	Assessment
Risk Metrics	Attributes of assessment
Vulnerability	Assessment
Risk Control, treatment and mitigation	Driver
Control requirement	Requirement
Asset at risk	Value / Other
Policy	Principle

Using these components allows us to map risks directly onto the layered ArchiMate$^{\text{TM}}$ models already in place. Figure 16 shows how vulnerabilities, risks and controls are modeled while still using the layered ArchiMate$^{\text{TM}}$ modeling approach. By repurposing ArchiMate$^{\text{TM}}$ vulnerabilities, threat events, loss events, risks and controls are modeled. Using this modeling approach a graphical overview is created which makes it easy to see the origin of risk, vulnerabilities, threats and other risk components.

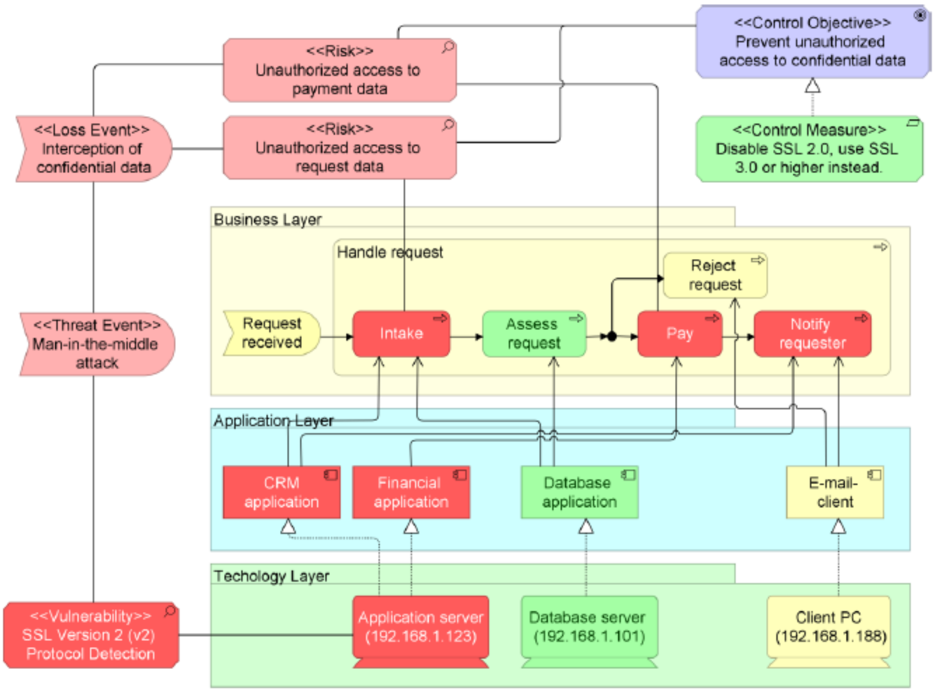

<<Risk>>
Unauthorized access to payment data
<<Control Objective>>
Prevent unauthorized access to confidential data
<<Loss Event>>
Interception of confidential data
<<Risk>>
Unauthorized access to request data
<<Control Measure>>
Disable SSL 2.0, use SSL 3.0 or higher instead.
Business Layer
Handle request
Reject request
Request received
Intake
Assess request
Pay
Notify requester
<<Threat Event>>
Man-in-the-middle attack
Application Layer
CRM application
Financial application
Database application
E-mail-client
Techology Layer
<<Vulnerability>>
SSL Version 2 (v2) Protocol Detection
Application server (192.168.1.123)
Database server (192.168.1.101)
Client PC (192.168.1.188)

FIGURE 16: Risk Modeling in ArchiMate$^{\text{TM}}$. Image from (Band et al., 2015).

3.7 ArchiMate$^{\text{TM}}$ model

Now that we introduced the concept available in ArchiMate$^{\text{TM}}$ together with its risk extension we can start modeling the Connected Car network structure in ArchiMate. Based on various sources of the in-car network architecture we develop a model in ArchiMate$^{\text{TM}}$ to link infrastructural elements to the application and business layers.

3.7.1 Design rationale

Since cars are equipped with a large number of ECUs our goal is not to come up with a complete list of ECUs in our model in order to keep the model comprehensive and understandable. The focus of the model is to map risks onto the in-vehicle networks which are located in the *Technology layer*. As mentioned in Section 3.3 on page 21 there are 4 major networks used within cars which are connected by a gateway.

Due to the hardware separation within cars an ECU is both a networking component as well as an application component. Modeling this as a collective entity is not possible within the layered ArchiMate modeling approach. Therefore, we have chosen to model the physical node in the technology layer whilst depicting the provided application in the application layer whenever possible. Since all the ECUs are a node in the network, a hardware device running a certain type of software and provide an infrastructural function one would need four ArchiMate concepts in order to model this correctly when striving for completeness.

Moreover, there are various business processes that can be carried out by the different actors involved. We have chosen not to model all of these, only a few to illustrate interactions with other layers and to illustrate how risks map onto the model.

3.7.2 Design traceability

Based on a variety of sources we identified which networks are present in a modern vehicle (Bosch, 2013, Fujitsu, 2006, Kleberger et al., 2011b, Koscher et al., 2010). Apart from which networks are used within cars they also state that all networks are somehow connected. This can be directly or indirectly through the use of a gateway ECU. We have chosen to model this as a single gateway (See Figure 17).

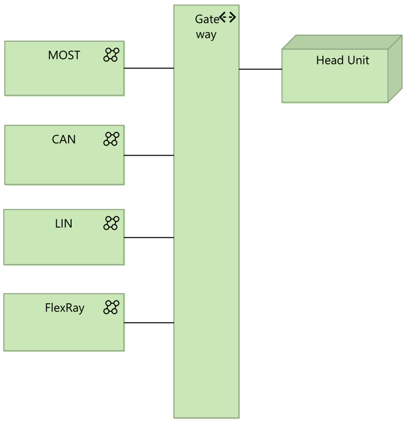


FIGURE 17: In-vehicle networks in ArchiMate^{TM}

Concerning the various networks involved there is no consensus within the ArchiMate^{TM} community on how to models those. Following the official documentation would result in using an *association* relation for all the nodes on the network. Due to the interconnectedness we have chosen to embed nodes on the network in the network node to improve readability, this based on the approach by Wierda (Wierda, 2014).

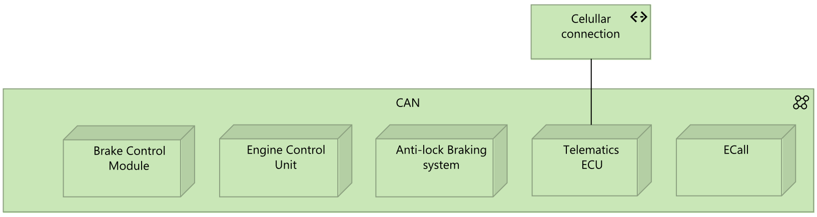


FIGURE 18: CAN network in ArchiMate^{TM}

Little information is found on where exactly the external connectivity reside in the nodes and the networks. Some argue that these functions operate as a node on the CAN or LIN network (Sagstetter et al., 2013), where others state that these functionalities are embedded in the head unit of a car (Jakob et al., 2012).

Figure 19 shows the technology layer of our ArchiMate model. The business layer and application layer of our model can be found in Appendix D. Once again, the focus of this study is on the technological layer and vulnerabilities resulting from the in-vehicle network. Other layers are partly filled to illustrate the interactions between the layers.

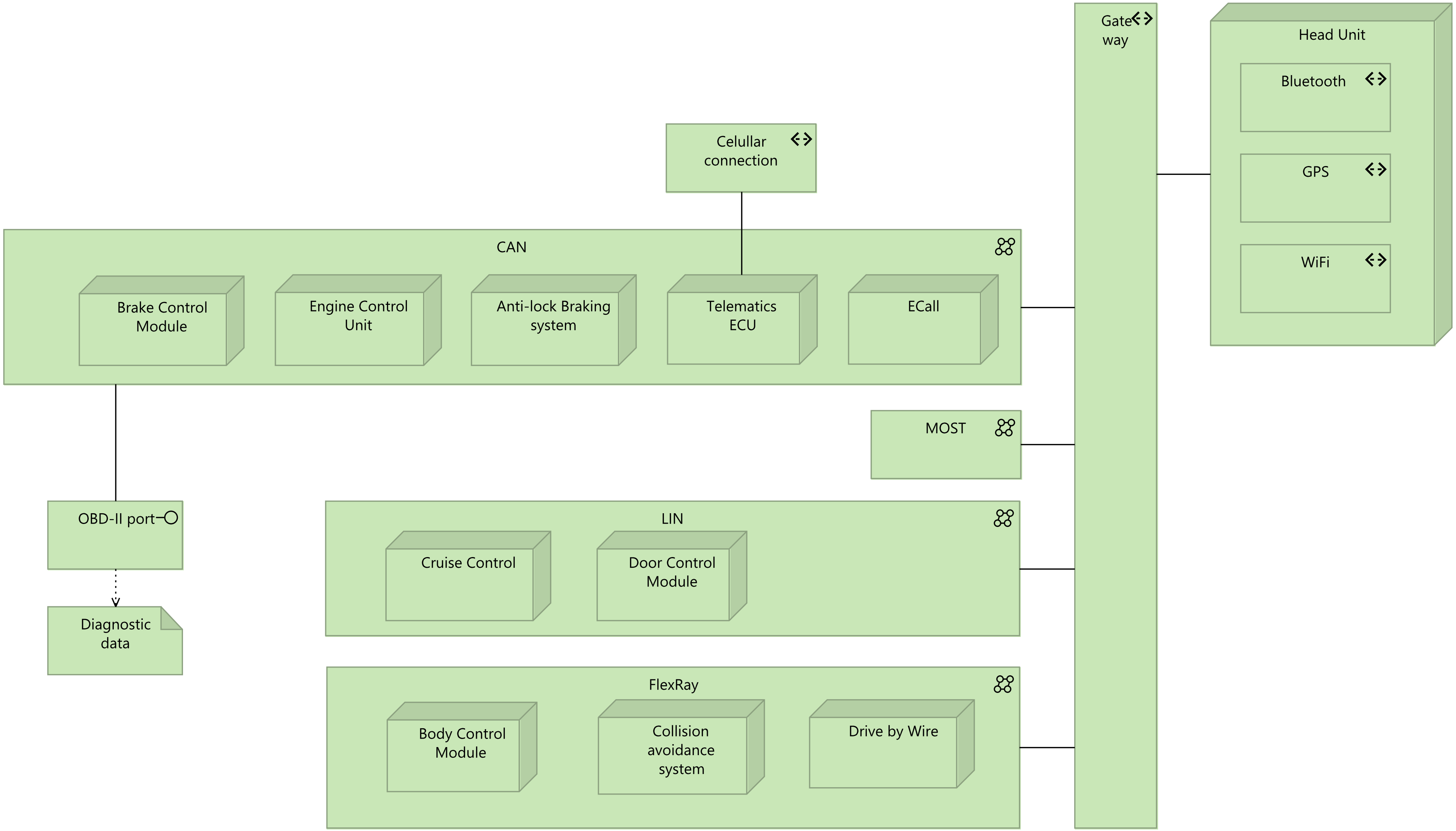


FIGURE 19: Technology layer of our ArchiMate^{TM} model.

3.7.3 Terminology

We use the following terminology as introduced in the white paper from Band et al. (See Table 6) in order to have a common understanding of the following terms.

Table 6: Definition of Risk concepts as used by ArchiMate^{TM} by Band et al. 2015.

Term	**Definition**
Asset	Anything that has value to the organization and is necessary for achieving its objectives.
Business Asset	Describes information, processes, capabilities, and skills inherent to the business and core mission of the organization, having value for it.
IS Asset	A component of the IS supporting business assets like a database where information is stored.
Security Goal	A property or constraint on business assets describing their security needs, usually for confidentiality, integrity, and availability.
Risk	The combination of a threat with one or more vulnerabilities leading to a negative impact harming the assets.
Impact	The potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or the cause of a risk) is accomplished.
Vulnerability	A characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security.
Threat	A potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed.
Risk Treatment	An intentional decision to treat identified risks.
Security Requirement	The refinement of a treatment decision to mitigate the risk.
Control	Controls (countermeasures or safeguards) are designed to improve security, specified by a security requirement, and implemented to comply with it.

Chapter 4

Risk

Based on the vulnerabilities found in the literature we will translate those into risks for car manufacturers. Firstly, we will present the vulnerabilities identified by the scientific community. Secondly, a more formulated definition of risk is given in order to make it more quantifiable. Based on this definition we identify various risks for car manufacturers. Furthermore, we elaborate on risk management strategies and on how controls influence the residual risk.

4.1 Vulnerabilities from literature

In this section we will elaborate on the vulnerabilities identified by the scientific community. Based our systematic literature review as mentioned in Section 2.2 vulnerabilities are identified (See Table 7). The legend for the papers used is found in Appendix B.

Within our literature review we noted that the terms "*vulnerability*" and "*risk*" were used inconsistently throughout the various papers reviewed. Risks resulting from a certain vulnerability were sometimes marked as vulnerability. Therefore we chose to omit any 'vulnerabilities' that did not fit within our taxonomy (as defined in Section 3.7.3).

Since the descriptions used in Table 7 can be somewhat ambiguous, a more detailed description of these vulnerabilities mentioned in the literature can be found in Appendix C.

All articles are from different authors excluding number I and IV. These are both written by Kleberger et al.. This illustrates that these are trustworthy since that department frequently researches Connected Cars.

TABLE 7: Literature review matrix

Articles, see Appendix B for legend	Integration of untrusted components	ECU reprogramming	Lack of CAN bus protection	Poor protocol implementation	Firmware update Over-The-Air	Misuse of protocols	Non-compliant to standard	Imperfect network segregation	Physical threats	Logical threats	Poor computational power	VANET security	Mobile integration	ECU Re flashing while driving	Based on embedded systems	Increasing number of wireless communication interfaces	Trojans & Malware
I.	✓	✓	✓	✓	✓	✓											
II.															✓		
III.												✓					
IV.									✓	✓							
V.		✓	✓								✓						
VI.	✓	✓		✓		✓											
VII.	✓																
VIII.	✓												✓			✓	
IX.		✓	✓														
X.			✓		✓		✓	✓						✓			
XI.	✓																
XII.																	✓
Totals	5	4	4	2	2	2	1	1	1	1	1	1	1	1	1	1	1

As shown in Table 7, the scientific community has identified the *integration of untrusted components* combined with the ability *reprogram ECUs* and the *lack of CAN bus protection* as biggest vulnerabilities. Based on discussions with domain experts and the fact that there are *17* vulnerabilities identified by the scientific community which are mostly closely related, we have chosen to group these vulnerabilities into categories.

The grouping of concepts is mentioned in the systematic literature review approach by Wolfswinkel et al.. Based on Webster and Watson he recommends to '*develop a logical approach to grouping and presenting the key concepts*'. Therefore we decide to group the vulnerabilities identified by the scientific community into categories. Based on reviewing the corpus of papers again and discussion with automotive specialists we define the following vulnerability categories:

C1. *ECU*
This category comprises all vulnerabilities which results from the technology used in **E**lectronic **C**ontrol **U**nits.

C2. *Protocols*
Vulnerabilities due to the resilience and implementation of protocols are grouped together here.

C3. *External devices*
These are risks that arise due to the integration of external devices. These can be mobile phones, tablets, pacemakers and so on.

C4. *Interconnectedness*
In contrast to the previous category these are risks that are due to the interconnectedness of the various in car networks. Note the difference between the coupling of external devices which is a post-production action and the interconnectedness of the networks which is by design.

C5. *CAN Bus*
Since a lot of vulnerabilities are related to the CAN bus we decided to group them separately to prevent the majority of issues falling in the protocol category.

Table 8: Vulnerability grouping

	C1. ECU	**C2.** Protocols	**C3.** External devices	**C4.** Interconnectedness	**C5.** CAN bus
Integration of untrusted components		✓	✓	✓	
ECU reprogramming	✓	✓			
Lack of CAN bus protection					✓
Poor protocol implementation		✓			
Firmware update Over-The-Air		✓	✓		
Misuse of protocols		✓			✓
Non-compliant to standard		✓			✓
Imperfect network segregation				✓	
Physical threats		✓			
Logical threats		✓			
Poor computational power	✓				
VANET security			✓	✓	
Mobile integration			✓	✓	
ECU Re flashing while driving		✓			
Based on embedded systems		✓			
Increasing number of wireless communication interfaces	✓	✓			
Trojans & Malware				✓	
Totals	*3*	*11*	*4*	*5*	*3*

Note that the categories used are not mutually exclusive since some concepts occur in multiple categories. Because vulnerabilities cover a variety of aspects it was not possible to come up with mutually exclusive categories.

As shown in Table 8 most vulnerabilities identified by literature are due to the **protocols** used within Connected Cars. This can either be due to poor protocol specification or poor protocol implementation. In the former case the protocol itself is not ideal within the context used whereas in the latter the implementation of the protocol does not reflect the specification correctly. For instance, in some cars it is possible to reprogram the Engine Control Module while driving, despite the fact that the protocol prescribes this should not be possible (Kleberger et al., 2011b).

Furthermore, the **interconnectedness** of the various in-car network leads to a high number of vulnerabilities, this is because all in-vehicle network are directly or indirectly connected to each other. In this manner a small breach can lead to a full loss of driving capabilities as argued by Koscher et al. (Koscher et al., 2010). This *unfair* battle between attackers and defenders should be noted and is frequently discussed within cyber security (Winterfeld and Andress, 2012). A hacker only needs a single vulnerability that can be exploited while defenders have to be right every time.

> "*For instance, from a tampered ECU, an attacker could easily inject a large number of messages with a high priority, hindering the correct functionality of other functions without having any knowledge about the architecture.*"
>
> — (Sagstetter et al., 2013)

4.2 Risk definition

In Section 3.7.3 we defined several terms including *Risk*. However, the definition "*The combination of a threat with one or more vulnerabilities leading to a negative impact harming the assets*" is hard to measure and therefore needs some additional definition in order to quantify risk.

The *National Institute of Standards and Technology (NIST)* defines risk as "*a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence*" (National Institute of Standards and Technology, 2012). This is in line with Boehm who states that Risk Exposure is the product of probability and loss (Boehm, 1989). Therefore, risk is often denoted as:

$$Risk = P \times I \tag{4.1}$$

As argued by Bannerman, this "*Common conception of risk has some limitations*" (Bannerman, 2008). This because, this definition "*ignores capabilities to mitigate and respond*" to risks (Zhang, 2007). Therefore, we look for other definitions of risks that are more feasible for our approach.

Based on the *Information System Security Risk Framework (ISSRM)* by (Dubois et al., 2010) as mentioned by Band et al. and shown in Figure 20 on page 43 we will derive vulnerabilities and come up with related risks. This model defines Risk as *Impact* times *Event* in which the latter is defined as a combination of a certain *Threat* and *Vulnerability*. Thus, based on this ISSRM and Jones and Ashenden we define Risk as the product of *Threat*, *Vulnerability* and *Impact* (Jones and Ashenden, 2005).

$$Risk = Threat \times Vulnerability \times Impact \tag{4.2}$$

Once again the definitions that we used in Section 3.7.3:

- *Threat* A potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed.
- *Vulnerability* A characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security.
- *Impact* The potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or the cause of a risk) is accomplished.

As Band et al. suggest, the term *threat* is ambiguous. It can refer to either "*a threatening circumstance ... or the actual event that may cause harm*". Therefore he suggest to decompose the term into *Threat Agents* and *Threat Events*. A Threat Agent is the entity that intents to harm assets, where a *threat event* is a *threat agent* exploiting a vulnerability using a certain attack method to harm the assets.

We choose to use Equation 4.2 to quantify risks as it takes ones ability to respond and mitigate the risk into account. Using this definition we will come up with risks based on the vulnerabilities found in literature.

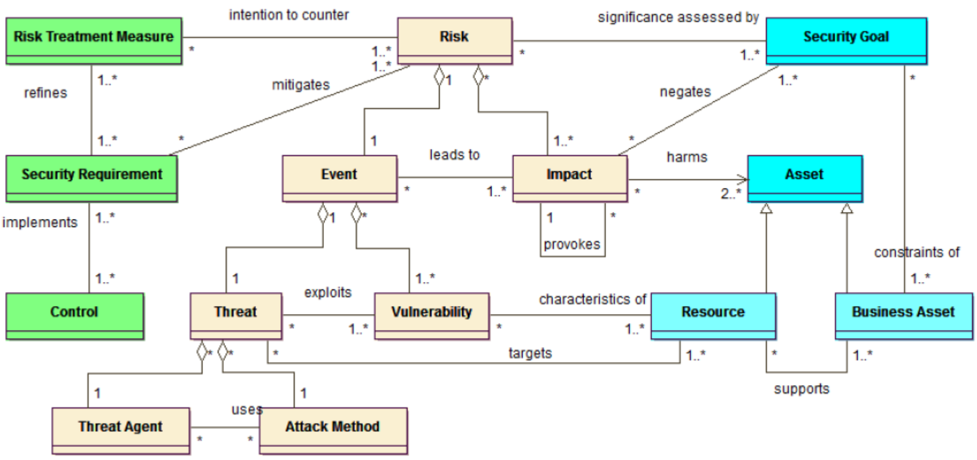


Figure 20: Information Security Risk Management. Image from (Dubois et al., 2010)

Furthermore, Figure 20 shows how security goals and treatments relate to risks. In order to protect a certain asset security goals are formalized. By identifying threat events that could harm the asset, security requirements can be developed. By putting controls in place, threat events with adverse impact on the asset can be prevented.

4.3 Information security

The term "*information security*" has been around for a long time, since the Roman Empire people felt the need to communicate with each other over a secure channel. Inventions like the Caesar cipher made secure communications possible and greatly decreased the likelihood that information would fall in the wrong hands. Until 2000 the discipline of information security was seen as merely a technical one focusing on mathematics in order to design ciphers that could protect data. After the millennium the definition of information security was extended and other disciplines such as computer science, economics and psychology were incorporated (Anderson and Moore, 2009).

In order to make sure we have a common understanding of the term "*information security*" we consult a variety of sources for a definition. Firstly the United States Title 44 Chapter 35 defines information security as follows (Cornell University Law School, 2002):

The term "*information security*" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide —

- (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information repudiation and authenticity;
- (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (C) availability, which means ensuring timely and reliable access to and use of information.

Because of the further digitalization of society this definition of Information Security recieved more critique over the last decades. Critics argue that elements such as non-repudiation, possession and utility should be added explicitly to the definition. Parker for example came up with a new definition and argued that Information Security comprises six elements (Gantsou and Sondi, 2014b).

He adds *authenticity*, *possession or control* and *utility* to the classic CIA triad (Parker, 1998). However, due to the broad definition of the classic CIA triad new definitions never really gained enough support. Therefore we chose to use the original definition of information security comprising of *Confidentiality*, *Integrity* and *Availability.*

Within automotive networking information security is an important. The components integrity, confidentiality and availability are all important within Connected Cars. From a privacy point of of view the component confidentiality is the most important, this in order to ensure that adversaries can not eavesdrop on personal information. Although privacy is important the other two aspects of information security might be even more important within Connected Cars. Availability of the several networks ensures that nodes can transmit their messages (near) instantly. Without capacity on the transport medium safety-critical messages might not arrive in time and may lead to potentially dangerous situations.

The most important aspect of information security in automotive networking is the message integrity, this was confirmed unanimously by subject matter experts within our focus group, which is discussed in Section 5.2. In order for nodes to react on a certain message on the network they have to be sure of the integrity of a message. A *hacked* ECU for example might propagate messages with a fake origin; as one can imagine this is a dangerous situation. Using such an approach a hacked radio for instance might be capable of controlling the engine. This is exactly what happened in the recent Jeep hack (Wired, 2015).

A flaw in Chryslers connectivity platform *Uconnect* exposed 1.4 million vehicles to remote hacks. *Uconnect* aims to increase the car's connectivity by using a cellular connection for tracking and entertainment purposes. This requires the car to have an Internet connection and hence having an IP address. This allowed hackers to remotely gain access to in-vehicle networks and insert packages.

4.4 Response strategies

Within the risk management discipline there are four response strategies identified by the literature. These are risk avoidance, risk transference, risk mitigation and risk acceptance (Bannerman, 2008, Boehm, 1989). A short summary of the various explanations by Bannerman:

- *Risk avoidance*
  In a risk avoidance strategy one would refrain from engaging in activities in order to avoid risks completely. By changing a projects scope risky activities can be avoided in order to protect assets.

- *Risk transference*
  In a risk transference strategy the risks are transfered to another entity in order to reduce ones accountability. This strategy does not actually reduce the risk but merrily transfers accountability.

- *Risk mitigation*
  In a risk mitigation strategy controls are being used to reduce the likelihood and/or the impact of a certain event. This is done in order to reduce, or completely diminish the risk.

- *Risk acceptance*
  In a risk acceptance strategy no action is taken. Within this strategy one is aware of the risks involved and accepts that they might impact certain assets.

In this study we will come up with mitigation strategies for the key risks from a car manufacturers perspective.

4.5 Controls

As discussed in Section 4.4 control measures are used in order to reduce the initial risk. Within this section we give insight in which control measures are currently in place within vehicular networking.

As shown in Figure 20 controls are put in place in order to decrease risks. As discussed in Section 4.4 this can either be done by reducing the *threat*, *vulnerability* or *impact* or a combination these elements. In line with Jones and Ashenden, they state that by putting controls in place the volume of the *risk cube* can be reduced (Jones and Ashenden, 2005). After applying these mitigative measures the risk owner only has to deal with the residual risk. This is depicted by the cube in Figure 21 below.

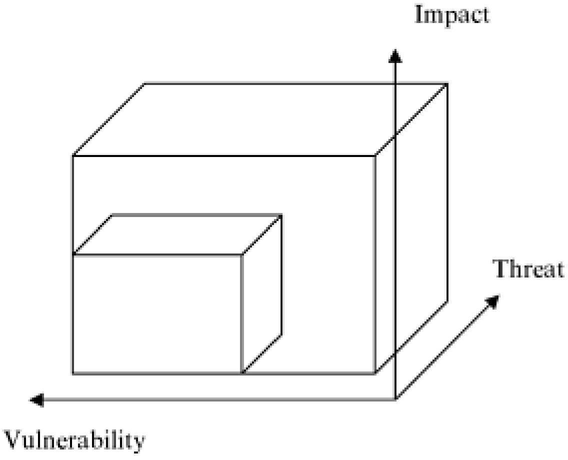
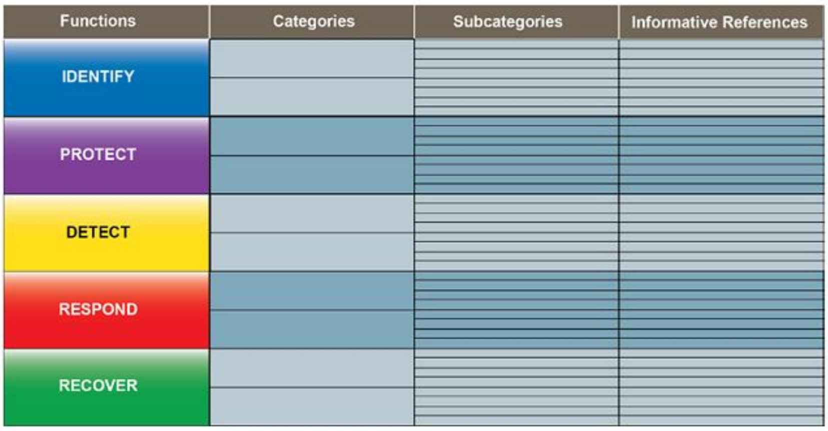


FIGURE 21: Risk quantification cube. Image from (Jones and Ashenden, 2005).

When searching for controls in place within connected cars little information is available. Some articles mention a firewall to shield traffic between networks but they appear easy to get around (Koscher et al., 2010). In order to get an overview of the current state of controls used within cars we use a industry standard control framework as reference.

Within an industry standard control framework such as NIST several control categories are identified (National Institute of Standards and Technology, 2012). We use these in order to check to what extent controls are currently applied within connected cars in Section 5.3. NIST defines a standard control scheme with the following steps (as shown in Figure 22):

- *Identify*
  Identification is about a proper understanding of the threat context. By concisely mapping the assets involved and determining their value for the business environment a risk assessment can be conducted.
- *Protect*
  Protecting your assets can be done by programs such as access control, data security, and protective technologies.
- *Detect*
  When an incident occurs it is essential that it is detected at all in order to be able to respond swiftly. NIST offers guidelines on anomaly detections, continuous monitoring and detection processes.
- *Respond*
  In order to be able to respond in a timely fashion it is essential that possible responses are planned beforehand. By analyzing possible outcomes and planning communications plans and mitigative measures the impact can be reduced.
- *Recovery*
  After an incident occurred it is necessary to restore capabilities thereby minimizing the impact of a cyber incident.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 22: NIST Control framework. Image from (National Institute of Standards and Technology, 2012).

Chapter 5

Results & Discussion

Within this Chapter we present the main results of our research. Firstly, we describe how our focus group was constructed. Secondly, the results of this focus group are presented. Thereafter, we elaborate on how the results from our systematic literature review and the outcomes of our focus group are mapped onto our ArchiMate^{TM} model. Subsequently, we evaluate the usage of the ArchiMate^{TM} language for risk modeling purposes. Lastly, we summarize the outcomes of this chapter and discuss implications for practice.

5.1 Focus group

We choose to use a focus group as means of validation and identification of missing components to our model if needed. By consulting experts with different background improvements in the validity of our architectural model and corresponding risks can be made. In our focus group we had experts from Deloitte with backgrounds in Cyber Security, Automotive Security and Privacy Protection.

The focus group method is a "*qualitative data gathering technique where focus group sessions involve several participants assembled for a planned discussion to explore a specific topic of interest to researchers in a permissive, non-threatening environment*" as stated by Lange (Lange, 2002). This with as purpose "*to acquire as much information as possible from a group of experts on a given topic. This is accomplished by prompting the group with pre-specified topics and open-ended questions, allowing the discussion to evolve around these open-ended questions, and facilitating interaction among the participants.*" (Sutton and Arnold, 2013).

The goals of our focus group are as follows:

I. To see if the vulnerabilities and risks identified from literature are recognized by practitioners.

II. To identify any missing vulnerabilities and risks.

III. To identify key risks for car manufacturers

IV. To validate mitigation strategies found in the literature

By having experts with different backgrounds in our focus group we ensure that outcomes will be as unbiased as possible. The experts which were present in our focus group are shown in Table 9. With six participants we had a proper group size to engage in discussions. Furthermore the mix between young, tech-savvy consultants and more experienced managers was ideal and led to many vivid discussions.

Table 9: Focus group participants

	Role
I.	Automotive security Consultant
II.	Automotive security Consultant
III.	Automotive security Consultant
IV.	Cyber & Privacy Advisory Manager
V.	Cyber & Privacy Advisory Director
VI.	Public sector Director

We opened our focus group welcoming the participants and again explaining why they were invited for the session. It was noted explicitly that there were no right or wrong answers and that all input was valuable for this research. After this introduction we gave more in-depth explanation of the subject to make sure all participants fully understood the network structure inside connected vehicles; this since not all participants had a technical background. A complete overview of activities in our focus group can be found in Table 10.

Within our focus group we first asked the participants to come up with risk and mitigation strategies prior to showing the results from our systematic literature review. This to stimulate creativity and prevent biased answers. Afterwards, based on their own responses, the results from the literature review were shown and discussed.

Table 10: Focus group program

Subject	**Time**
Introduction	10 minutes
On In-Vehicle networking	10 minutes
Risk identification	20 minutes
Risk mapping	20 minutes
Risk mitigation	20 minutes
Discussion and further remarks	10 minutes

In this next section we will discuss the outcomes of our focus group.

5.2 Focus group results

Within this section we will present the results from our focus group. We combine the data from the conducted focus group with insights from our systematic literature review as described in Section 2.2. By combining data from scientific data with empirical insights a more detailed overview of risks is created. Within Section 4.2 we defined risk as follows: $Risk = Threat \times Vulnerability \times Impact$ (See Equation 4.2 on page 42)

Using this formula we aim to quantify the risk of the several vulnerability categories as identified in Table 8 on page 40. This by quantifying the three components of risks as shown in the formula above. In Table 7 on page 38 we researched vulnerabilities which can be used within this formula.

Within the articles studied several concepts were identified. These concepts are discussed and grouped in Section 4.1. Based on the frequency of the identified concepts within the categories, we ranked the categories using *very high* for the ones that contain the largest number of vulnerabilities relative to the other categories and very low for categories that contain less vulnerabilities. This gives us an overview of how frequent vulnerabilities occur in a category when compared to others. Table 11 shows how *Vulnerability* (grayed out) is ranked along the various categories.

Table 11: Risk quantification.

	Risk components			
	Threat	Vulnerability	Impact	Risk
ECU		+	++	+
Protocols	+	++	++	++
External devices	−	+		
Interconnectedness	++	+	++	++
CAN Bus	+	++	++	++

Legend

++	Very high
+	High
	Neutral
−	Low
−−	Very low

When it comes to the other two factors within our risk formula *threat* and *impact* we consulted the subject matter experts within our focus group. They provided us with information regarding the *threat* component, how easy it is to exploit a certain vulnerability. Based on this information we quantified the threat levels for the several vulnerability categories identified. Combining this empirical data with additional information from the studied articles we came to our ranking.

As shown in Table 11 nearly all risks have a significant impact. This is due to the fact that connected cars are *Cyber-Physical Systems (CPS).* In such a system a computer controls a physical system; in our case, a car. When the cyber system is breached the possibilities to alter the physical system are nearly limitless. In the event of an adversary breaching the computer system the majority of driving controls can be influenced by the adversary. Therefore the impact of a greater deal of the vulnerability categories is very high. This was acknowledged by the participants in our focus group.

For instance as discussed by Jakob et al. "*an attacker could potentially use the brake control unit to block the left front wheel completely causing the car to spin while driving on the motorway at high speed*" (Jakob et al., 2012). This illustrates the dangerous outcomes of a hacker breaching the in-vehicle network.

Table 12: Information security risks.

	Information Security		
	Confidentiality	Integrity	Availability
ECU	✓	✓	✓
Protocols		✓	✓
External devices	✓	✓	✓
Interconnectedness		✓	✓
CAN Bus			✓

Based on the definition of information security given in Section 4.3 can identify which vulnerabilities may harm the information security within cars. Table 12 shows what aspects of information security might be harmed by certain vulnerability categories.

The protocols used within the in-vehicle networks are the biggest threat to integrity. The absence of cryptographic capabilities or other means of validation result in messages on the network that can not be authenticated. Within a Cyber Physical System this is crucial. Not knowing if a message is authentic and should thus be trusted in disastrous.

Within the scientific community several risk mitigation strategies are introduced to decrease information security risks. Table 13 shows which risk mitigation strategies were identified by which article in particular. Since the literature was primarily focused on risk identification, we used our focus group both to validate these findings and to come up with new risk mitigation strategies.

TABLE 13: Risk mitigation traceability matrix

	M1. Network honeypots	**M2.** Intrusion Detection Systems	**M3.** Improve protocols	**M4.** Flow analysis	**M5.** Increase computational capabilities	**M6.** Improved device verification
I						
II						
III	✓					
IV						
V						✓
VI						
VII		✓				
VIII						
IX						
X			✓		✓	
XI				✓		
XII						

Within our focus group we discussed the risk mitigation strategies identified by the scientific community with our subject matter experts. This to see if these strategies are observed in practice or not. Table 14 shows which risk mitigation strategies were observed by our subject matter experts, risk mitigation strategies underneath the double line are newly found strategies within our focus group (from **M7** onwards).

Table 14: Validity of risk mitigation strategies

	Strategy	**Observed**
M1.	Network Honeypots	−−
M2.	Intrusion Detection Systems	−
M3.	Improve protocols	++
M4.	Flow analysis	−
M5.	Increase computational capabilities	+
M6.	Improved device verification	++
M7.	Network separation	+
M8.	Secure by Design	++
M9.	PEN-testing	++

	Legend
++	Most of the time
+	Often
	Sometimes
−	Rarely
−−	Never

Unanimously, strategies **M1** and **M4** were not observed in practice by our participants. According to our experts *Network Honeypots* were not suited for risk mitigation because these are merely a tool to analyze the attackers behavior. Due to the isolated nature of these honeypots it is hardly possible to use this information in an ongoing attack.

The increase in computational capabilities (**M6**) was observed frequently and useful within our focus group. Having more computational capabilities allows ECUs to perform cryptographic functions in order to authenticate packets on the network. Currently the computational capabilities of ECUs are not sufficient to perform cryptographic functions in a real time manner.

Furthermore, Secure by Design (**M8**) was considered a valuable risk mitigation strategy since it resolves a variety of issues. By rethinking the architecture used in vehicles and overhauling the entire architecture, other design principles can be adopted. Originally the in-vehicle network was seen as a trusted network with all nodes acting in the best interest of the entirety.

However, due to the rapid growth of embedded systems and potential adversaries on the network this premise no longer holds. Therefore, the in-vehicle network was labeled as a "*hostile environment*" by Henniger et al. within the EU sponsored vehicle intrusion project EVITA (Henniger et al., 2009). Adopting a Secure by Design approach requires a change in protocols, hardware and software architecture. These efforts were observed by our participants, however they do to take significant time and resources.

Lastly, PEN-testing (**M9**), short for penetration testing, was observed frequently by our subject matter experts. Within such a test so called *white hat* hackers attempt to breach a car in order to identify vulnerabilities. Opposed to *black hat* hackers, *white hat* hackers are not motivated by profit, fame or enjoyment. By working together with software developers they help to reduce the number of weaknesses and vulnerabilities in software and hardware, thus improving safety.

This approach is useful because most new automobiles have Over-The-Air update capabilities (Koscher et al., 2010). This enables car manufacturers to push software updates to vehicles already sold. This instead of recalling those cars and applying the software updates at dealer stations. This improves software flexibility and reduces warranty costs (Red Bend Software, 2011). For example Toyota spent 2 percent of their total sales on recalls only. This is nearly 5 times the industry average (Red Bend Software, 2011).

However issuing software patches poses risks. Every update has to be checked concisely to make sure the software is as safe as possible. In order to check the car software PEN-testing was identified as a valuable tool in practice by our focus group participants. By periodically testing the car software, vulnerabilities can be identified and resolved in a timely manner.

As shown in Table 13 papers V and X proposed mitigation strategies which are observed by subject matter experts (See Table 14). This means that, based on this study, one could argue that mitigative strategies are hardly applied within the automotive industry. Based on evidence from Section 4.5 regarding controls in place, it seems obvious that security within connected cars is currently immature.

5.3 Controls in place

Based on the mitigation strategies identified in the previous Section 5.2 we will map those strategies onto the NIST framework as introduced in Section 4.5. This in order to assess to what extent controls are currently in place within Connected Cars.

Table 15 below shows how the various mitigation strategies identified map onto the NIST control framework. Since car manufacturers are currently in the process of developing new networking standards they are, at least partially, aware of the risks that current standards pose. When it comes to protection and detection, however, controls are still immature. Car manufacturers use very little protective technologies and have no ability to detect threats and respond in a real time manner (Koscher et al., 2010).

Table 15: Mitigation strategies mapped to NIST categories

	Identify	Protect	Detect	Respond	Recover
M1. Network Honeypots			✓		
M2. Intrusion Detection Systems			✓		
M3. Improve protocols		✓			
M4. Flow analysis		✓	✓		
M5. Increase computational capabilities		✓			
M6. Improved device verification		✓			
M7. Network separation					
M8. Secure by Design					
M9. PEN-testing	✓	✓			

As shown in Table 15 the control measure currently in place within Connected Cars are primarily focused on *protecting* and *detecting* potential hacks. This illustrates that little effort is put into identifying the threat landscape and preparing response strategies. Also, recovery measures were not observed by us based on the literature review and the input from subject matter experts.

> "*While we believe that standard access controls are weak,*
> *we were surprised at the extent to which the controls that did exist were*
> *frequently unused.*"
>
> — (Koscher et al., 2010)

5.4 Mapping

Within this section we will map the risks and vulnerabilities identified onto the ArchiMate^{TM} model we developed. Figure 19 on page 35 shows the technology layer of our developed model. Based on this layer of the ArchiMate^{TM} model we map the vulnerabilities identified in Table 11 on page 52. By mapping the vulnerabilities identified earlier in this thesis, we want to discover which architectural components are responsible for the majority of the vulnerabilities and risks arising from them.

Using this information, both Deloitte and car manufacturers can trace risks towards specific components or architectures. As argued by The European Union Agency for Network and Information Security a "*thorough examination of the risk sources*" is an important part of risks analysis (The European Union Agency for Network and Information Security). Therefore, we use ArchiMate^{TM} to map the risks and vulnerabilities identified onto the in-vehicle network. Based on this mapping we can recommend Deloitte on which topics it might be able to assist automotive manufactures. This is highly relevant since Deloitte services several parties within the automotive sector. Figure 24 shows the various vulnerabilities identified within the category they belong to.

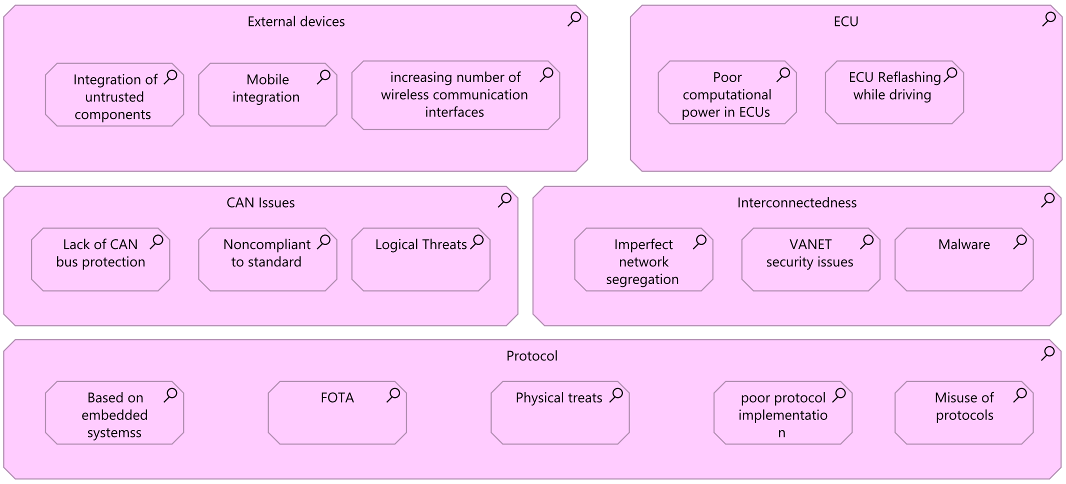

External devices
Integration of untrusted components
Mobile integration
increasing number of wireless communication interfaces
ECU
Poor computational power in ECUs
ECU Reflashing while driving
CAN Issues
Lack of CAN bus protection
Noncompliant to standard
Logical Threats
Interconnectedness
Imperfect network segregation
VANET security issues
Malware
Protocol
Based on embedded systemss
FOTA
Physical treats
poor protocol implementatio n
Misuse of protocols

Figure 23: Vulnerability grouping in ArchiMate^{TM}

Some of the vulnerabilities identified by the scientific community can be mapped easily onto a single hardware components. However some vulnerabilities are not directly to be traced to a single hardware component. Figure 24 shows how the identified risks map onto our architectural model.

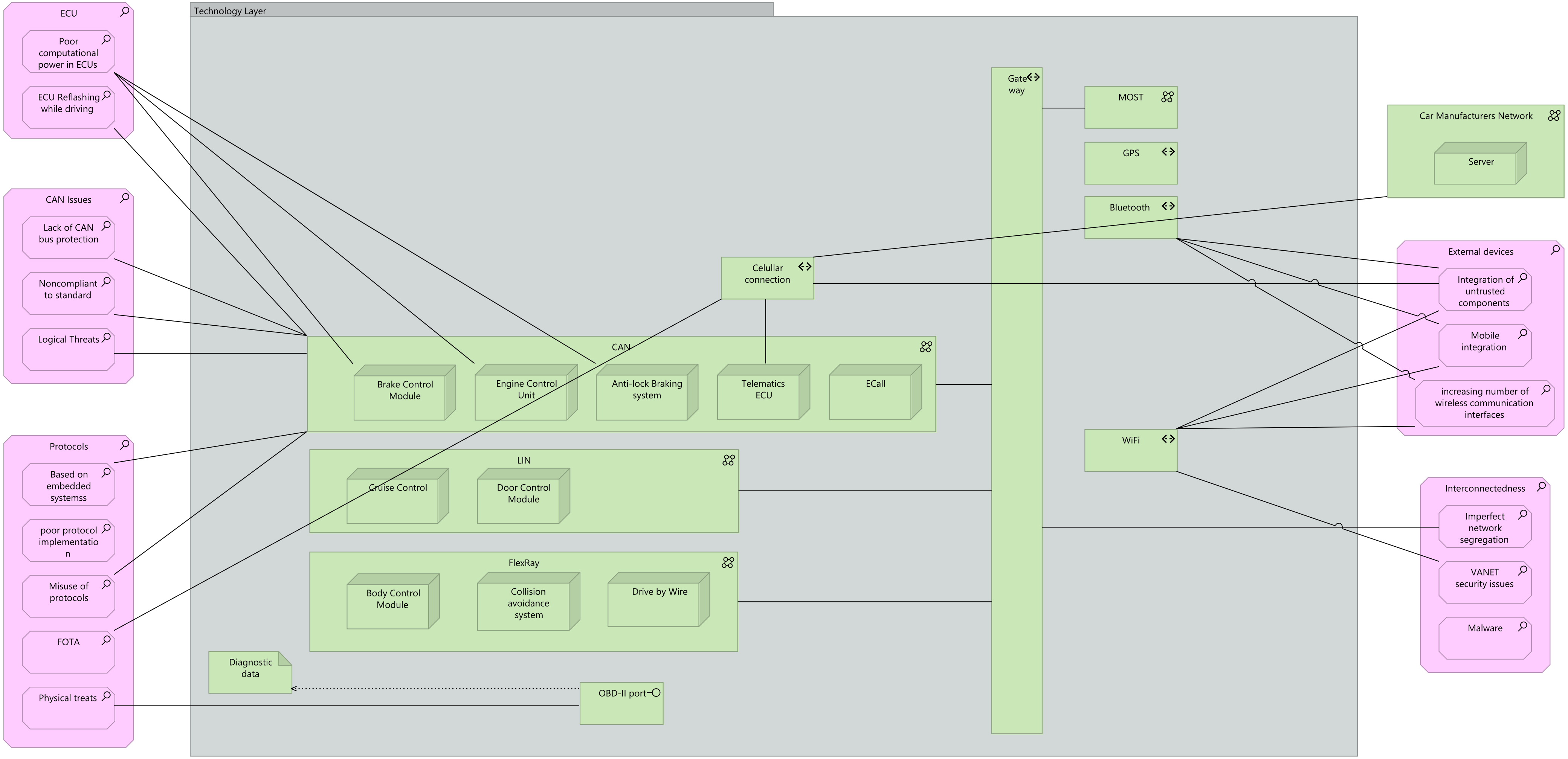


Figure 24: Technology layer of our ArchiMate^{TM} model

Figure 25 shows how several vulnerabilities can be used in order to create an information security risk for car manufacturers. By combining one our more vulnerabilities a hacker is able to create an event that harms elements of Information Security, this can either be the *integrity*, *availability* or *confidentiality* of information.

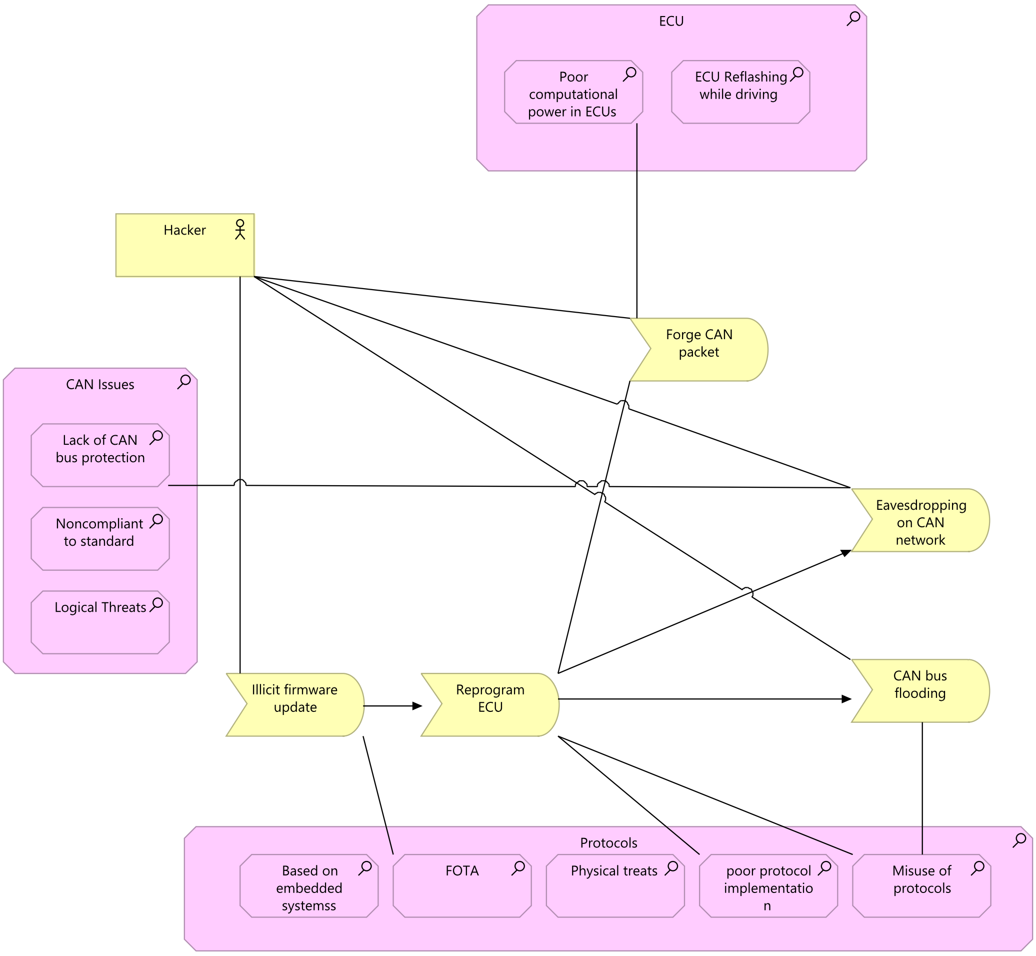


FIGURE 25: Attack path of a hacker

5.5 Evaluation

Based on our experiences with ArchiMate$^{\text{TM}}$ and its risk extension we evaluate its usefulness for risk modeling purposes. ArchiMate$^{\text{TM}}$ offers a variety of concepts that can be used for modeling, because of the generic nature of these concepts ArchiMate$^{\text{TM}}$ is suited well to model the architecture of Connected Cars, this was to be expected since ArchiMate$^{\text{TM}}$ is developed as an Enterprise Architecture modeling instrument.

By re purposing elements from the motivational layer ArchiMate$^{\text{TM}}$ has powerful means to model risks. However, it is clear that it was not developed for this purposes. There is no ability ot group concepts and create connections with other elements. Furthermore, the only *universal* connector is the associative one. This gives little options to depict causality and to show which control measure mitigates which risk.

Lastly, ideally you want to have a language and tool that support different automated views on the architecture. Within ArchiMate$^{\text{TM}}$ one has the ability to manually construct views, however, in such a complex environment as a car the ability to zoom in and zoom out would be ideal. This yields useful overviews on a variety of abstraction levels.

5.6 Discussion

Within this section we discuss the implications for practice based on everything until this point. Based on our systematic literature review, as discussed in Section4.1, we argue that the threat landscape of Connected Cars has became more complex over the last years. The addition of wireless capabilities has opened up a wide range of possible attack vectors. Researchers have proven that it is easy to exploits wireless communication protocols in order to do harm (Checkoway et al., 2011, Kleberger et al., 2011b, Sagstetter et al., 2013).

> " *Therefore, any ECU accessible from outside the vehicle provides a potential intrusion point, including particularly the wireless access points.*"
>
> — (Sagstetter et al., 2013)

Exploiting weaknesses in remotely accessible hardware, it has been shown that arbitrary code can be executed thus allowing hackers to send packets on one this various networks. This due to the interconnectedness of the several in-vehicle networks as pointed out in Section 2.2. All ECUs on the various networks treat the network as a trusted environment, however it has been labeled as a "*hostile environment*" by researchers (Henniger et al., 2009).

> "*The exploit then forces the telematics unit to download and execute additional payload code from the Internet using the IP-addressable 3G data capability.*"
>
> — (Checkoway et al., 2011)

Currently, the lack of shared business case is withholding car manufacturers from engaging in network research activities. As pointed out by our focus group participants car manufacturers rely on proprietary designs and use controllers from preferred suppliers. Therefore, they have little flexibility to adopt new standards.

Currently, the majority of new automobiles has the ability to update (parts of) the in-car software. This gives car manufacturers the ability to update car software in a cost effective manner. With the growing base of software within cars chances increase that critical vulnerabilities are present. By issuing regular updates, Tesla updates its software every 2 weeks for example, manufacturers can prevent that newly found vulnerabilities are exploited. This is something car manufacturers can start doing right away for new vehicles.

Furthermore, the automotive industry does not exactly has a good track record when it concerns passenger safety. Ford did a cost-benefit analysis in the 60s and concluded that it was cheaper to let people burn to death in their vehicles compared to recalling 1.5 million vehicles. For that reason it would be could is a legislative body would develop new standards and oversee implementation.

Since it is likely that developing a new standard will take some time the automotive industry can increase its efforts on a short term to implement cryptography in its vehicles. By using more computational capabilities CAN packets can be signed and authenticated by nodes. This improves network security. Furthermore software should be tested more rigorously in order to decrease the number of vulnerabilities that is due to implementation faults.

In the long term, something has to be done regarding the network structure. Having the ability to patch software only gives flexibility on a software level, not on a hardware level. And given the fact that an average car last 8 to 10 years the network architecture of cars has to be future proof (Weisbaum, 2006). In order to achieve this car manufacturers and part suppliers have to agree on a new standard, preferably one issued by a regulatory body. This new standard should be secure by design. Ideally this to be developed standard finds a way to separate the safety critical and non-safety critical network. Ideally, to truly be resilient, safety-critical components should be "airgapped" (physically not connected) to any remote connectivity.

5.7 Business development opportunities

In order for Deloitte to be able to engage in the vehicular network security more domain specific knowledge has to be gained. Currently Deloitte employs a large number of talented security specialists but in-depth vehicular knowledge is limited. Developing these particular skills requires training and is likely to be time consuming.

A less time consuming alternative is to engage in *crisis management* en *privacy* issues involving cars. Deloitte has extensive experience within these disciplines in a variety of fields. Furthermore there is far less domain knowledge required to assist companies on these fields when compared to vehicular network security.

Deloitte has a variety of services available that could assist car manufacturers in improving the security and privacy in cars. Services such as *security by design* and *privacy by design* help companies to develop systems from the ground up whilst paying attention to security and privacy. By incorporating multiple layers of defense, systems are harder to breach.

Another service that might be useful is *Hacking as a Service (HaaS)*. This service periodically tests the infrastructure of companies for vulnerabilities. Since the software within cars is changing more frequently due to Over-the-air update abilities it is good practice to keep testing your software. In this manner bugs can vulnerabilities can be found before they can be exploited by attacks.

Last but not least is *Crisis Management* and *incident response.* Even when car security has improved seriously it is still likely that cars will be hacked some day. Hackers have infinite time and physical access to a car which makes it easier to find a security vulnerability (Henniger et al., 2009). Therefore, manufacturers should have contingency plans available when this event occurs. Preparing for such events before they actually happen improves the flexibility of an organization in times of crisis. This considering that the amount of controls identified in the respond and recover parts of the NIST framework is low.

Chapter 6

Conclusion

Within this thesis we combined scientific information regarding network vulnerabilities with empirical domain knowledge from the automotive experts and combined this in order to identify information security risk for car manufacturers. Furthermore we constructed an architectural model of connected cars in ArchiMate$^{\text{TM}}$ in order to map map vulnerabilities and risks onto architectural elements. This chapter will synthesize previous chapters into conclusions and recommendations. This based on the research question as stated in Chapter 1. Furthermore future work and limitations of this study are discussed.

6.1 Objectives

For evaluation purposes we reflect on the objectives stated at the beginning of this thesis. Within this thesis the following main objective was identified:

To map and asses information security risks within connected cars in order to make recommendations for risk mitigation and business development.

In Section 3.3 we investigated the networks used in connected cars. Based on vulnerabilities in those networks we identified information security risks in Chapter 4. Other objectives of study were:

SO1. Getting an overview of the architecture within a Connected Car.

SO2. Identifying the largest information security risks and map those onto the in-vehicle architecture using ArchiMate.^{TM}

SO3. Identifying risk mitigation strategies for the identified information security risks.

SO4. Measuring to what extent ArchiMate^{TM} is feasible for risk modeling.

SO5. Identifying promising areas for Deloitte for the development of new business propositions.

By developing an architectural model in ArchiMate^{TM} in Section 3.7 on page 32 we succeeded in **SO1**. Furthermore, we engaged in a systematic literature review in Section 2.2 in order to fulfill **SO2**. Our third objective is accomplished by combining data from our systematic literature review with data from our focus group described in Section 5.2. Within Chapter 5 we accomplished both **SO4** and **SO5**.

6.2 Research questions

In Section 6.1 we discussed how this thesis handled the different research objectives. In this section we will answer the various research question posed in Chapter 1. This in order to answer our main research question at the end of this chapter.

RQ. 1 What does the architecture of Connected Cars look like?

Throttle, gear and breaks are handled by computers while steering is assisted by power-steering computers. The phenomenon of a computer handling driving actuators is referred to as drive-by-wire.

As mentioned in Section 3.3 there is a variety of networks present in modern vehicles, this in order to support all drive-by-wire functionalities. Although exact responsibilities may vary across different manufacturers and car models the network found in cars are the **C**ontroller **A**rea **N**etwork (*CAN*), the **L**ocal **I**nterconnect **N**etwork (*LIN*), the *FlexRay* network and the **M**edia **O**riented **S**ystems **T**ransport (*MOST*).

These networks are present in order to provide a communication channel for the several **E**lectronic **C**ontrol **U**nits found in cars. These ECUs are embedded systems with a distinct functionality. Think of *Anti Lock Braking (ABS)*, *Air conditioning (AC)* and *Lane Assist (LA)*. In order to illustrate this architecture we developed an ArchiMate$^{\mathrm{TM}}$ model (See section 3.5). This model shows how various task are accomplished through the use of the various ECUs and networks.

Based on this we can say the architecture within Connected Cars is very distributed. This because car manufacturers have chosen to separate functionalities into distinct micro controllers. Over the last years the automotive industry adopted new functionalities such as: eCall, Wi-Fi and Bluetooth. These functions for external connectivity further complicate the threat landscape. Previously, physical access was needed in order to reprogram an ECU, now this can be done remotely.

RQ. 2 What architecture related information security risks are identified by the scientific community?

As mentioned in Chapter 2 there are several vulnerabilities identified for in-vehicle networks by the scientific community. Based on these vulnerabilities, we identified *5* categories of information security risks. These are **ECU**, **Protocols**, **External devices**, **interconnectedness** and **CAN bus**. In Table 11 we quantified the several risk categories identified.

Subsequently, we assessed to what extent information security is threatened by the various categories identified. Based on the most frequently identified vulnerabilities, **protocols** and **interconnectedness** we argue that primarily the *integrity* and *availability* of information security are threatened. Vulnerabilities that are responsible for these threats to information security are for instance: the ability to reprogram ECUs while driving, flood the network with high priority messages and the poor authentication of untrusted components.

New functionalities rapidly came to market over the last year and further complicated the threat landscape. However, both the vehicular networking protocols, as well as other protocols within cars were not designed with this in mind. Due to this increasing connectivity and integration of untrusted components combined with drive-by-wire functionality in cars a dangerous threat scenario emerges. Especially given the fact that this digitization will continue over the next decade.

Information security risks identified by the scientific community are primarily focused on abusing protocols to illicitly reprogram ECUs. In this manner attackers can send packets on the trusted CAN-network in order to modify driving behavior and virtually do anything.

RQ. 3 What architecture related information security risks are identified by practitioners in the field of automotive security?

Within our focus group, subject matter experts came up with a variety of information security risks. They however stressed that when it concerns information security within automotive networking, the *InfoSec* elements *Integrity* and *Availability* should be considered the most important. Of course privacy is always an issue but that does not necessarily influence the safety of the car. When the network Integrity or Availability is breached, safety-critical functions may not perform as desired.

According to our subject matter experts the biggest information security risk is the lack of flexibility on the hardware level of cars. Since all networks are connected on a hardware level safety-critical components can be accessed when a certain node is breached.

By introducing 3G/4G connectivity within vehicles, manufacturers have the ability to patch (parts of) the in-car software. This is particularly useful when new vulnerabilities in well established standards arise; think of the recent OpenSSL flaws Heartbleed and FREAK. These can be patched remotely instead of physically recalling the vehicles involved. Patching the software, however, does not change the fact that networks are still physically connected.

Lastly, our participants argue that car manufacturers should also focus on the phases *identify*, *respond* and *recover* within the NIST framework. This in order to get an thorough overview of the threat landscape and to prepare for possible attacks, this because it is very likely that cars will be hacked some day according to our subject matter experts.

RQ. 4 To what extent can ArchiMate$^{\text{TM}}$ with its extensions be used to model security risks?

Originally ArchiMate$^{\text{TM}}$ is developed to model Enterprise Architectures. Therefore it focuses on the technology, application and business layer. In order to model risks we adopted the practices as suggested by Band et al. in a whitepaper from *The Open Group*. He suggests to-re purpose elements from ArchiMate's motivation layer in order to be able to model risk, vulnerabilities and threats.

This extension gives valuable extra elements to model risks, vulnerabilities and threats. However within our case we ran into some problems. ArchiMate$^{\text{TM}}$ does not provide means for abstraction. Many of the vulnerabilities found have its impact on a number of nodes. Ideally you want to map vulnerabilities on an abstracted form of the problem, not on every node itself. Unfortunately ArchiMate$^{\text{TM}}$ has no way to do this nor to group elements and associate groups with elements.

The ArchiMate$^{\text{TM}}$ language specification states that "*In contrast to the aggregation or composition relationships, there is no "overall" object of which the grouped objects form a part.*". This forces one to place elements with a parent element to mimic the concept of abstraction. This concept is probably lacking because ArchiMate$^{\text{TM}}$ focuses on functional behavior of a system.

Furthermore, all views within the model have to be constructed manually.
ArchiMate$^{\text{TM}}$ does not provide means to automatically generate views on different abstraction levels. This is desired since vulnerabilities are usually present in small architectural components, for instance a single network node or communication path used. However, within risk management, one wants to get a high level overview of the risk involved. Within such an overview it is more important to see where this vulnerability is roughly, instead of a specific location. Ideally, the precise location could be determined by zooming in, into the model.

RQ. 5 How can these risks be mitigated?

The majority of risk identified was due to the **protocols** used within Connected Cars. In some cases the protocol specification is not resilient enough but there are numerous cases in which the protocol implementation is insufficient. This is likely due to the fact that the automotive sector is currently very focused on time-to-market and wants to develop new functionality as quickly as possible to keep competitive advantage.

Currently hardware and software architecture are drastically intertwined, due to the fact that car manufacturers buy ECU from preferred suppliers. This gives car manufacturers little flexibility regarding hardware architecture. Combined with the relatively long lifespan of a car and the progressing technology car manufacturers have to support a wide variety of vehicles. This makes it hard to standardize and focus on the development of a single platform. Furthermore, the car business is highly competitive and most car manufacturers use their own proprietary software.

In the long term the networking protocols within Connected Cars should be revised. Ethernet looks promising in early research but needs additional studying before it can be applied as vehicular backbone.

On the short term the automotive should implement incident response plans and start testing their own software more rigorously. By doing so security flaws can be adequately patched before hackers start to abuse them.

RQ. 6 Which areas are suitable for business development purposes for Deloitte?

Over the last decade software started to play a more important role within cars. The continuous expansion of the embedded network in cars led to an increase in code base. Combing this with the Over-the-Air update capability that modern automobiles possess, Deloitte can play an important role in this.

It is expected that in-car software will be updated frequently and will therefore need thorough and frequent testing. Deloitte could use its *Hacking as a Service* proposition to periodically PEN-test the car infrastructure. This in order to find vulnerabilities as quick as possible and work with car manufacturers to patch them as soon as possible. In this manner zero-day attacks can be avoided and continuous monitoring for the quality of software is in place.

Furthermore Deloitte can assist car manufacturers in the development of crisis management strategies. This in order to be more resilient in the event of a car hack.

Based on the answers to our research questions above we now answers our main research question:

> *What are the key information security risks within connected cars deriving from the in-vehicle network architecture and how can they be mitigated?*

The most important information security risk is that all in-vehicle networks are somehow connected. Due to the large amount of nodes on all the networks it is very likely that a single node will be breached some day. With such a large amount of source code inside all the embedded systems, this presents potential threats in a modern vehicle.

This serves as catalyst for other problems. When a single ECU is breached due to a vulnerability in its software, no real risk emerges. However, when this node is able to communicate with all other nodes and starts propagating malicious commands a big problem arises. Further research is needed to develop and test a new vehicular network, in the meantime car manufacturers should keep their software as secure as possible and should prepare their responses for another car hacking event.

6.3 Limitations and Validity

In this section we will elaborate on possible limitations and threats to the validity to this study. The field of automotive security is far from mature and is rapidly evolving. This reflects on the amount of high quality scientific papers available and thus on the corpus of articles that we selected for this study.

Within this study there are some threats to validity. Firstly, the literature review was conducted by a single author, this might result in misinterpretation or biases. Although we used well established research methodologies and qualitative methods to validate our results errors in judgment are possible.

In our focus group all subject matters experts work at Deloitte, this might affect their judgment in certain ways. Furthermore, the focus group was led by a single researcher, ideally one would also have a facilitator present. Other threats to validity within our focus group are *compliance* and *identification*. In the former a participant answers in a way that the moderator expects, where in the latter a participant responds similar to another person in the group.

Furthermore, we modeled the in-vehicle network as accurately as possible based on the sources available. However the field of vehicular networking is relatively young and is progressive at a high pace. Therefore, some information might not be as accurate as hoped.

This thesis presented a high level overview of the risks involved in automotive networking and how they impact the information security. Therefore, we do not claim that the vulnerabilities, risks and mitigation identified are exhaustive, they rather give an overview of important aspects and aid in prioritizing actions for Deloitte and possibly car manufacturers.

As mentioned earlier, the results of this thesis are generalizable within the domain of autonomous vehicles since they work in a similar manner as Connected Cars.

6.4 Contributions

Within this thesis we systematically investigated the information security risk within connected cars. By studying the network architecture vulnerabilities we derived risks to the information security. Subsequently these vulnerabilities and risks were mapped onto our model in ArchiMate^{TM} to illustrate the origin of these risks.

Furthermore, we linked these risks to mitigation strategies and came up with recommendations for the automotive sector. No other study provides this connection between vulnerabilities, risks, architecture and mitigative strategies. This contributes to the scientific corpus of articles on automotive security.

For Deloitte this study is relevant since it identifies business opportunities whilst keeping current propositions in mind. In this manner services can be altered slightly in order to better serve the automotive sector.

6.5 Recommendations

This section gives recommendations for both the automotive industry and for Deloitte. But firstly some general recommendations are made.

6.5.1 Automotive industry

There should be a serious joint effort by the automotive industry to develop new standards that are tailored to the automotive environment. This in order to develop a more resilient hardware structures that ensure separation between safety critical and non-safety critical networks. Furthermore attention should be paid to the quality of software. Improved testing and validation should be carried out before using the software in a production environment.

During our research a lot of things happened when it comes to connected car legislation. Due to recent hacks the topic of automotive security gained lots of momentum in the United States. Begin August a legislation was filed that would require the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to develop industry wide standards to improve security and privacy in cars.

6.5.2 Deloitte

Within Section 6.2 **RQ6** recommends business development activities for Deloitte. There is a variety of service lines that can easily start to serve the automotive industry. Think of *Crisis management & Incident Response*, *Hacking as a service* and *Secure by Design.*

These can all engage in aiding the automotive sector since Connected Cars require a multi disciplinary approach. Furthermore cars are also an element within the Internet of Things which is already researched at Deloitte. In time it is likely that a majority of devices will have similar issues in terms of security, privacy and data ownership.

6.6 Future work

Based on this study it is clear that the field of automotive security has not been studied sufficiently. Additional research is needed on how to segregate the safety-critical and non safety-critical networks. Can this be achieved softwarematically or is a physical disconnect (air gap) needed? Furthermore it is clear that the CAN bus contributes to a great amount of problems. Further testing is needed to see if Ethernet is a candidate to replace the CAN bus. Using a network that implements more layers in the OSI stack features such as addressing, transport security and reliable transfer. These features would greatly increase the resilience within vehicular networking.

For politics it is time to introduce more legislation on this matter. Within the United States autonomous cars are already permitted to drive in some states. However little attention is paid to the legal aspect. There is no clear legislation that state who or what is responsible when accidents happen. In order for connected cars to become the new normal within transportation these problems should be handled.

Appendix A

Search terms

1. *SCOPUS-CAR (24 results)*

   ```
   (TITLE-ABS-KEY ( connected  car  OR  smart  car  OR  autonomous
   vehicle ) AND TITLE-ABS-KEY ( risk*  OR  secur* ) )  AND
   DOCTYPE ( cp ) AND SUBJAREA ( mult  OR  ceng  OR  CHEM  OR
   comp  OR  eart  OR  ener OR engi  OR  envi OR  mate  OR math
   OR  phys  OR  mult  OR  arts  OR busi OR  deci  OR  econ  OR
   psyc  OR  soci )  AND  PUBYEAR  >  2009
   ```

Appendix B

Articles used

	Article
I.	Kleberger et al. (2011b)
II.	Schweppe and Roudier (2012)
III.	Gantsou and Sondi (2014a)
IV.	Kleberger and Olovsson (2013)
V.	Han et al. (2013)
VI.	Ring et al. (2014)
VII.	Bouard et al. (2013)
VIII.	Jakob et al. (2012)
IX.	Sagstetter et al. (2013)
X.	Koscher et al. (2010)
XI.	Markelj and Bernik (2011)
XII.	Zhang et al. (2011)

Appendix C

Vulnerability description

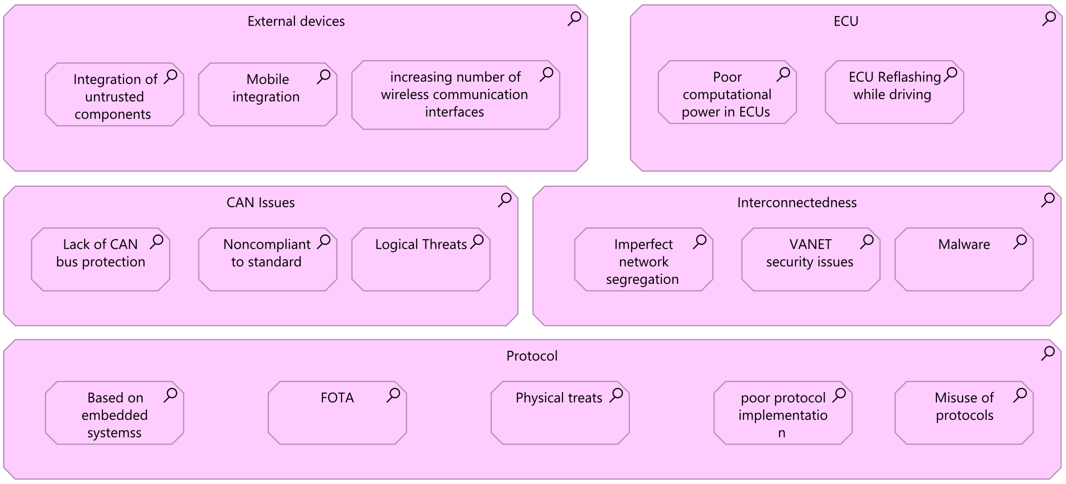
Vulnerability	Explanation
Integration of untrusted components	An information leakage from the vehicle can be triggered by manipulating the diagnostic protocol, creating a potential privacy violation
ECU reprogramming	It is possible to illicitly reprogram ECUs with new firmware
Lack of CAN bus protection	The CAN-bus lacks necessary protection to ensure confidentiality, integrity, availability, authenticity, and non-repudiation. Messages on the CAN-bus can be read by other nodes, have no sender or receiver address, and are not protected by any Message Authentication Code (MAC) or digital signature.
Poor protocol implementation	In some cases the protocol implementation is such that it does not properly reflect the protocol standard. For example, the standard specifies that it should not be possible to put the Engine Control Module (ECM) into programming mode while the vehicle is moving.
Firmware update Over-The-Air	Equipping the vehicle with a wireless connection will create many opportunities for new services, e.g. firmware update over the air (FOTA) and remote diagnostics. However, those very attractive features come with great challenges.
Misuse of protocols	For the CAN protocol, a Denial-of-Service (DoS) attack may be carried out using the bus arbitration mechanism
Non-compliant to standard	While the telematics unit is not technically a gateway, it connects to both networks and can only be reprogrammed (against the spirit of the standard) from the low-speed network
Imperfect network segregation	Once reprogrammed, our telematics unit acts as a bridge, relaying packets from the lowspeed bus onto the high-speed bus. This demonstrates that any device attached to the low-speed bus can bypass the BCM gateway and influence the operation of the safetycritical components.
Physical treats	An attacker is assumed to be able to steal diagnostics equipment, which is able to authenticate itself properly to any vehicle at any time.

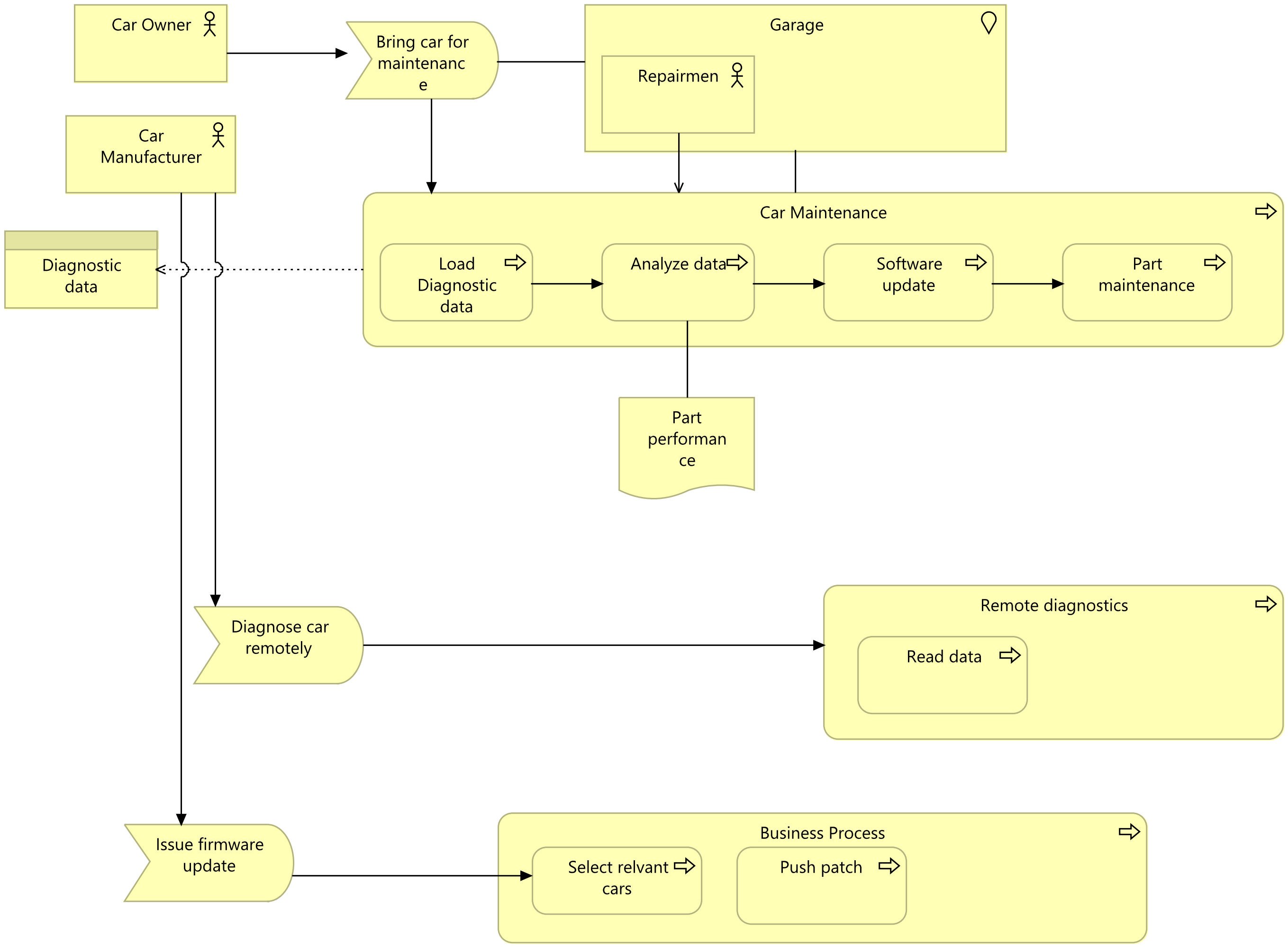
Continued on next page...

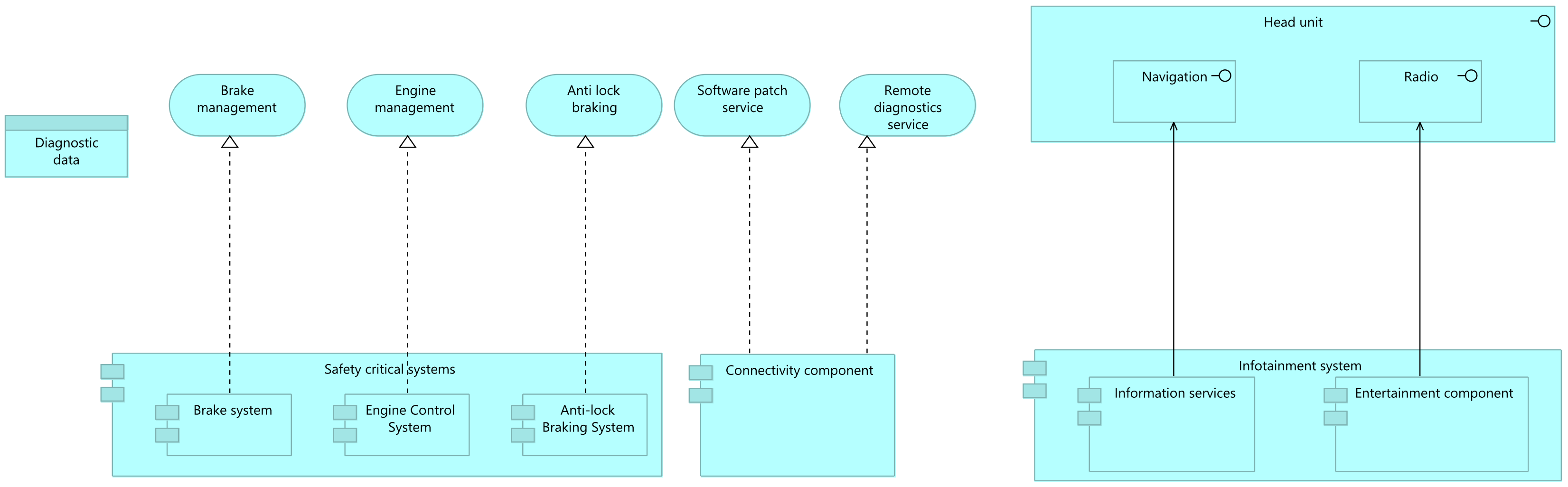
Vulnerability	**Explanation**
Logical treats	An attacker is assumed to be able to copy the authentication keys within the diagnostics equipment. It is then possible to use/have any type of equipment to authenticate as diagnostics equipment to any vehicle at any time.
Poor computational powers	ECUs do not have the computational power to support cryptographic functions.
VANET security	This gateway between vehicles and external resources may lead to security attacks that could have a greater impact than on conventional information technology systems. Therefore, prevention and early detection of attacks are essential.
Mobile integration	Increasing complexity in ICT systems and automotive electronics as well as the increased integration of vehicle networks with ICT networks lead to increased IT security risks for the consumer.
ECU Re flashing while driving	Many of the vulnerabilities we discovered were made possible by weak or unenforced protections of the diagnostic and reflashing services.
Based on embedded systems	A typical on-board architecture of vehicles, that we describe in more detail in the following section, is based on paradigms from the embedded world and thus allows little room for additional security features by means of processing power and bandwidth
Increasing number of wireless communication interfaces	Especially the increasing number of wireless communication interfaces lead to the fact that the attack surface of a modern car has increased quite dramatically
Trojans & Malware	Currently trojans, eavesdropping software, rogue software, etc have become increasingly rampant

Appendix D

ArchiMate$^{\mathrm{TM}}$ Model


External devices
Integration of untrusted components
Mobile integration
increasing number of wireless communication interfaces
ECU
Poor computational power in ECUs
ECU Reflashing while driving
CAN Issues
Lack of CAN bus protection
Noncompliant to standard
Logical Threats
Interconnectedness
Imperfect network segregation
VANET security issues
Malware
Protocol
Based on embedded systemss
FOTA
Physical treats
poor protocol implementatio n
Misuse of protocols


Car Owner
Bring car for maintenanc e
Garage
Repairmen
Car Manufacturer
Car Maintenance
Diagnostic data
Load Diagnostic data
Analyze data
Software update
Part maintenance
Part performan ce
Diagnose car remotely
Remote diagnostics
Read data
Issue firmware update
Business Process
Select relvant cars
Push patch


Diagnostic data
Brake management
Engine management
Anti lock braking
Software patch service
Remote diagnostics service
Head unit
Navigation
Radio
Safety critical systems
Brake system
Engine Control System
Anti-lock Braking System
Connectivity component
Infotainment system
Information services
Entertainment component

Bibliography

Ross Anderson and Tyler Moore. Information security: where computer science, economics and psychology meet | Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, June 2009. URL http://rsta.royalsocietypublishing.org/content/367/1898/2717.

Iver Band, Wilco Engelsman, BiZZdesign Christophe Feltus, Sonia González Paredes, and Dux Diligens. Modeling Enterprise Risk Management and Security with the ArchiMate®. 2015. URL https://pure.fundp.ac.be/portal/files/12366722/Modeling_Enterprise_Risk_Management_and_Secutity_with_the_ArchiMate_Language.pdf.

Paul L. Bannerman. Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, 81(12):2118–2133, December 2008. ISSN 01641212. doi: 10.1016/j.jss.2008.03.059. URL http://linkinghub.elsevier.com/retrieve/pii/S0164121208000897.

Barry Boehm. *Software risk management*. Springer, 1989. URL http://link.springer.com/chapter/10.1007/3-540-51635-2_29.

Bosch. OSI Layers in Automotive Networks, March 2013. URL http://www.ieee802.org/1/files/public/docs2013/new-tsn-diarra-osi-layers-in-automotive-networks-0313-v01.pdf.

Alexandre Bouard, Benjamin Weyl, and Claudia Eckert. Practical information-flow aware middleware for in-car communication. pages 3–8. ACM Press, 2013. ISBN 9781450324878. doi: 10.1145/2517968.2517969. URL http://dl.acm.org/citation.cfm?doid=2517968.2517969.

Brian Bramer. Local Area Networks, 2003. URL http://www.cse.dmu.ac.uk/~bb/Teaching/NetWorks/LANS/LANS.htm.

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, and others. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In

USENIX Security Symposium. San Francisco, 2011. URL `http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf`.

Cognizant. Exploring the Connected Car. Technical report, November 2012. URL `http://www.cognizant.com/InsightsWhitepapers/Exploring-the-Connected-Car.pdf`.

Cornell University Law School. 44 U.S. Code § 3542 - Definitions | LII / Legal Information Institute, December 2002. URL `https://www.law.cornell.edu/uscode/text/44/3542`.

John W Creswell. Mixed-method research: Introduction and application. *Handbook of educational policy*, pages 455–472, 1999.

Deloitte. Annual Report 2013-2014, 2014. URL `http://2013-2014.deloitteannualreport.nl/fbcontent.ashx/downloads/2013-2014/Annual_report_2013_2014.pdf`.

Delphi. Delphi set to acquire connection systems maker - automotiveIT International, 2012. URL `http://www.automotiveit.com/delphi-set-to-acquire-connection-systems-maker/news/id-005927`.

Larry Dignan. AT&T adds 684,000 connected cars in Q1, April 2015. URL `http://www.zdnet.com/article/at-t-adds-684000-connected-cars-in-q1/`.

Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering*, pages 289–306. Springer, 2010. URL `http://link.springer.com/10.1007/978-3-642-12544-7_16`.

Forbes. Connected Cars By The Numbers, January 2015. URL `http://www.forbes.com/sites/niallmccarthy/2015/01/27/connected-cars-by-the-numbers-infographic/`.

Fujitsu. Next Generation Car Network - Flexray. Technical report, June 2006. URL `http://www.fujitsu.com/downloads/CN/fmc/lsi/FlexRay-EN.pdf`.

Dhavy Gantsou and Patrick Sondi. Toward a honeypot solution for proactive security in vehicular ad hoc networks. In James J. (Jong Hyuk) Park, Ivan Stojmenovic, Min Choi, and Fatos Xhafa, editors, *Future Information Technology*, volume 276 of *Lecture Notes in Electrical Engineering*, pages 145–150. Springer Berlin Heidelberg, 2014a. ISBN 978-3-642-40860-1. doi: 10.1007/978-3-642-40861-8_22. URL `http://dx.doi.org/10.1007/978-3-642-40861-8_22`.

Dhavy Gantsou and Patrick Sondi. Toward a Honeypot Solution for Proactive Security in Vehicular Ad Hoc Networks. In James J. Park, Ivan Stojmenovic, Min Choi, and Fatos Xhafa, editors, *Future Information Technology*, volume 276, pages 145–150. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014b. ISBN 978-3-642-40860-1, 978-3-642-40861-8. URL `http://link.springer.com/10.1007/978-3-642-40861-8_22`.

Gartner. Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities, January 2015. URL `http://www.gartner.com/newsroom/id/2970017`.

Eric Grandry, Christophe Feltus, and Eric Dubois. Conceptual integration of enterprise architecture management and security risk management. In *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2013 17th IEEE International*, pages 114–123. IEEE, 2013. URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6690541`.

GSM Association. Technology Roadmap Connected Car Forecast, June 2013. URL `http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf`.

Hacking, Security, Cybercrime, Vulnerability, Malware, 400 from leak Ashley Madison hack miscreants may have earned $6, Malvertising attack menaces Match com users with tainted love, and IoT baby monitors STILL revealing live streams of sleeping kids. Samsung smart fridge leaves Gmail logins open to attack. URL `http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/`.

Kyusuk Han, S. Divya Potluri, and Kang G. Shin. On authentication in a connected vehicle: secure integration of mobile devices with vehicular networks. In *Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on*, pages 160–169. IEEE, 2013. URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6604010`.

Olaf Henniger, Ludovic Apvrille, Andreas Fuchs, Yves Roudier, Alastair Ruddle, and Benjamin Weyl. Security requirements for automotive on-board networks. In *Proceedings of the 9th International Conference on Intelligent Transport System Telecommunications (ITST 2009), Lille, France*, 2009. URL `http://www.cse.msu.edu/~cse435/Handouts/CSE435-Security-Automotive/Automotive-SafetyReqts-2009.pdf`.

Original created by JB Hewitt. English: OSI RM Model. Intent: This was created to clearly show layers in the OSI model., March 2005. URL `https://commons.wikimedia.org/wiki/File:Osi-model-jb.png`.

IBM. Driving security. Technical report, June 2014. URL `http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03610usen/GBE03610USEN.PDF`.

International Standards Organization. ISO/IEC 7498-1:1994 - Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, 1994. URL `http://www.iso.org/iso/catalogue_detail.htm?csnumber=20269`.

Felix Jakob, Wolfgang Kremer, Andreas Schulze, Jürgen Gro\s smann, Nadja Menz, Martin Schneider, and Alain-Georges Vouffo Feudjio. Risk-based testing of Bluetooth functionality in an automotive environment. In *Automotive-Safety & Security*, pages 211–228, 2012. URL `http://cs.emis.de/LNI/Proceedings/Proceedings210/211.pdf`.

Andy Jones and Debi Ashenden. *Risk management for computer security: protecting your network and information assets.* Elsevier, Amsterdam, 2005. ISBN 978-0-7506-7795-0.

H. Jonkers, E. Proper, M. M. Lankhorst, D. A. C. Quartel, and M. . Iacob. Archimate® for integrated modelling throughout the architecture development and implementation cycle. In *Proceedings - 13th IEEE International Conference on Commerce and Enterprise Computing, CEC 2011*, pages 294–301, 2011. URL `www.scopus.com`.

Eugene Kaspersky. Five Reasons Connected Cars Are A Security Issue, 2015. URL `http://www.forbes.com/sites/eugenekaspersky/2015/02/11/five-reasons-connected-cars-are-a-security-issue/`.

Barbara Kitchenham. Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, EBSE Technical Report EBSE-2007-01, 2007. URL `https://www.cs.auckland.ac.nz/~norsaremah/2007%20Guidelines%20for%20performing%20SLR%20in%20SE%20v2.3.pdf`.

Pierre Kleberger and Tomas Olovsson. Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties. In *Computer Safety, Reliability, and Security*, pages 70–81. Springer, 2013. URL `http://link.springer.com/chapter/10.1007/978-3-642-40793-2_7`.

Pierre Kleberger, Asrin Javaheri, Tomas Olovsson, and Erland Jonsson. A Framework for Assessing the Security of the Connected Car Infrastructure. In *ICSNC 2011, The Sixth International Conference on Systems and Networks Communications*, pages 236–241, 2011a. URL `http://www.thinkmind.org/index.php?view=article&articleid=icsnc_2011_10_30_20229`.

Pierre Kleberger, Tomas Olovsson, and Erland Jonsson. Security aspects of the in-vehicle network in the connected car. In *Intelligent Vehicles Symposium (IV), 2011*

IEEE, pages 528–533. IEEE, 2011b. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5940525.

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and others. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5504804.

Jeffrey Lange. Review: Richard a. krueger & mary anne casey (2000). focus groups. a practical guide for applied research (3rd edition). *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 3(4), 2002. ISSN 1438-5627. URL http://www.qualitative-research.net/index.php/fqs/article/view/791.

Left Lane. NHTSA Levels of Vehicle Autonomy Infographic, 2015. URL http://www.leftlaneadvisors.com/project/nhtsa-levels-of-vehicle-autonomy-infographic/.

Blaž Markelj and Igor Bernik. Accessing information systems with mobile devices and information security. In *Proceedings of the 2nd international conference on Applied informatics and computing theory*, pages 158–161. World Scientific and Engineering Academy and Society (WSEAS), 2011. URL http://www.wseas.us/e-library/conferences/2011/Prague/AICT/AICT-25.pdf.

Ed Markey. Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk. Technical report, 2015. URL http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

National Institute of Standards and Technology. SP 800-53 Rev. 3. Recommended Security Controls for Federal Information Systems and Organizations. September 2012. URL http://dl.acm.org/citation.cfm?id=2206266.

Nicolas Navet, Yeqiong Song, Francoise Simonot-Lion, and Cedric Wilwert. Trends in automotive communication systems. *Proceedings of the IEEE*, 93(6):1204–1223, 2005. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1435746.

Wanda J. Orlikowski and C. Suzanne Iacono. Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information systems research*, 12(2):121–134, 2001. URL http://pubsonline.informs.org/doi/abs/10.1287/isre.12.2.121.9700.

Donn B. Parker. *Fighting Computer Crime: A New Framework for Protecting Information.* John Wiley & Sons, Inc., New York, NY, USA, 1998. ISBN 0-471-16378-3.

Red Bend Software. Updating Car ECUs Over - The - Air (FOTA). Technical report, 2011. URL `http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf`.

Martin Ring, Tobias Rensen, and Reiner Kriesten. Evaluation of Vehicle Diagnostics Security–Implementation of a Reproducible Security Access. *SECURWARE 2014*, page 213, 2014. URL `http://www.researchgate.net/profile/Carlos_Westphall/publication/275463281_SECURWARE_2014_-_The_Eighth_International_Conference_on_Emerging_Security_Information_Systems_and_Technologies/links/553d04b70cf245bdd7696e3d.pdf#page=214`.

Florian Sagstetter, Martin Lukasiewycz, Sebastian Steinhorst, Marko Wolf, Alexandre Bouard, William R. Harris, Somesh Jha, Thomas Peyrin, Axel Poschmann, and Samarjit Chakraborty. Security challenges in automotive hardware/software architecture design. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 458–463. EDA Consortium, 2013. URL `http://dl.acm.org/citation.cfm?id=2485398`.

Hendrik Schweppe and Yves Roudier. Security and privacy for in-vehicle networks. In *Vehicular Communications, Sensing, and Computing (VCSC), 2012 IEEE 1st International Workshop on*, pages 12–17. IEEE, 2012. URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6281235`.

Till Steinbach, Hyung-Taek Lim, Franz Korf, Thomas C. Schmidt, Daniel Herrscher, and Adam Wolisz. Tomorrow's in-car interconnect? A competitive evaluation of IEEE 802.1 AVB and Time-Triggered Ethernet (AS6802). In *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, pages 1–5. IEEE, 2012. URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6398932`.

Steve G. Sutton and Vicky Arnold. Focus group methods: Using interactive and nominal groups to explore emerging technology-driven phenomena in accounting and information systems. *International Journal of Accounting Information Systems*, 14 (2):81–88, June 2013. ISSN 14670895. doi: 10.1016/j.accinf.2011.10.001. URL `http://linkinghub.elsevier.com/retrieve/pii/S1467089511000613`.

Telefonica. The 5 best and most demanded Connected Car features, May 2015. URL `https://m2m.telefonica.com/blog/the-5-best-and-most-demanded-connected-car-features`.

The European Union Agency for Network and Information Security. Risk Assessment — ENISA. URL `https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment`.

The Open Group. ArchiMate® 2.1 Specification, 2015. URL http://pubs.opengroup.org/architecture/archimate2-doc/.

P. J. M Verschuren and H Doorewaard. *Het ontwerpen van een onderzoek*. LEMMA, Utrecht, 2000. ISBN 978-90-5189-886-6.

Jane Webster and Richard T. Watson. Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly*, 26(2): 3, 2002. URL http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2625&context=misq.

Herb Weisbaum. What's the life expectancy of my car?, 2006. URL http://www.nbcnews.com/id/12040753/ns/business-consumer_news/t/whats-life-expectancy-my-car/.

Gerben Wierda. *Mastering ArchiMate*. R&A, The Netherlands, 2014. ISBN 978-90-819840-4-1.

Roel Wieringa. Relevance and problem choice in design science. In *Global Perspectives on Design Science Research*, pages 61–76. Springer, 2010. URL http://link.springer.com/chapter/10.1007/978-3-642-13335-0_5.

Wikipedia. Connected car, January 2015. URL http://en.wikipedia.org/w/index.php?title=Connected_car&oldid=644900017. Page Version ID: 644900017.

Steve Winterfeld and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Newnes, December 2012. ISBN 978-0-12-405181-2.

Wired. Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED, 2015. URL http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Marko Wolf, André Weimerskirch, and Christof Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, 2004. URL http://www-afs.secure-endpoints.com/afs/ece.cmu.edu/usr/tdumitra/18849/public_html/papers/wolf04_automotive_bus_security.pdf.

Joost F. Wolfswinkel, Elfi Furtmueller, and Celeste PM Wilderom. Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, 22(1):45–55, 2013. URL http://www.palgrave-journals.com/ejis/journal/v22/n1/abs/ejis201151a.html.

Hongliang Zhang. A redefinition of the project risk process: Using vulnerability to open up the event-consequence link. *International Journal of Project Management*, 25(7):

694–701, October 2007. ISSN 02637863. doi: 10.1016/j.ijproman.2007.02.004. URL `http://linkinghub.elsevier.com/retrieve/pii/S0263786307000452`.

Pengwei Zhang, Xiaojing Jiao, and Ruijin Zhou. Investigation of the Information Security in Mobile Internet. In *Advanced Research on Computer Science and Information Engineering*, pages 140–144. Springer, 2011. URL `http://link.springer.com/chapter/10.1007/978-3-642-21411-0_22`.