MASTER THESIS

SECURITY IN V2I PROJECTS

Incorporating Security into a Framework for Communication between Connected Cars and Infrastructure

LAURENCE ARNOLD
FACULTY: ELECTRICAL ENGINEERING, MATHEMATICS & COMPUTER SCIENCE (EEMCS)
PROGRAMME: MSC BUSINESS INFORMATION TECHNOLOGY
EMAIL: L.H.A.ARNOLD@ALUMNUS.UTWENTE.NL

GRADUATION COMMITTEE

DR. M. DANEVA
FACULTY OF ELECTRICAL ENGINEERING, MATHEMATICS AND COMPUTER SCIENCE (EEMCS)
DEPARTMENT: CYBERSECURITY & SAFETY

DR. A.I. ALDEA
FACULTY OF BEHAVIOURAL, MANAGEMENT AND SOCIAL SCIENCES (BMS)
DEPARTEMENT: INDUSTRIAL ENGINEERING & BUSINESS INFORMATION SYSTEMS (IEBIS)

DRS. M. M. J. PASCHEDAG CPO
ORGANISATION: NORTHWAVE
DEPARTEMENT: BUSINESS SECURITY

NORTHWAVE UNIVERSITY OF TWENTE.

PREFACE

A lot has changed in the last year. Although difficult to imagine a few years ago, my graduation took place via video conferencing, the new standard in 2020. However, to adapt ourselves to the new situation, we must be curious and open-minded. With this exact mindset, I started the master Business Information Technology in 2017 at the University of Twente, coming from Groningen.

This choice would turn out to be the right one. During my time in Enschede, I learned how to think critically and thoroughly conduct research. Above that, I have developed myself as a person I could not have imagined before I started my master in 2017. The result of all these developments is put into this master thesis.

The journey I have been through would not have been possible without the help and support of many persons. Here, I would like to express my gratitude towards all of them.

First of all, I want to sincerely thank my supervisors from the University of Twente, Maya Daneva and Adina Aldea. Even in the challenging times they faced, they tirelessly answered all my questions and supported me in creating this research, challenging me along the way and always giving me the power to make decisions myself, of which I learned the most.

Furthermore, I would like to thank my supervisor at Northwave B.V, where I executed my thesis. Marcel Paschedag, during all the conversations that we had, you provided me with many valuable insights of which I would have never thought of myself. In the meantime, you never failed to teach me several valuable life lessons.

Also, I would like to thank my colleagues at Northwave: you made my time at Northwave enjoyable and showed why this company is so full of great people. I really enjoyed the atmosphere and the useful feedback you provided me with. Besides, I would like to thank to all the participants in the conducted interviews and case study: without your time and expertise, this research would not have been the same.

Furthermore, I would like to emphasise the ever-lasting support of my parents, sisters, friends, and my girlfriend. The encouragement, endless support and motivation on which I can always rely upon, regardless of where my future lies: you know how important you are to me.

I hope you enjoy reading my research. If you have any questions, do not hesitate to contact me.

Laurence Arnold,

Gouda, October 5th, 2020

SUMMARY

Due to the increasing amount of IT in connected cars, the corresponding cybersecurity and privacy risks are also increasing. Through built-in systems, connected cars can communicate with external infrastructure like traffic lights and digital traffic signs. This form of communication is called Vehicle to Infrastructure (V2I). Currently, V2I is not yet available to the mass. In this phase where exploring functionality of V2I is the most important aspect, security can often be overlooked. There is no consolidated view of the state-of-the-art literature regarding security and privacy requirements in connected cars, as well as risk assessment approaches in the area.

This research aims to address this problem by proposing a framework specifically for handling security in V2I projects. The framework is aimed at both security consultants and project managers of V2I projects involved in security, to achieve an as secure V2I system as possible. The following aspects are processed in this framework, forming a coherent overview:

1. List of 9 vulnerabilities specific to V2I projects
2. List of attack methods corresponding to these vulnerabilities
3. Risk analysis of the vulnerabilities, including attack impact and attack likelihood. In total 4 risks are judged as critical, 4 major and one minor
4. Security requirements corresponding to the vulnerabilities
5. Measures originating from ITU, UNECE and ETSI mapped to the attack methods
6. Security requirements corresponding to these measures

The proposed framework was developed through the application of the Design Science Methodology of Wieringa (2014). Throughout this research, several research techniques were used, while definitions and security requirements were formed throughout a structured literature review, analysing a total of 52 papers. The literature review served to obtain 1) a comprehensive overview of the functionalities of the connected car in literature 2) what the security and privacy requirements are and 3) what the most suitable risk assessment framework is regarding connected cars.

Of the 15 papers about security requirement in connected cars, only two had relevance to V2I. The security requirements according to literature and European documentation are confidentiality, authentication, authorisation, integrity, availability and non-repudiation. These security requirements formed the base of our proposed framework. There were no specific privacy requirements found regarding V2I and therefore these were disregarded for the framework.

The framework is verified via a case study at Concorda, a project run at Rijkswaterstaat. Three security experts of both vendors and Rijkswaterstaat itself largely agreed that the main aspects of the framework being included would be useful in their work. The framework would especially be useful in future projects due to the current immature state of V2I.

The contributions of this research are manifold. For practitioners, this framework gives a comprehensive overview of the above-mentioned aspects by combining literature and existing documentation, raising awareness for security regarding both current and future projects in V2I to achieve 'security by design.' In terms of research, this research mainly identifies the lack of focus on specifically V2I projects in the connected car area, of which this research forms a base to work further upon.

Contents

List of Figures

List of Tables

1 INTRODUCTION

Personal transportation in the form of cars being connected to the internet becomes more and more common. These cars offer new functionalities like streaming services, real-time traffic information or even operating some functionalities remotely via an app. This makes connected cars more like a computer on the road. Today, cars can have up to 100 million lines of code, compared to a passengers aircraft which has 15 million code, a modern jet fighter with 25 million and an OS from a PC close to 40 million (Deichmann, 2019). It is also estimated that by 2020, 75% of cars will be built with the necessary hardware to connect to the internet (Coppola and Morisio, 2016).

The underlying theme behind these developments is computerisation: the more information is available and processed, the more useful it (potentially) is for car manufacturers. In our modern society, this theme often appears, with many of our day-to-day services being online. Connected cars will be an important part of this process with gathering, processing and distributing data to first and third parties. EU standards in the form of aspects like mandatory event data recorders, advanced emergency braking systems and 'advanced driver distraction warning systems' from May 2022 and onwards accelerate this movement towards computerisation.

Besides giving direct benefits to consumers in the form of more functions, connected cars can also communicate with external parties. All communication between connected cars and these external parties is called Vehicle to <X> (V2X) communication. V2X communication can be divided into several subcategories with different corresponding functionalities. The most important categories are V2V and V2I, as explained below:

- V2V: Vehicle to Vehicle communication between cars. This technology is important for self-driving cars in the future, when cars, for instance, arrange themselves who gives way or form certain closed trains by following each other (platooning) in order to drive as efficient as possible.
- V2I: Vehicle to Infrastructure communication and vice versa, directly between a built-in system in the car and external infrastructure like traffic lights, street lights, toll road ports, gates, and traffic signs communicate with (a group of) cars. V2I is also important for providing accurate information to self-driving cars, e.g. the condition of the road or which speed limit is set.

V2V and V2I can also work together. Connected cars can use V2V communication technology to talk to each other, exchanging essential safety data such as speed and position, real-time location services and routing based on traffic conditions, facilitating vehicle diagnostics, maintenance, leveraging vehicle-to-road infrastructure communication technologies (Möller and Haas, 2019).

V2I is already being tested in the Netherlands and gives functions like warnings via an build-in system of closed lanes on a highway, that an emergency vehicle is coming up or that you will shortly encounter a traffic jam (see Figure 1.1).

Figure 1.1: German example of V2I Communication built directly into a Car

From now on, in this research when referring to V2X, V2V or V2I communication, this means communication between both parties, and not only from Vehicle to <X>. This is to have a consequent definition throughout this report.

1.1 Background

Connected cars, and all their related services to security, efficiency, economic and environmental impact, are part of what is called an Intelligent Transport System (ITS). An ITS contains not only the cars, but also pieces of the road infrastructure (like traffic signs, toll collection machines or speed signs), which are connected via various networking and access technologies including the internet, public and private networks, Bluetooth, Wifi, cellular technologies, etc. (Coppola and Morisio, 2016), (Sabaliauskaite et al., 2018).

In C-ITS (Cooperative Intelligent Transport Systems), the service provision is enabled by the use of live data from other vehicles and infrastructure, which are implemented using V2V and V2I communications, collectively called V2X.

There are multiple definitions of the connected car. In this research, a merge from Möller and Haas (2019) and Coppola and Morisio (2016) is used to cover both what a connected car is and what the consequences are. This leads to the following definition:

> *The term connected car refers to the usage of car technologies making use of the internet by using a built-in connection, enabling the passengers of the vehicle to take advantage of numerous new services and functions.*

Examples of new services and functions are modern applications and dynamic contextual functionalities, offering advanced infotainment features to the driver and passengers. These applications and functionalities are part of the term ”telematics”. More on telematics in Chapter 3.

> *Telematics refers to the use of wireless components and technologies to transmit data in real-time within a network.*

1.2 Scope

The connected car can be distinguished by two categories: internal and external communication. Internal communication is the communication of the car with build-in systems like ECU's, brakes, steering, central locking, etc. This internal communication can be functional (as the previous mentioned examples are) and non-functional like self-driving aids (also called Advanced driver-assistance systems, ADAS, e.g. adaptive cruise control).

External communication is the communication between a connected car and external infrastructure, exchanging messages between each other. Another possibility with external communication is the communication from the build-in vehicle system to other parties, e.g. when using apps. This categorisation can be seen in Figure 1.2. In the systematic literature review in Chapter 3 the focus is solely towards external communication of connected cars, indicated by the black boxes in Figure 1.2.

Much existing research about security and connected cars focus on a specific technical solution of a connected car and how this can be made as secure as possible. This research, however, will not take that direction and therefore not focus on internal communication of connected cars (indicated by red in Figure 1.2).

This thesis will 1) focus on security in combination with the functionalities in external communication of connected cars and 2) focus on the combination of the management of security and the technical implementation. Therefore how certain requirements or measures are implemented is not part of this research. Furthermore, the focus lies primarily on the external communication side, i.e. sending and receiving data between the car and other parties.

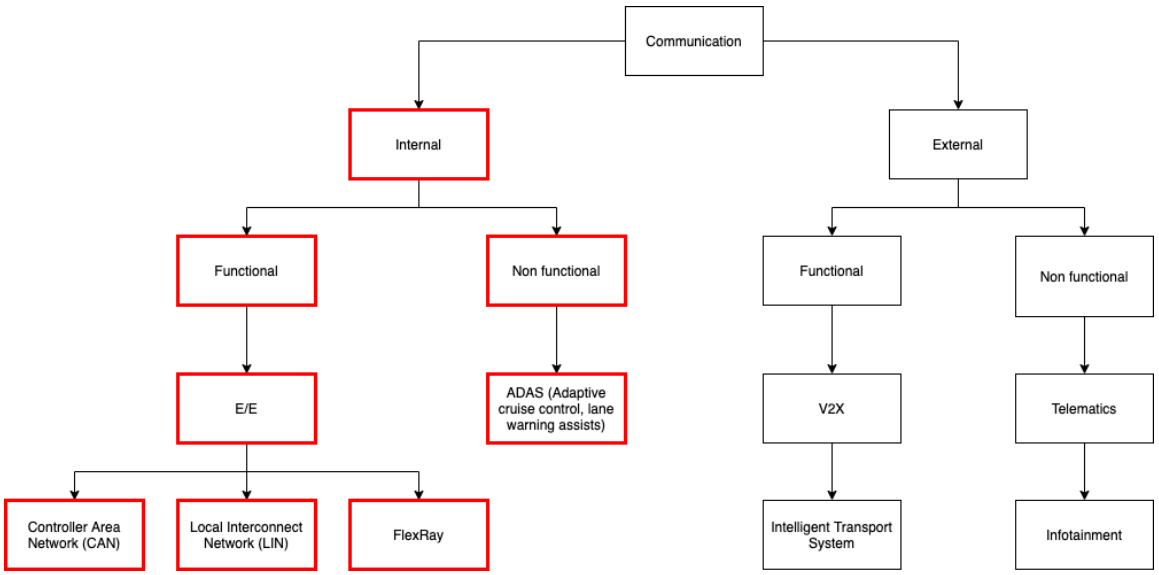

Figure 1.2: Categorisation of Connected Cars

Zooming in on external communication, two categories can be distinguished: functional and non-functional communication. In Chapter 3 both functional and non functional communication is analysed. After that, the remaining chapters will focus on V2X and especially V2I communication. This is done because first a comprehensive picture of the connected car as a whole was to be studied before certain aspects could be picked to elaborate upon for the framework.

Lastly, the focus of this research is towards the European market in regard to existing legislation / standards, because there is too much difference between (to be published) standards of other parts of the world to get a coherent view of all existing standards regarding V2X.

1.3 Problem Statement

Research involving automotive security is becoming increasingly important as rapid advances are being made in the digitisation of cars, as mentioned above. Driverless vehicles, over-the-air firmware updates, vehicle-to-vehicle communication, and the collection/storage of private information by the automobile are all part of this development (Möller and Haas, 2019).

This development of making cars more and more digital and sophisticated offers new challenges. An aspect that can be often overlooked in this relatively new and fast developing area, where functionality is key, is cybersecurity. This research aims to address this problem.

The advances in wireless networks of connected cars have a negative impact due to the emergence of new types of cyberattacks. Therefore, cybersecurity is becoming a key issue with the main objectives of detecting, deterring, and averting vulnerabilities.

Cybersecurity is the body of technologies, processes, and practices designed to protect computers, data, networks and programs against intrusion, damage, or unauthorised access by cyberattacks (Möller and Haas, 2019).

Examples of connected cars being hacked / attacked can be found, but are not widespread (yet). We found two well-known examples: white-hat hackers found 14 vulnerabilities in the vehicles of a European premium-car maker in 2018, while Jeep recalled approximately 1,4 million cars in 2015 as one of the first cases involving automotive cybersecurity (Möller and Haas, 2019).

Currently, there is no standard for the car industry for dealing with cybersecurity, although regulators are preparing minimum standards for vehicle software and cybersecurity (Macher et al., 2017). Examples are the upcoming ISO 21434 standard, while the World Forum for Harmonisation of Vehicle Regulations under the United Nations Economic Commission for Europe (UN-ECE) is expected in 2020 to finalise its regulation on cybersecurity and software updates.

This research aims to fill this gap between (closed source) the not yet published standards and security in a comprehensive and publicly available way, focusing on specifically V2I communication. The reason why the created security framework of V2I will differ from existing security standards of connected cars or autonomous vehicles is because of the involved parties involved in these aspects. Communication data between infrastructure and the vehicle involves two parties who have an influence on security, whereas with a self-driving vehicle driving only the manufacturer of the car is involved. Also, the transferred data with V2I is different from V2V, with V2I purely focusing on the functional aspect, while the manufacturer of a connected car can also communicate non-functional aspects, like how often the horn is used, how much a driver brakes, etc.

1.4 Research Objective

The primary objective of this research is to make a scalable and up-to-date framework regarding security and V2I by combining multiple (research) sources and executing a risk analysis. This is to have a better understanding of what security involves in current and future V2I projects and how this can be best handled in order to have an as much as secure V2I system. To fulfil this primary objective, secondary objectives like the gathering of security requirements by combining literature with European documentation, vulnerabilities of V2I projects with a risk assessment, attack methods and measures are also included in this research.

In order to get a clear picture of the to be designed artefact and its goal, the design science methodology of Wieringa (2014) is used. The template for this methodology is as shown below, followed by the mapping to the context of this research:

improve	< a problem context >
by	< (re)designing an artefact >
that satisfies	< some requirements >
in order to	< help stakeholders achieve some goals >

improve	< the security of V2I projects >
by	< designing a framework >
that satisfies	< identified security requirements on a data level >
in order to	< support current and future V2I projects in a fast moving environment >

1.5 Research Questions

Due to the quickly changing developments from the market and, as stated before, the lack of existing literature regarding specifically V2I, a state of the art and scalable framework for V2I will be developed in this thesis. The framework will encompass the scope of V2I and a suitable risk analysis, taking into account corresponding security requirements and existing European standards combined with literature. This leads to the following main research question:

> How can current and future V2I projects deal with security requirements regarding communication with connected cars?

With the addition of 'regarding communication of connected cars' we mean that we look at the security aspect between infrastructure and connected cars, and not focus on how security at the V2I project internally is arranged, i.e. components from a project communicating with each other.

This main research question is decomposed into the following seven research questions (RQ's):

Sub questions:

1. What specific security and privacy requirements do connected cars, including V2I projects, have?

   1.1. What types of external connectivity functions are present in connected cars according to literature?

   1.2. What cybersecurity requirements for connected cars and specifically V2X are discussed in literature?

   1.3. What privacy requirements for connected cars and specifically V2X are discussed in literature?

   In order to know what aspects of security are important to connected cars, first an accurate picture of what external connectivity functions connected cars are according to literature has to be created. This is done in research question 1.1. Another goal is to see whether there is a relationship between specific functionalities and security requirements. After that, security and privacy requirements of connected cars are gathered, with a focus towards V2X communication.

2. What is the current state-of-the-art in literature regarding assessing cybersecurity and privacy risks in the automotive area?

   2.1. What is the most suitable framework for a risk assessment of V2I projects?

   In order to execute a risk analysis of V2I projects, a suitable risk assessment framework has to be found and selected. This is the aim of research question 2 and 2.1. The risk

analysis itself will be executed in research question 4.

3. How does existing European documentation regarding security in V2I collaborates to the identified security requirements in literature?

   Current European documentation are also analysed to get a comprehensive picture of V2I and security and what documentation already exists. All this documentation is used as input for the final framework.

4. What are the most important risks an V2I project is exposed to regarding communication on a data level?

   As explained above, in this RQ we will execute the risk analysis, with the outcome a list of ordered risks regarding V2I projects.

5. How can potential measures in V2I projects be mapped to specific security requirements?

   The base of the framework are security requirements gathered from RQ 1 and RQ 3. These identified security requirements have to be mapped to measures being found in documentation. This research question describes how this process is being done.

6. How can the identified security requirements, risks and measures contribute to a scalable and up-to-date guideline for V2I projects regarding security requirements?

   In this research question the final deliverable (i.e. the framework) is presented by combining the above RQ's. With scalable we mean that our framework should be fitting to multiple kinds of V2I projects which receive and send messages to / from connected cars, while with up-to-date we aim that our framework can be used for both current and future V2I projects.

7. How can the proposed framework be applied and evaluated for the Dutch market?

   In this research question we validate our framework. We chose specifically for the Dutch market since in this country there are already some existing projects / pilots concerning communication with connected cars with e.g. traffic lights / other external infrastructure, e.g. Talking Traffic or Concorda. Talking Traffic encompasses multiple Dutch projects run with traffic lights, traffic flows or when to join the highway coming from a slip road (Dynniq, 2019). In this research question we verify whether our created framework fits with one of these existing projects.

The relationship between all research questions and chapters can be seen in Figure 1.3.

1.6 Research Design

Throughout this research, the design cycle of Wieringa (2014) will be used. This design cycle comprises of three main steps for the development of artefacts, i.e. the methodology (see also Figure 1.4).

The goal of the first step, 'problem investigation', is to 'investigate an improvement problem before an artefact is designed and when no requirements for an artefact have been identified yet' (Wieringa, 2014). The first tasks in this step include the identification, description, explanation and evaluation of the to be treated problem.

The following phase, 'treatment design' comprises the process of designing the actual research artefact. Finally, the third phase of the design cycle serves to validate whether the artefact can help to achieve the previously set goals. The treatment implementation and implementation

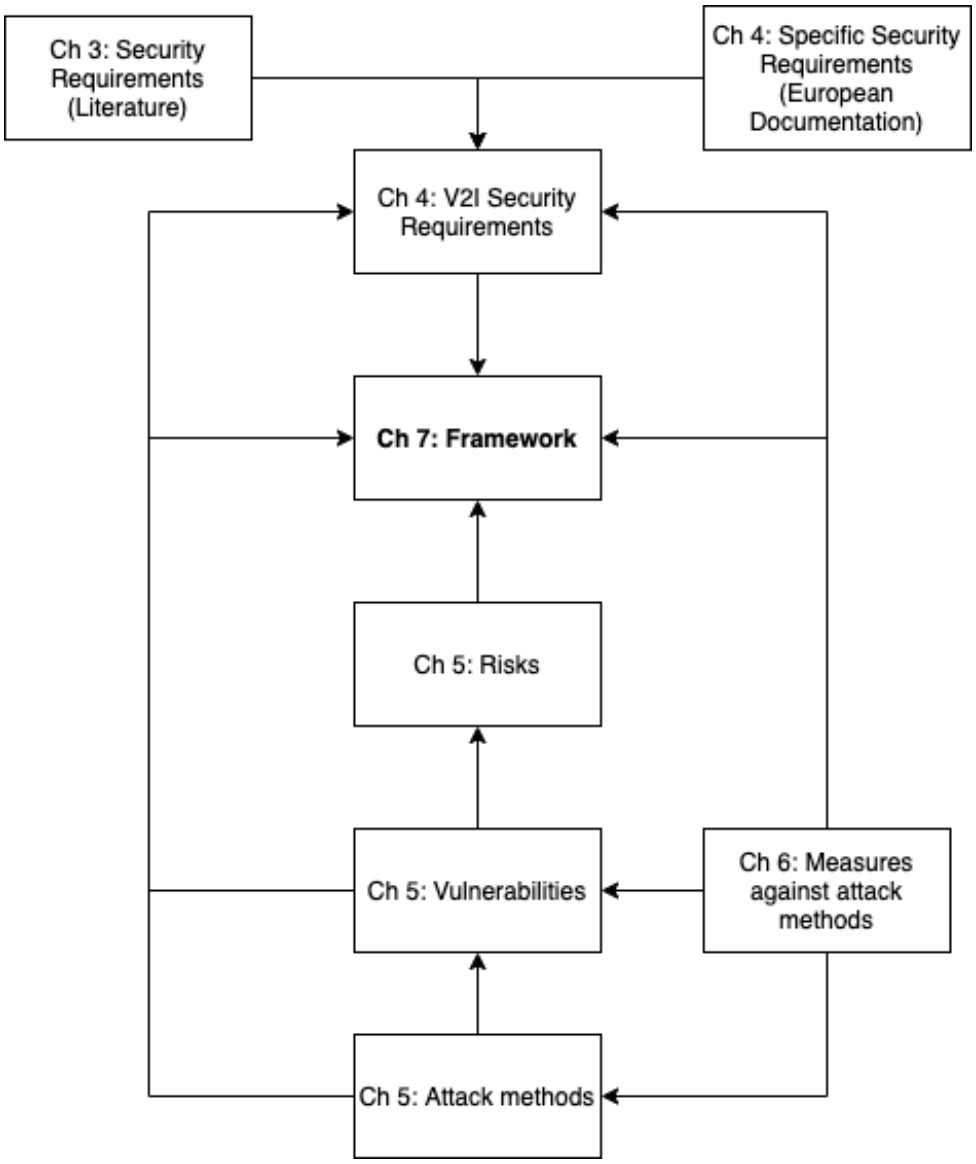

Figure 1.3: Relations of Research Questions to Chapters to Final Artefact

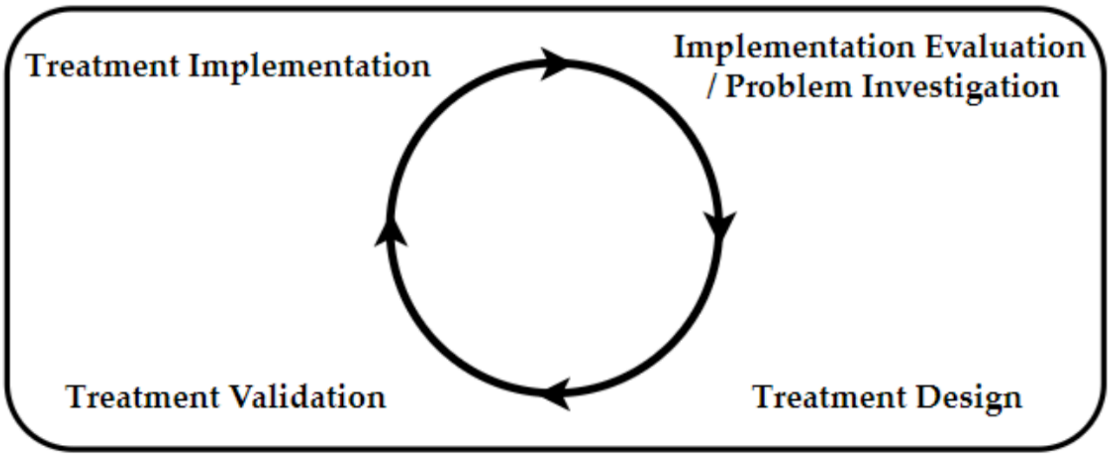

Figure 1.4: Engineering Cycle of Wieringa (2014)

evaluation are not relevant due to the implementation of the artefact in practice which is out of scope for the thesis. The design cycle could be referred to as a 'higher-level' research process, where essential steps for design science research are proposed.

Mapping these three steps to this research, in the problem investigation we first determine what security requirements for connected cars are necessary (RQ 1), together with a risk analysis needing to be held (RQ 2 + 4). An improved version specifically for V2I is going to be developed.

With the outcome of this analysis, the requirements can be compared to how V2I projects handle security (RQ 3). An important subpart is to map the taken security measures of these projects to specific requirements (RQ 5). If it turns out these projects do not hold any standard, a proposal for such a standard regarding security requirements can be developed based on literature and (recent) European legislation.

In RQ 6 the framework will be designed (i.e. the treatment design), which takes into account the before identified requirements for V2I projects. This framework will be combined with the before designed risk analysis and will be verified on a existing V2I project to verify its contribution to practice in RQ 7 (the treatment validation).

1.7 Thesis Structure

As can be seen in Figure 1.3, the base for the framework are the security requirements. These are derived from both literature and European standards. After that, the vulnerabilities, corresponding attack methods and measures are outlined. The attack methods and vulnerabilities are used as input for the risk analysis, which in turn is the next building block for the framework. Note that the risks themselves are not directly coupled to the security requirements. However, these risks are based upon both vulnerabilities and attack methods which are based on security requirements. Therefore the risks and security requirements can be coupled to each other but this is not explicitly done in this research or framework.

Table 1.1: Mapping from Design Science Methodology (DSM) to Structure of Thesis

DSM Activity	**Description**	**RQ's**	**Chapter**	**Research Technique**	**Outcome**
Problem investigation	Identify research problem, context and stakeholders	1 - 2	1 - 3	Literature Review	• Scope of artefact • List of Security Requirements mentioned in literature • Risk Analysis framework for V2X
Treatment design	Desired elements for the artefact in order to contribute to stakeholders goal	3 - 6	4 - 7	• Analysis of existing European V2X standards • Interviews • Situational Method Base Engineering	• Specific security requirements for V2I • List of vulnerabilities and risks • List of attack methods • List of corresponding mitigations
Treatment validation	Validate artefact in context to justify it contributes to stakeholder goals	7	8	Surveys	Evaluation of designed framework in practice with strengths and weaknesses

Also, the mitigations are mapped to attack methods but not directly to vulnerabilities. This is because a vulnerability exists of multiple attack methods to be potentially exploited. Therefore a single measure will not stop a vulnerability. Furthermore, some attack methods belong to multiple vulnerabilities, making it more difficult to implement all measures. However, once

this is once done, this also means the vulnerability is no longer in place, but only then in this hypothetical scenario.

First, this research will start with the explanation of the methodologies of the systematic literature research and the components of the framework in Chapter 2. After that, the systematic literature review with the scope of connected cars (as explained above) is presented in Chapter 3. Consequently, the security requirements of European standards of V2I projects are explained in Chapter 4, followed by the vulnerabilities of V2I projects in Chapter 5 and the mapping of measures against the vulnerabilities via security requirements in Chapter 6.

In Chapter 7 the final artefact in the form of the framework is presented where the validation is being done in Chapter 8. Finally, the discussion and conclusions of this research are presented in Chapters 9.2 and 9, respectively.

Note that whenever you encounter a reference to a source, a chapter, section, table, figure, image or an Appendix, you can click on this reference and you will automatically move to the corresponding part in the document.

2 RESEARCH METHODS

In this chapter, the research methods regarding four major parts of this research are described. First, we explain the systematic literature review we executed and how we have achieved this. After that, we explain the steps in developing the final framework of this thesis. Here, we have a sub-step explaining how we set up and processed the results of the interviews we held. Third, in our case study where we validate the framework, we explain both the set up of the case study and the validation process.

2.1 Literature Review

In this section the research methodology applied throughout our systematic literature review is discussed.

Considering that the (academic) field of connected cars is rapidly involving and the development only accelerates in the upcoming years, the availability of generally accepted academic articles is expected to be scarce. Therefore, it is important to obtain a current overview of the available literature. To ensure comprehensiveness and repeatability, a scientifically systematic approach can prove highly valuable. The created approach below is based on Kitchenham and Charters (2007), Bandara et al. (2015), Webster and Watson (2002) and Okoli (2015). Accordingly, the review documented in this report follows the guidelines of a systematic literature review. In the next sections, the protocol, prescribing the undertaken steps of the review, are discussed. In addition, the applied strategies and search criteria are covered in this chapter.

2.1.1 Pre-mapping

As suggested by Kitchenham and Charters (2007) a pre-review mapping study can be conducted to help in scoping the research questions. To execute this pre-mapping two steps are taken. First, the book of Möller and Haas (2019) named 'Guide to Automotive Connectivity and Cybersecurity' is read to identify relevant aspects in the connected car. Secondly, unstructured interviews with four experts in the automotive area are held. These experts ranged from training (international) mechanics for car manufacturers, to extract data from the OBD port of cars in order to help car garages to fix cars, to a former IT engineer working between the Enterprise Resource Planner (ERP) of car manufacturers and car dealers / importers of cars. These interviews were not structured nor recorded. The target of every interview was to see which aspects in the automotive industry play a part in practice and how people envision the connected car of today / the future and whether they had any aspects to add which are not mentioned in the book of Möller and Haas (2019).

This initial pre-mapping leads to the choice of focusing on external communication, specifically both telematics and V2X communication in connected cars, instead of infrastructural aspects like the CAN (Controller Area Network) Bus, the manufacturing process or the (informational) architecture of connected cars. Although these aspects are relevant in the overall process

of achieving and maintaining a high standard in security risks and privacy, the CAN Bus and manufacturing process are well defined and researched and have remained relatively static over the past years. The informational architecture is still relevant for cybersecurity but more from a structural perspective, whereas this research will focus on information security, not a product-specific perspective. In contrast, the telematics and V2X side is confirmed in the interviews as being relevant and relatively unknown due to the fast developments the past years. In Figure 2.1 the chosen scope of this research can be seen after the pre-mapping. Red indicates out of scope.

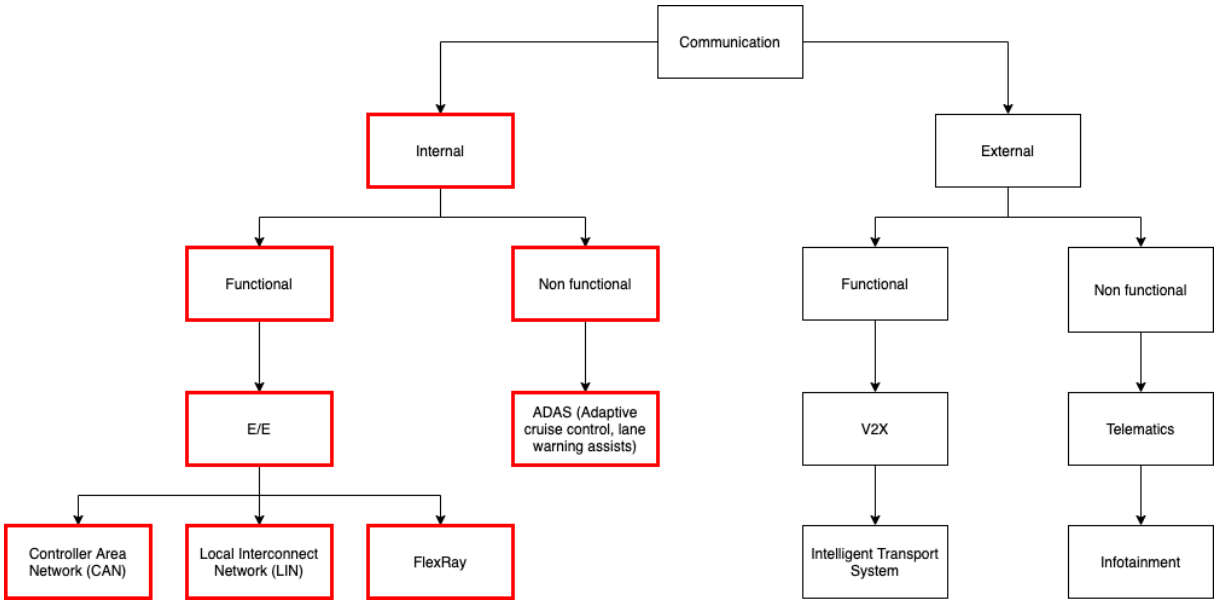

Figure 2.1: Scope of Research

An aspect which arose from the interviews is (the lack of) international standards. Car manufacturers are currently not obliged to follow any standard which improves cybersecurity or privacy, although such standards are in development / being monitored by authorisations (as mentioned in the interviews). Examples are the TISAX norm, ISO 26262 and ISO 21434. Also, the GDPR law came forward but one expert mentioned he is 'sure' car manufacturers are not complying to this law at the moment.

2.1.2 Selection of Sources

Automotive connectivity and cybersecurity is a multidisciplinary domain, founded in computer science, systems and software engineering, mechanical engineering, simulation science, and communications engineering as well as electronics (Möller and Haas, 2019). This requires a multidisciplinary approach when using different sources to find relevant literature.

In an attempt to perform an exhaustive literature search, the article of Kitchenham and Charters (2007) lists several electronic sources, supplemented with additional sources of Okoli (2015). The final list of used search engines is:

- Scopus
- ScienceDirect
- IEEExplore
- Springerlink
- ACM Digital Library

2.1.3 Search Strategy

The search strategy is be based on the research questions. Per RQ different keywords are used. After a trial search with the five selected sources, the exact scope of every search term was determined by analysing at the number of the search results. This way the search terms are updated until for every term a manageable sample is left.

In the list below you can see the definitive search terms per RQ. The title and abstract are searched in every search engine via advanced search and the usage of booleans. If the title and abstract are connected via an 'AND' statement (as is the case with Springer) the most important term of the query is required in the title, i.e. automotive or connected car. If the title and abstract are searched via separate fields (and therefore an OR statement) the same terms and booleans for both the title and abstract are used for consistency. In Scopus and ScienceDirect the keywords of the article are also searched upon.

Via booleans and wildcards the search terms below are used in order to narrow down the results. The used wildcard for * is to catch both the singular and plural. This holds true for all the terms of which singular and plural are applicable, e.g. connected car / connected cars (which also resulted in a few articles with the term connected care), system/systems, framework/frameworks, etc.

- RQ 1.1
  - ”Connected car*” AND (features OR possibilities)
  - (“Connectivity features” OR “Connectivity functions”) AND automotive
  - (”Infotainment system*” OR Telematics) AND ”Connected car*”
  - “Connected car*” AND “Vehicle communication system*”
- RQ 1.2
  - ”Cyber security” AND (Automotive OR ”Connected Car*”)
  - ”Cyber security” AND (”ISO 26262”)
  - ”Cyber security” AND (”connected car*” OR automotive) AND (standard OR framework)

The ISO 21434 ('Road vehicles — Cyber security engineering') is also searched for but no direct results could be obtained. However, via the other search terms, two relevant articles about this ISO standard are obtained and therefore included in this literature review. Also the term 'cyber security requirement*” is used but returned no results, therefore omitted from the terms stated above.

- RQ 1.3
  - ”Connected Car*” AND (Privacy OR GDPR)
  - ”Connected Car*” AND (”data gathering” OR ”big data”)
  - ”Connected Car*” AND ”privacy requirement*”
  - ”Privacy” AND ”Connected car*” AND (”standard*” OR ”framework*”)

GDPR was added to the first search query due to the pre-mapping where this law is mentioned in relation to privacy.

- RQ 2

- ("Risk Analysis" OR "Risk Assessment framework" OR "Classification Framework") AND (Automotive OR "connected car*" OR "Connected vehicle*")
- ("Cyber Security Assessment" OR "Cyber security analysis") AND (Automotive OR "connected car*" OR "Connected vehicle*")
- ("Privacy analysis" OR "Privacy Assessment") AND (Automotive OR "connected car*" OR "Connected vehicle*")

The reason for including connected vehicle (which could be any motorised vehicle like a truck or motorcycle) in every second part of the query is because RQ4 has a broader focus than the other RQ's. This is the case when looking for risk analysis frameworks / methods, etc. Here the results from Springerlink are omitted since the search form did not pick up the requested queries, resulting in exactly 1980 results for every query of RQ 2.

In Appendix A remarks for every used search engine are described for reproducibility, while in Appendix B the number of publications per search engine and search terms are listed after the year filter was applied.

After completing the online review backward searching is applied. Here the citations in the relevant publications identified in the final sample are carefully reviewed to learn about older articles that may be relevant. In backward searching via Scopus the relevant articles are selected by how often they are cited by other articles (forward-searching). The limit of inclusion is set to 20 or more citations.

This number is taken arbitrarily. It should be taken into account that citations do not indicate the 'popularity' or 'quality' of a publication. A publication can demand a subscription and is, therefore, less likely to be cited than a open-access publication. Figure 2.2 shows the global search process and study selection as a whole, with slight deviations in the process of selecting articles, as described below.

2.1.4 Quality Assessment

The goal of using a quality assessment is to investigate whether quality differences provide an explanation for differences in study results and as means of weighting the importance of individual studies when results are being synthesised (Kitchenham and Charters, 2007). For the quality assessment the checklist used in Inayat et al. (2015) and Darvish Rouhani et al. (2015) are used as a base. Below five questions to assess the quality of studies are listed. The first four can be answered by three options per question: yes, partially and no, while the last question has a response grading of 1 (more than 80%), 0 (less than 20%) or 0,5 (in between).

1. Is the research aim/objective clearly defined?
2. Is the context of research well addressed?
3. Are the findings clearly stated?
4. How well has diversity of perspective and context been explored?
5. Based on the findings, how valuable is the research?

The complete outcome of the quality assessment of every RQ can be seen in Appendix C, each page corresponding to a research question. Due to the iterative nature of the selection of the final sample, some publications were dismissed in this phase due to exclusion criteria being strictly applied. In total 7 articles in the quality assessment phase were dismissed: in RQ 1.1 three articles, RQ 1.2 two articles, RQ 1.3 also two and for RQ 2 none.

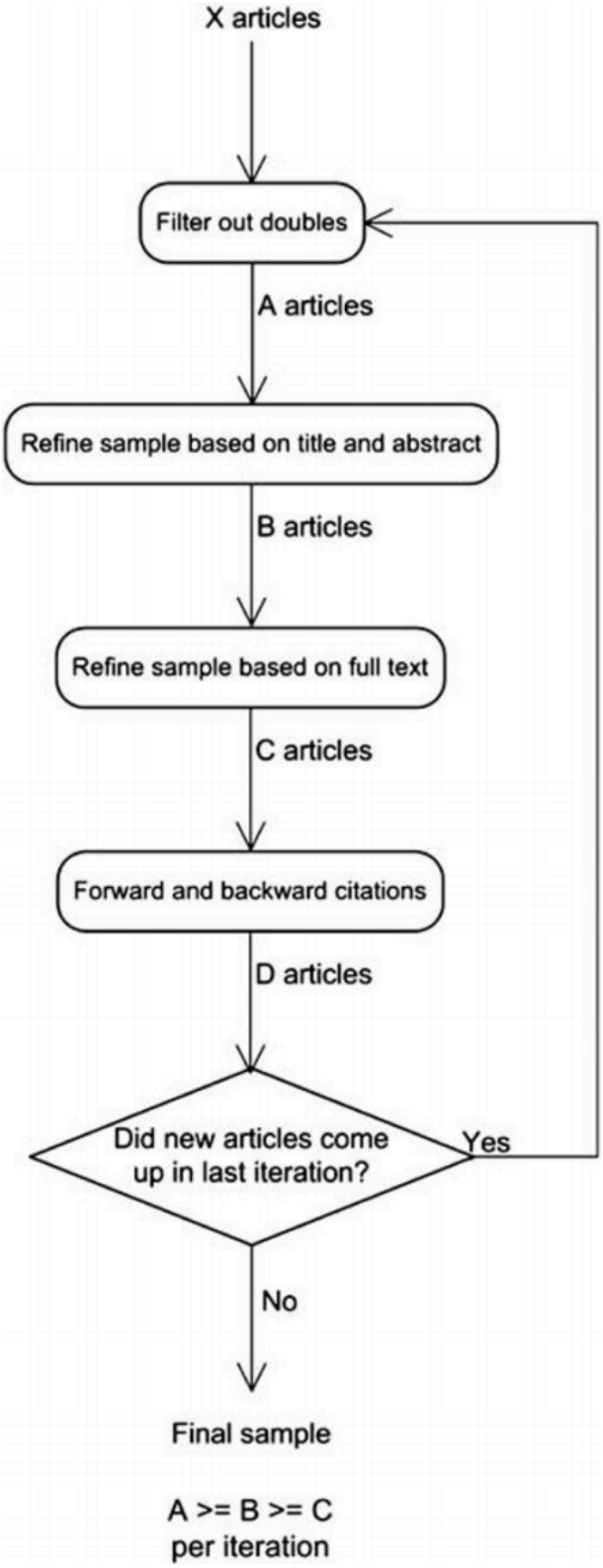

Figure 2.2: Study Selection according to Wolfswinkel et al. (2013)

2.1.5 Data Extraction & Synthesis

After the final sample has been created data extraction and synthesis to identify relevant from the articles can be executed. As Bandara et al. (2015) and Kitchenham and Charters (2007) suggest, a data extraction form should be created to reduce the opportunity for bias.

In addition to including all the questions needed to answer the research questions and quality assessment criteria, data collection forms should provide standard information including: Title, authors, journal, publication details (i.e. year) (Kitchenham and Charters, 2007). This information is stored in Endnote X9, divided per RQ. This information is gathered by automatic extraction via the used search engines.

When synthesising the data for the report, the line of argument synthesis is applied. This approach is used when researchers are concerned about what they can infer about a topic as a whole from a set of selective studies that look at a part of the issue. This analysis consists of two parts. First the individual studies are analysed, then an attempt is made to analyse the set of studies as a whole. This approach is similar to a descriptive synthesis. Issues of importance are identified and the approach to each issue taken by each study is documented and tabulated (Kitchenham and Charters, 2007).

Two specific and frequently used approaches for coding (synthetisation) are according to Bandara et al. (2015):

1. Inductive: where the themes to be reported on are purely derived from the literature analysis itself
2. Deductive: where the themes to be reported on are already predetermined to some extent

In an inductive analysis, the literature review explores what past studies have reported on. It is focused on extracting and synthesising the voices of past scholars from a data-driven approach. In an deductive approach evidence of predetermined themes is searched. These themes can be qualitative (i.e., definitions of key concepts, arguments made) or quantitative (i.e., meta data such as year of publication) (Bandara et al., 2015).

This systematic literature review is going to be both an deductive and inductive one, focusing on security and privacy within connected cars, as determined by the pre-mapping. Within these areas, the themes are subjective and open to interpretation. Therefore themes identified in literature within security and privacy will be derived using the inductive method.

2.2 Framework

As explained in section 1.7, a framework will be created based on to be studied aspects regarding security of V2I projects:

1. Risks - based on vulnerabilities (see section 5.3)
2. Security requirements (see sections 3.3 and 4.3)
3. Vulnerabilities and attack methods (see section 5.2)
4. (Potential) mitigations of risks (see chapter 6)

The goal of the following section is to create a structured plan regarding the framework in order to achieve repeatability and a structure for creating the framework. This final artefact can be described as a comprehensive summary of all the above-mentioned aspects.

The section below consists of two parts: the creation of the framework itself based upon situational method engineering and the conduction of interviews. The output of the interviews will

be taken into account in the creation of the framework.

The final artefact of this research is called a framework since we focus on giving stakeholders input when going through the process of securing V2I projects. We start with a list of vulnerabilities, followed by a general risk assessment, the corresponding attack methods, security requirements and corresponding measures and how these aspects are all related. Our framework outlines what can be done in order to achieve maximum security in V2I projects per specific risk / vulnerability, but does not explain how to identify a certain situation, assess a risk or how a company goes throughout these steps, so therefore it is not a method.

The plan for creating the framework is mainly based on Situational Method Engineering, extracted from Harmsen (1997).

2.2.1 Designing the Framework

The article of Harmsen (1997) will be used as a baseline for developing the security framework of this thesis. We use Situational Method Engineering to structurally move from all the aspects regarding security to a coherent framework.

Since the final artefact of this thesis is in the form of a framework, it is different than a project due to different requirements: this thesis improves the context of a (general) V2I project from a security point when applied, and not the project performance itself. First, we look at the problem explanation. This phase encompasses the explanation of the problem, i.e. V2I, including the context characterisation and what makes this problem unique.

Problem Explanation

For V2I projects there are several aspects / vulnerabilities from a security perspective which influence the security as a whole. These vulnerabilities are risk-based in order to analyse which threats are most important to tackle. The specific functionalities of V2I projects (what they do and communicate) bring security and privacy risks with them, which can be mitigated with several measures. We see V2I projects themselves are separate entities, not communicating with each other (as of yet) due to the novelty of the area. This means identified risks are only applicable for a specific project and not multiple projects as a whole.

The context the framework will operate in is of a security company, in this research Northwave, consulting parties which are involved in the design, set up and execution of V2I projects. The task of Northwave is to help the client, which is responsible for security giving a framework and guide how to implement this is the most efficient way.

Selection of Parts

The selection of framework fragments is induced by the characterisation of the project at hand (Harmsen, 1997). The above problem explanation emphasises the individual parts of the final framework, namely:

1. General vulnerabilities and risks for V2I projects
2. Security requirements (based on literature and standards)
3. Corresponding (high-level) measures, coupled to the general risks

These fragments can be manipulated and changed when a more specific V2I project and functionalities appear when applying the security framework. Harmsen (1997) mentions the order of method engineering steps is twofold. One option is to first completely characterise the project, after which the selection of method fragments can take place (Harmsen, 1997). This is feasibly

when a project is already finished. However, when a project is new, Harmsen (1997) gives another option: first select the method fragments, then characterise the project. This would be more from a 'security by design' perspective in the V2I projects, starting with the security requirements and matching functionality of the project afterwards. In our framework, we aim to achieve both situations in our framework: it should be used in order to analyse both existing as well as new (and not existing) projects in order to achieve maximum security.

Framework Assembly

The above mentioned 3 framework fragments are fixed, meaning they do not change with a changing problem description or context, only the content of the framework fragment differs per situation. This means that per situation / V2I project the specific risks, corresponding security requirements and measures should be chosen.

The advantage of the framework is that the framework fragments are already matched with each other by combining the vulnerabilities and measures (see Chapter 5). Therefore the individual vulnerabilities can be easily swapped or manipulated for every project, as long as the relevant risks stay with the corresponding requirements and measures. Here the vulnerability is the first step in the chain, after which the corresponding risk assessment, requirements and measures are taken, and not the other way around. If you would start with implementing measures without a clear goal of what you are protecting against this could lead to unnecessary spending of resources.

Harmsen (1997) mentions the possibility of starting with the assembly of method fragments from a provisional set of method fragments. For this methodology this could be a baseline, after which you could expand. However, for our framework, the second option mentioned in Harmsen (1997) is chosen: all method fragments that are necessary to cover the situation can be selected, after which they are assembled into a specific situation / project (Harmsen, 1997).

For existing V2I projects wanting to check whether they are conformant to relevant security requirements, the characterisation of the situation is fixed and cannot be changed. This makes the order of the framework fragments for a specific situation irrelevant, as all fragments have to complied to in order to be as secure as possible. However, from a management point of view, it would be logical to first tackle the highest risk before moving to lower priorities. This will be indicative in our framework and not mandatory.

Framework Performance

Since the to be designed framework also is applicable for new V2I projects, for every new phase in the project the situational method can be chosen and adapted based on the results and evaluations of earlier stages, as mentioned in Harmsen (1997). This could be the case when building new projects after the high-level security requirements are fulfilled, another risk analysis is done with new measures being implemented, a so-called second cycle. This cycle could be done endlessly or even with the same security requirements and measures, but on a more detailed or more strict level. The framework will be assessed with a case study where relevant employees of an existing V2I project judge the framework based upon usability and content. More details can be found in section 2.3 below.

2.2.2 Interviews

Several interviews at Northwave B.V. will be held in order to find out practical details of how the security framework can be made useful for a security consultancy company. The output of the interviews is linked to the research question 'how can the proposed framework be applied

and evaluated for the Dutch market?' This sub-question will also be answered by a case study where the framework will be applied to practice. However, this section is about the design of the security framework from a practical perspective.

Four security consultants with multiple years of working experience with (ISO) standards, frameworks, guidelines, best practices and templates of Northwave were interviewed in a semi-structured way. Northwave has several units focusing on behaviour, bytes and business. The interviews were held with four consultants working in the business unit (Northwave Business Security). All sessions were conducted via video conferencing, recorded and generally lasted about 30 minutes. Each user interaction session began by explaining the research project and the interview session format that was to follow.

The interviews were held semi-structurally, where the questions were used as a guide throughout the interviews, but the order in which the questions were asked was not fixed. Also, several sub-questions to gather more information or specify certain information were added in every interview. The semi-structured interviews also allows us to check the quality of the answers and ask deeper questions when possible. The interviews were set up with five open questions regarding two specific aspects: from a usability aspect and a content-wise aspect. Participants were asked how they assess existing frameworks if they are suitable for specific usage or if they are content-wise suitable for their usage. The questions can be found in Appendix H.

Semi-structured interviews are in contrast to a strictly structured (also called direct) interview, where every question is prepared and you aim to gather specific information. A closed interview with a prefixed set of choices would not fit the interview format of collecting as much useful input as possible (Wiebering-Losse, 2009; Nederhoed, 2015). Another option would be a solely unstructured interview, where only a few attention points / subjects are documented before the start of an interview and the questions revolve around the answers of the interviewee (Nederhoed, 2015). An open structure was, however, not fitting because certain information about methodologies / guidelines was required in order to be useful for the final artefact.

In order to accommodate the semi-structured interview form, the questions of the interview itself were aimed to be as open as possible so that consultants could give their own input. However, the same examples when asking a question were given in order to give the consultant a certain context of the question and make clear what was meant. An example is the question about which aspects of a guideline were looked at by a consultant in order to judge a framework, it was added if the level of detail is such an aspect, since this aspect was important to know for the creation of the framework of this research.

The transcription of all interviews can be seen in Appendix I. However, the answers were all categorised in the original question, even though several sub questions were asked. Since the interviews were semi-structured, the order of the questions as in Appendix H was also not followed strictly. However, for clarity, the transcriptions are processed from the order of these questions.

In accordance to the book of Verhoeven (2007) the outcome of the interviews are explored (which terms are used in the interviews), specified (develop and name specific terms, reduced (order and reduce found terms to the original problem statement, i.e. create a framework which is useful in practice) and integrated (analysed and process terms in a certain form, e.g. a diagram). The coding process takes place in the program Atlas.ti.

Therefore the outcomes of the interviews has been coded with the answered per question summarised, see Appendix J. The most mentioned aspects will be incorporated into the final framework. It is important to emphasise that these aspects are not prescriptive but rather indicative of the ideal framework in practice. This is also because the framework is not solely targeted towards consultancy employees but also relevant parties in the V2I projects.

The coding process tries to make a coherent overview of the input the respondents gave to the questions, with the emphasis on categorising the aspects mentioned per question and how this can be translated to the final framework, if possible and on which aspect the answer has influence, e.g:

- Scope of framework
- Detail of information included in the framework
- Workability of the framework: how easy can a consultant work with the framework?

2.3 Case Study

In this section the validation of the framework is described. First, the process of selecting a suitable V2I environment is described by analysing different existing V2I projects and trails. In the sections after that, we explain the choice of using the expert opinion validation method to validate the framework and how we do this by using a survey. Furthermore, we explain the target audience for the survey.

2.3.1 Set Up

There are several (trial) projects running in the Netherlands at the moment of writing this research in 2020. The biggest are listed below, along with the involved parties and the scope of the project:

- **Concorda**: Connected Corridor for Driving Automation. This is an initiative from the Rijkswaterstaat consisting of multiple test areas and projects. Areas being tested are the A5 / A9, N205 and the centre of Amsterdam. The municipality of Noord Holland participates under the name 'Smart Mobility.' The main goal is to 'establish a common understanding on autonomous vehicles.' Examples of trial projects are that of testing self-driving cars, advancement of cellular communication technology or super GPS to achieve high precision location data (Rijkswaterstaat, 2020). However, multiple trial projects are running regarding V2I communication, where Rijkswaterstaat developed and implemented projects in coordination with technical partners like V-Tron, Swarco and Qualcomm via ITS-G5 (also called WiFi-p). Functionalities being tested are communication with connected cars about slow or stationary vehicles, closed lanes of a highway or lowered speed in case of an upcoming traffic jam (PraktijkproefAmsterdam, 2020).
- **Talking Traffic**: Talking Traffic is an initiative between the government of Infrastructure and Water authorities, Rijkswaterstaat, around sixty decentralised governmental parties and twenty (inter)national companies, working together on the development and usage of innovative traffic applications. Real-time information between drivers and traffic infrastructure / systems is the key point to achieve this (CROW, 2019). Flitsmeister, a Dutch app with 1,7 million users, has the ability to see the status of certain connected traffic lights throughout the Netherlands. The next step is, according to the press release at the end of 2019 (Traffic, 2019), to count down until the light goes on green and giving advice to the driver of which speed to maintain to get a green light. More connected traffic lights are continuously being deployed in the Netherlands.
- **Intercor**: Also an initiative from Rijkswaterstaat. InterCor is a 3-year project of 30 million Euros co-financed by the European Union under the Connecting Europe Facility. The project aims to enable vehicles and related road infrastructure to communicate data through cellular, ITS G5 or a combination of both networks on road corridors running through the Netherlands, Belgium, the UK and France (Intercor, 2020). This is more of

a collaboration / knowledge exchange project and therefore not fully relevant for this research.

- **Socrates 2.0**: a project that mainly focuses on sharing and integrating traffic information, in order to improve traffic information, navigation services and prepare for the future of self-driving cars (Socrates2, 2020). This scope is partly within V2I projects but not as a whole since only the gathering of detailed traffic information is the main focus, narrowing the scope for a case study.

Based on the above information, we have chosen for Concorda because it is the only project with a broader scope regarding multiple V2I projects and focusing on specific V2X (and therefore V2I) communication. The best example of this is the project of Praktijkproef Amsterdam, as explained above. Since the framework is aimed to be applicable to multiple V2I projects Concorda is the best suiting environment for validating the framework from different use cases and perspectives.

2.3.2 Validation

As Wieringa (2014) mentions in his design cycle, we want to validate the treatment (i.e. our developed framework) to justify it contributes to stakeholder goals when implemented in the problem content (i.e. V2I projects). However, no real-world implementation is available to investigate whether the framework contributes to stakeholder goals.

Therefore validation models are used to simulate implementations (Wieringa, 2014). In our research, the validation model means we study the framework, interacting with a model of V2I projects, to develop a design theory about the interactions between the framework and V2I projects. In the section below, the chosen research method for studying the validation model is outlined, along with an explanation of the choices made. The possibilities of research methods are outlined in Figure 2.3, extracted from Wieringa (2014).

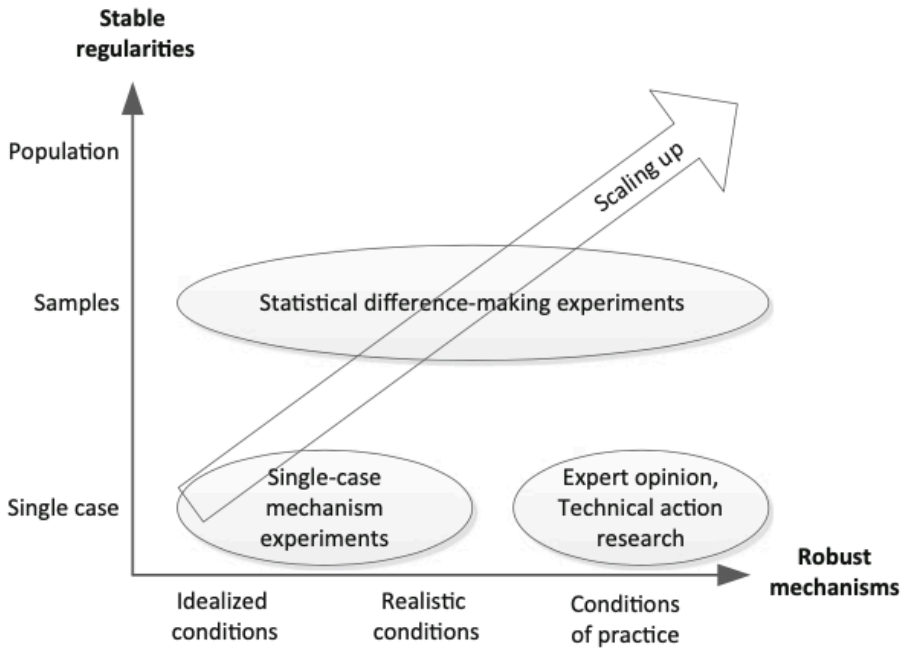

Figure 2.3: Empirical Research Methods

Due to resource limitations, for this research, it is not possible to adopt a sample based research

method. This is due to the novelty of the field of V2I projects, resulting in a limited set of cases that are available for data collection and validation, see also above section. Consequently, a single case-based approach is adopted for the validation process. The framework, or artefact, in this context serves as the case and can be used to retrieve information about its applicability and relevance.

We choose for the expert opinion validation method as the most suitable form regarding the validation process. Here experts are asked about the perceived usability and utility of the new artefact in the contexts that they know first-hand. Furthermore, it is essential that the conducted scenarios with the experts are representative for the total (future) population, i.e. V2I projects.

Survey

In order to extract the opinion of the experts, there are different options: observational case studies, surveys and focus groups (Wieringa, 2014). For the validation process in this research a survey / questionnaire is made. This questionnaire is aimed at project managers regarding security within Dutch Concorda projects.

The aspects to be surveyed are on a high-level the same as consultants were questioned at Northwave, i.e. content and form-wise. The following specific aspects about the framework will be questioned:

- Presented overview of vulnerabilities and risks
- Presented overview of attack methods
- Presented overview of corresponding measures
- Presented overview of security requirements
- Mapping between all the parts (i.e. risks, requirements, attack methods and measures)
- Usefulness of the framework

Of the above 6 mentioned aspects, only the mapping between all the parts in the framework is not a separate section in the survey. This is because the mapping aspects for the vulnerabilities and risks, attack methods, measures and security requirements is processed in the section about that aspect itself. For instance, we ask about the mapping between the attack methods and measures in the 'measures' section in the survey.

Of the 4 main aspects of the framework (i.e. vulnerabilities and risks, attack methods, measures and security requirements) we structurally ask the experts about the following perspectives to judge the framework. Here <aspect x> can be replaced by one of the four main aspects of the framework:

1. Has <aspect x> previously been used or identified in Concorda?
2. The presented aspects of <aspect x> are relevant regarding current and future projects within Concorda
3. Is <aspect x> is made clear by the accompanying description
4. The mapping between <aspect x> and <previous aspect x of survey> are relevant for current and future projects within Concorda
5. Do you agree with the presented overview of <aspect x> regarding current and future projects within Concorda?
6. Do you agree with the mapping of <aspect x> with other aspects in the framework?

As can be seen, with several questions we ask explicitly about both current and future projects in order to make sure the framework also is up-to-date and scalable to future projects of potentially different scale. This matches with RQ 6 (section 1.5). Furthermore, some questions specific to an aspect were added, for instance about the usage of vulnerabilities as the starting point of the framework or the inclusion of security requirements.

Finally, regarding the usefulness we focus on the framework regarding 4 aspects:

1. If the framework as a comprehensive overview regarding cybersecurity would help the experts in their daily work at all
2. If the framework itself would have a positive impact on current / future projects of Concorda
3. If the expert would consider incorporating a framework similar to this research into his or her daily work
4. How relevant the proposed framework is as a whole regarding security in V2I projects

The people chosen to fill in the questionnaire were picked by an employee of the involved project since there is no public knowledge as to know which employees are involved in both security and management, if any for such a V2I project. If there is not dedicated management regarding security of the V2I project, the general project manager will be asked to judge the framework since the goal is to have a guideline which can be steered by him, since there are also processes described in the final guideline. This is in contrary to the technical side where employees are actually implementing several security measures, for which this framework is not aimed at.

The questionnaire starts with a short description of the goal of the guideline. It is not explained, however, how certain aspects of the framework work, this is something that should be self-explanatory when using the framework. This way the usability of the framework can be judged.

The first few questions focus on the general background information of respondent, regarding working experience / working field and for how many years, etc. After that, the individual components of the mythology are to be judged on both content and relevance. Lastly, the experts are asked to judge the usefulness of the framework itself.

It is important to notice that Concorda is only a temporary trail environment with multiple parties involved in order to test primarily functionality. This makes the mapping from the designed framework to the case study in the form of Concorda not a direct relationship, but rather theoretical. Therefore both current and potential future projects of Concorda (when for instance security is being implemented or functionalities are added or combined) were questioned in the survey, which aligned with the goal of the framework of being up-to-date and scalable for future V2I projects as mentioned in research question 6.

There are several types of questions which can be chosen from regarding the questionnaire, varying from open to closed questions, yes/no questions or multiple-choice questions. To get the opinion / feelings of the respondents in a structural manner, mostly multiple-choice questions are used. The scale is purposely chosen with no middle ground possible, since a disproportionately large part of respondents tends to answer the middle answer, i.e. 'no opinion' when possible (Nederhoed, 2015). Therefore we have the following 5 answers, extracted from Nederhoed (2015):

- Strongly disagree
- Disagree
- Do not disagree, but also not agree
- Agree

- Strongly agree

However, open questions were also added in order to gather background information of the respondent, how certain current processes regarding security are being executed and get the sentiment of respondents about the individual parts / the order they appear in. Lastly, multiple-choice questions regarding the usefulness of the framework as a whole were asked with predetermined answers, e.g. the framework could help now, in the future, none, or both. This in order to adequately judge whether the framework is suitable for current or future projects, since Concorda currently exists of trails which could influence the focus on security. The questionnaire as a whole can be found in Appendix K.

3 LITERATURE REVIEW

In this section, the first two research questions about the functions of connected cars, security requirements, privacy requirements and current risk analysis methods are answered. This is done by executing a systematic literature review, of which the methodology is described in section 2.1. The review conduction of this methodology is first described in the sections below, stating how the selection process regarding literature is executed along with findings regarding the literature about connected cars in general.

We first research which functions connected cars have in order to get a clear picture of what literature says about the connected car in general, while also taking V2X (and therefore V2I) into account. The mapping from connected cars to V2I is unconventional but necessary, considering the lack of literature about specifically V2I or even V2X. As mentioned, the aim for listing the functionalities of connected cars is to see which aspects of security are important of connected cars by looking at functionalities, and if there is a relationship between these specific functionalities and security requirements.

Second, the security and privacy requirements regarding connected cars are researched to have these serve as a base for the final framework. This approach means that the identified security requirements are a guide throughout the framework, giving it a scientific backing.

Finally, we analyse the existing risk analysis methods regarding connected cars and determine which one is the most suitable for a risk analysis we will execute on V2I projects in general (Chapter 5).

In the following sections, both the conduction of the systematic literature review and the findings for the first two research question will be outlined. After every subsection, a brief conclusion will be stated with the takeaways for the to be created framework.

3.1 Review Conduction

3.1.1 Study Selection

In order to gather a representable sample of literature, first the double articles were filtered out. After that, the title, abstract and full text were analysed (in that order). Subsequently, backward citation is executed (Kitchenham and Charters, 2007). The disjunction of title and abstract is made because of pragmatic reasons: reading abstracts of more than 700 articles would take too much time for this literature review.

Inclusion and Exclusion Criteria

To execute the title and abstract analysis, inclusion and exclusion criteria are used. These are formulated per RQ and listed below.

- RQ 1.1

  - Inclusion criteria
    * Current or future possibilities / functions of connected cars are explicitly mentioned
    * Internal / external communication with connected car is main topic of article
  - Exclusion criteria
    * Connected cars are mentioned as example without being the main topic, i.e. in articles about Internet of Things or Smart Cities
    * No future or purely theoretical solutions / propositions are the main focus of the article
- RQ 1.2 / 1.3
  - Inclusion criteria
    * Cyber security or privacy in automotive is main topic, e.g. case study or overview
- RQ 2
  - Inclusion criteria
    * Risk analysis / assessment focuses on automotive
    * Risk analysis / assessment is focused towards information security of the connected car
  - Exclusion criteria
    * Risk analysis / assessment is about automotive manufacturer itself, e.g. supply chain, production or driving style of cars

We found that many articles about privacy in connected cars are about triangulation for location and how to make this as privacy friendly as possible, which is out of the scope of this review. This was also the case regarding RQ 1.2, where many structural / architectual solutions were described, including (production) implementation details.

Therefore general inclusion and exclusion criteria were created in order to filter out these cases, along with setting a limit to the age of the articles. This limit is set to 2015 as to include relatively recent articles, in line with the quickly changing status of the connected car in the last 5 years.

- General criteria
  - Inclusion criteria
    * Article is available online and in English
  - Exclusion criteria
    * Article focuses on research / implementation of structural or architectural aspect of connected car, e.g. encryption, specific set up, mitigation measures or cloud environment
    * Main topic of article is about Electrics / Electronics (E/E) or internal infrastructure of a car, e.g. ECU
    * Article is focusing on autonomous cars
    * Article is published before 2015 (5 years at the time of writing)

* The article does not originate from an academic journal or conference or is not available online
* Article is guest contribution of a scientific magazine

In total 41 articles which we identified were applicable for other RQ's. Some articles have overlap between subjects, e.g. publications which describe a framework for assessing cybersecurity also describe functionalities or corresponding risks. Thirty articles of conference proceedings were excluded due to their lack of online availability. The division of the final selection per RQ can be seen in Table 3.1, while the amount of articles per selection phase can be found in Figure 3.1.

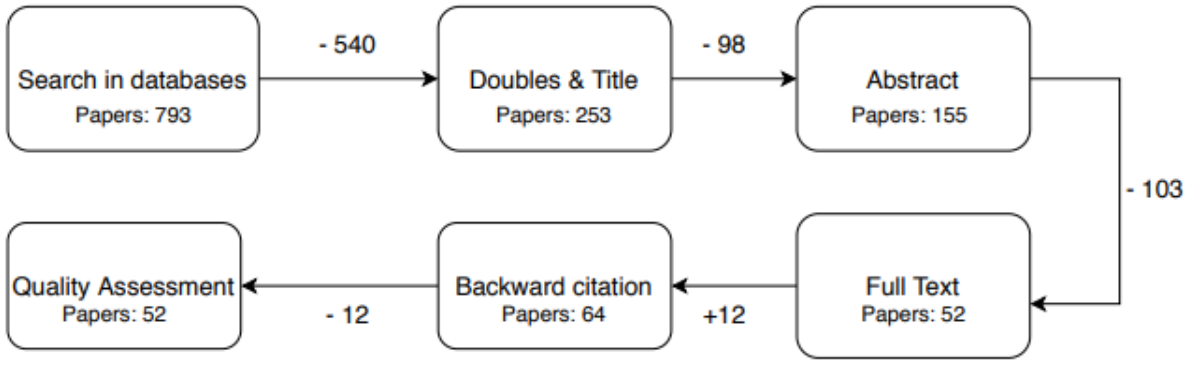

Figure 3.1: Amount of Articles per Selection Phase

Table 3.1: Division of Articles per Research Question

RQ 1.1	12
RQ 1.2	15
RQ 1.3	7
RQ 2	18

Based on Table 3.2 and Figure 3.2 we conclude that the research field of connected cars regarding security and privacy is still in its infancy, although on a decreasing rate. Where in 2016 36% and in 2017 30% of the final literature sample originates from a journal, in 2018 this has already raised to 41%.

Since this review took place at the end of 2019, a possible explanation of the lack of journals in this year are the review times for publication in such journals. Furthermore, the most amount of articles are found in 2018, indicating the raise in literature regarding security and privacy in connected cars. A reason for the high presence of conference articles is that these are quicker to be published to the public and therefore more state of the art, which is valuable in such a fast moving industry. This development can clearly be seen in Figure 3.2, where the blue parts of the bar indicate the publications originating from conference papers.

Table 3.2: Division of Articles per Year

	1999	2012	2015	2016	2017	2018	2019
Journal	1	1		4	3	7	1
Conference			2	7	7	10	4
Chapter			1			1	3

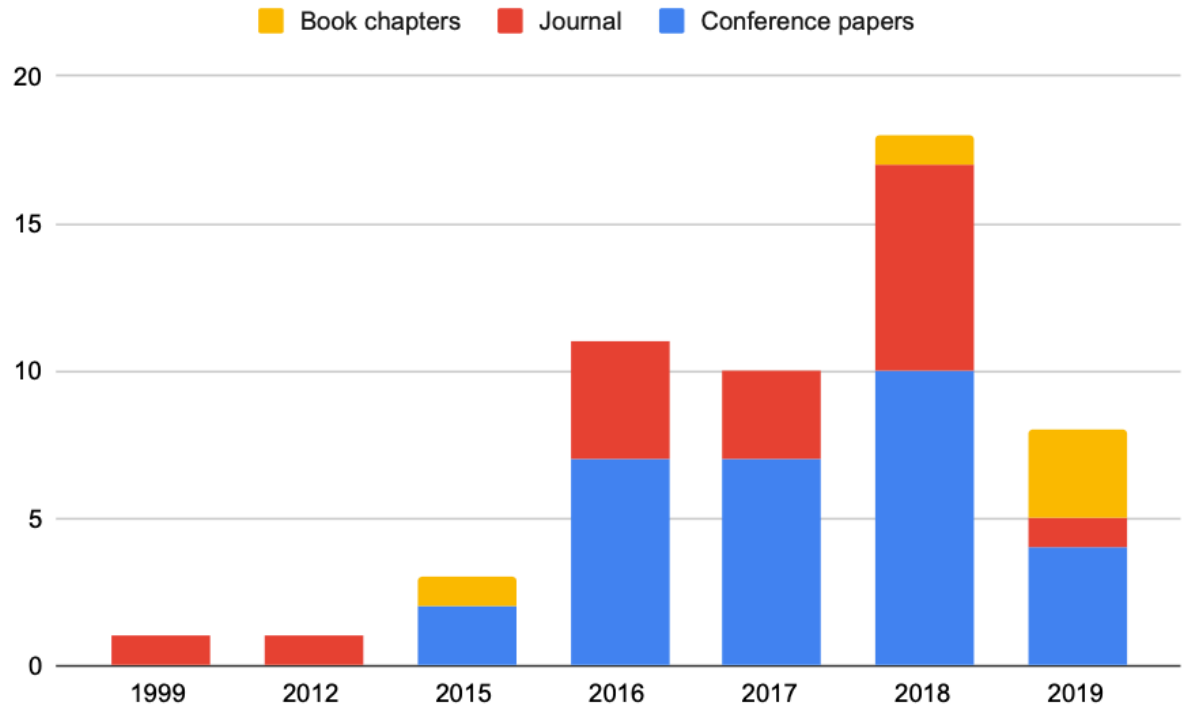

Figure 3.2: Division of all Articles per Year and Origin

Ram et al. (2018) mentions how among all the documented concerns in his systematic literature review, communication in connected cars has managed to draw a significant attention, especially in recent years. 33 primary studies investigated this aspect between 2007 and 2016. However, in 2017 alone, 27 primary studies reported on this concern. This emphasis suggests that the security concerns related to communication in connected cars is drawing, and will continue to draw, attention of the research community for the foreseeable future (Ram et al., 2018).

3.2 Functions of Connected Cars

In this and the sections below, we focus on answering the research questions 1.1, 1.2, 1.3 and 2. In this section, we answer research question 1.1: 'What types of external connectivity functions are present in connected cars according to literature?' As a reminder, we distinguish two categories in external connectivity: telematics and V2X. The section below will therefore also be separated by this categorisation.

3.2.1 Telematics

Telematics are, as explained in the introduction, the usage of wireless components and technologies to transmit data in real time within a network, i.e. on a car level. Telematics are used for integrated use of telecommunication and informatics, applied in vehicles and for control of vehicles on the move, i.e. infotainment systems. Another possibility is vehicle tracking via (GPS) location. Consumers frequently desire safety and security telematics applications, including automatic collision notification, roadside assistance, remote door unlocking and voice services.

There are three options to connect a car to the internet regarding telematics (Vékony, 2016):

- **Embedded**: communication module and SIM card are built into the car
- **Tethered**: utilises mobile phone for connecting with an automobile's infotainment system
- **Integrated**: most recent addition. Usage of mobile phone functionality via car itself, e.g. Android Automotive

We identify two categories regarding telematics: convenience functions and functionality enablers. This first category encompasses direct usable functions for the user of a connected car, while the latter category are aspects in which new functionalities can be accessed, e.g. Android Auto or Apple CarPlay.

With Android Auto or Apple CarPlay you can connect your smartphone (wired or wirelessly) to a car and access a special version of e.g. WhatsApp, Spotify or Google Maps on the infotainment screen of your car. These systems do not function without a smartphone.

All the listed functions in Table 3.3 are derived from Siegel et al. (2017), Mourad et al. (2017), Hong et al. (2016), Coppola and Morisio (2016), Svangren et al. (2017) and De (2018). The listed functions can often already be found in current connected cars.

Table 3.3: Functions of Connected Cars

Convenience Functions	**Functionality Enablers**
Start engine remotely	Apple CarPlay / Android Auto
Start automatically when sitting in the vehicle	Streaming music
Warm up the engine before sitting in the car	Wifi hotspot
Open/close doors automatically	Social media
Open/close the trunk / fold the side view mirrors	App store access
Start air conditioning/ventilation before departure	Voice (assistant) services
Set burglar alarm/impact detection	Roadside assistance
Remote door unlocking	Video streaming
Driver's fatigue / stress detection	Receiving wireless software updates
Predictive maintenance	
Emergency responds	

Hong et al. (2016) focuses on 'vehicle actions requested from outside the car' and communication from cars to homes. Via examples of consumer preferences, deducted from 220 US customers between 18 and 60 years, seven current applications of specific in car functional examples came forward, which are included in above Table.

The article of Vékony (2016) details more about the speech capabilities of assistants in connected cars. The main takeaway is that speech assistant from both OEMS and tech companies (i.e. Apple and Google) can be natively used within a car. Basic examples are voice prompts (warnings, traffic information, navigating to places of interest / address entries) and telephony (accepting / ignoring calls).

3.2.2 V2X Communication

With V2X communication, vehicles exchange messages with neighboring (close by) vehicles and with road side units (RSUs). Each vehicle communicates with the neighboring RSUs to inform them about itself. The information may include location, speed, heading, and to get traffic conditions of the road, i.e. traffic lights or digital speed signs (Othmane et al., 2015).

Möller and Haas (2019) mention several examples of V2X communication, which always encompasses possible communication between both the sending and receiving party and visa versa (Axelrod, 2017).

- V2V: Vehicle to Vehicle: inter-vehicle networks (also called VANets) communication about safety and efficient situations to other cars (typically based on broadcast capability (Ahmadi, 2019)).
- V2I: Vehicle to Infrastructure / Vehicle to Road (V2R): communication with infrastructure devices, i.e. traffic control systems, smart traffic light systems, finding free parking spots and automatic parking.
- V2H: Vehicle to Home. Communication between a vehicle and home appliances, e.g. garages or gates.
- V2E: Vehicle to Environment. Communication between vehicles and infrastructure that are operated privately and commercially, e.g. communication with a parking garage when a spot is available.

Axelrod (2017) distinguishes V2X communication not by function but by distance. For instance V2S (Vehicle-to-surroundings, similar to V2I) is where the car communicates with nearby infrastructure in the form of an automated toll collecting booths. Another example is V2E, where the scope is the local vehicle ecosystem, i.e. the remote locking of a vehicle when stolen.

As can be seen, different authors use different definitions of V2X communication. In this research, we use the definitions of V2X per function according to Möller and Haas (2019).

Focusing on specific functions, the article of Coppola and Morisio (2016) is one of the few articles solely targeted towards V2X and current functions. The main functions that are derived from this article are listed below, with in brackets the corresponding V2X aspect.

These functions are theoretically already possible, but currently not used due to dependence of (external) infrastructure and corresponding difficulty to implementation when working with different stakeholders, e.g. communication standards, government institutions, car manufacturers, etc. The categorisation of functions is listed below:

1. **Traffic Safety**

1.1. Accident avoidance and assistance (ADAS / eCall) (also mentioned in Siegel et al. (2017)) (V2I)

1.2. Night Vision Assistant and Head Ups Display: navigation info, warnings signs, expected hazards shown on the windscreen (V2I)

1.3. Remote maintenance: in advance detection of malfunctions (also mentioned in Siegel et al. (2017)) (V2I)

2. **Traffic Efficiency**

2.1. Navigation, online route planning, street view: send routes to car, see photographs and recommendations about nearby places (V2I)

2.2. Traffic, weather, road condition monitoring: communication to gather information, e.g. with a blockage on the road (also mentioned in Siegel et al. (2017)) (V2I)

2.3. Assisted driving and autonomous vehicles: keep distance from cars, help driver with driving the car (V2V)

3. **Convenience, interaction and others**

3.1. Smart home integration (see also publication of Hong et al. (2016)): enable devices like lights, heatings, garage doors before actually approaching home (V2H)

We can conclude from the above information that in connected cars there are two categories regarding current external connectivity functions: telematics and V2X communication. Telematics are features on a car level and have two types: convenience functions and functionality enablers. Most of these functions are often already found in modern connected cars.

V2X, on the other hand, is dependent on external communication and infrastructure and therefore more difficult to implement due to the variety of stakeholders. V2X consists of four general categories: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Home (V2H) and Vehicle to Environment (V2E) communication. (Possible) functions focus on three categories: traffic safety, traffic efficiency and convenience functions, where V2V and V2I are most often mentioned. Finally, we could not identify any overlap between the features of connected cars and security requirements in the articles.

For the remainder of this thesis, the categorisation of functions of V2X mentioned in section 3.2.2 - i.e. traffic safety, traffic efficiency and convenience functions - are the most important take-away since this is the scope of the final framework and V2I.

3.3 Security Requirements

In this section we describe cybersecurity requirements for connected cars, therefore answering research question 1.2: 'What cybersecurity requirements for connected cars and specifically V2X are discussed in literature?'

With a requirement we mean a need or expectation, generally implied or obligatory, in order to achieve a certain state. The desired state in this case is maximal security against threats and vulnerabilities. No measures on how to achieve these states are described in this section, e.g. encryption, cryptography, gateways, virtualisation or any other measures. Instead, the (high-level) requirements for reaching the desired state are described. These security requirements are taken into account when designing the final framework as in: the security requirements regarding V2X / V2I form the scientific backing of this framework.

The systematic literature review about security and privacy concerns in connected cars of Ram et al. (2018) mentions how threats are most mentioned, with 84 publications, followed by authentication, authorisation and privacy under identify management, without any additional information. We aim to improve upon the lack of backing of these claims in this section.

Furthermore, only accepted standardisation documents and requirements in literature are described, not regulations from e.g. the European Union, working groups or other public bodies / regulation authorities. The existing European guidelines / standards about V2I can be found in Chapter 4.

In our structured literature review we identified three international standards regarding (connected) cars, although the to be published ISO 21434 standard is focused on cybersecurity in connected cars, while the other two identified standards - ISO 26262 and SAE J3061 - are only partly relevant. Since these standards were often mentioned in literature in regards to security and connected cars, beneath follows a summary of all three standards and their relevance to connected cars.

Note that the author of this literature review did not have access to the mentioned standards. Furthermore, information about the ISO 21434 is scarce due to the standard being in concept-phase and therefore only a hand full articles are written about the high level contents of this, arguably, important international standard.

First, however, we focus on the terms 'safety' and 'security' and how they differ and relate to each other. We do this since we identified many publications discuss the term 'safety' when it gets down to security in connected cars. In section 3.3.1 below we elaborate on this finding.

3.3.1 Safety vs Security

Safety is built upon reliability theory and looks into statistical malfunctions of components with small probabilities and how they will impact functionality. Security, on the other hand, has to deal with the worst cases with a probability of one because once known, they will be exploited (Ebert, 2017).

On a high level, the goal of functional safety and cybersecurity is the same: reduce risk to an acceptable level. Both disciplines agree that elimination of risk - called hazards in ISO 26262 and threats in SAE J3061 - is not possible. However, it must be ensured that steps are taken and mechanisms are used that help to reduce risk and are feasible and reasonable concerning the related development effort, costs, and functional impact, and that the remaining risk is acceptable (von Wedel and Arndt, 2018).

The most obvious overlap occurs whenever a system is safety-relevant, cybersecurity must analyse whether it might be possible for an attacker to negatively influence the functional safety

of the system, and implement mechanisms to prevent this if necessary (von Wedel and Arndt, 2018).

However, there can be conflicts between functional safety and cybersecurity. An example is that of the central door locking functionality. In case of a crash, the doors of the car should be unlocked to allow injured passengers to exit the vehicle and first responders to be able to get to them quickly. If there is uncertainty as to whether a crash occurred or not, the safe reaction is therefore to unlock the doors. The central door locking function also serves a security purpose though, namely to keep unauthorised people out of the car. From a security point of view, the best reaction in case of doubt regarding the current state of the vehicle is therefore to have the doors locked. An attacker could exploit the safety mechanism that unlocks the doors in case a crash is assumed to have occurred.

The solution according to the opinion of von Wedel and Arndt (2018) is to that, as long as safety and security are not both handled as an integral part of the overall development process, functional safety and cybersecurity should be treated as separate disciplines during development while maintaining close coordination. Since safety and security mechanisms do not only influence each other but also the overall system design, not only coordination between the two disciplines, but also their integration into the overall development processes is essential for an efficient development. Communication paths need to be established early in the development project to ensure coordination of the technical concepts.

However, Schmittner et al. (2018) indicate that not every safety-critical system is equally security-critical and that there are security-critical systems without immediate safety impact, hence the development of the ISO 21434 solely focused towards security.

When summarising the difference between safety and security, we would say the following statements covers the above section the most accurate: safety focuses on risks originating in faults within the vehicle system, while (cyber)security looks at risks caused by attacks from outside the system.

As can be noticed, literature mainly describes safety and security from a process point of view. Both ISO 26262 and SAE J3061 are also primarily process oriented. This means they explain from the concept phase of designing a car to the decommissioning of a car, that functional safety and cybersecurity are to be considered throughout the whole development project and build into the design, rather than added onto a finished system at the end of the development.

In the beneath sections, we will elaborate on what ISO 26262, SAE J3061 and ISO 21434 means for security, starting with ISO 26262.

3.3.2 ISO 26262

ISO 26262, from the well known International Standard Organisation, is primarily a safety standard. ISO 26262 was extended in the second edition to cover the relationship between functional safety and cybersecurity. On the cybersecurity side, the process framework introduced in SAE J3061 in January 2016 was intentionally aligned with that of ISO 26262 to ease the introduction of cybersecurity processes where those for functional safety are already in place (von Wedel and Arndt, 2018).

ISO 26262 edition 2.0, which was published at the end of 2018, includes recommendations for the interaction between safety and security. Based on a initial discussion on how to treat safety and cybersecurity in automotive standardisation, it was decided to publish separate standards, resulting in the ISO 21434 (Schmittner and Macher, 2019).

A number of existing functional safety standards define variants of safety integrity levels, which

specify the level of risk reduction required and approaches for achieving it. In ISO 26262 this is the Automotive Security Integrity Level (ASIL) (Ward and Wooderson, 2016). The possible ASILs range from QM (no safety measures required) and from ASIL A until ASIL D. For functions with ASIL A, ASIL B, or ASIL C, fewer requirements on the development processes, safety mechanisms, and evidences are given in ISO 26262 than ASIL D Beckers et al. (2016). These requirements focus mainly of functional safety and are therefore not of relevance for this literature review.

3.3.3 SAE J3061

The second often mentioned international standard about security and connected cars is SAE J3061. Due to the joint development of ISO 21434, SAE J3061 was at the time of writing pulled from the market and will be reworked to cover additional topics, outside the scope of ISO 21434 (Schmittner and Macher, 2019). This information is, however, very recent and therefore many publications we identified in our systematic literature review from before 2019 have not had this knowledge. Therefore SAE J3061 is still being (separately) treated in this literature review.

SAE J3061 was the available guideline for automotive cybersecurity engineering. The standard establishes a set of high-level guiding principles for cybersecurity by: (a) defining a complete life cycle process framework, (b) providing information on some common existing tools and methods, (c) supporting basic guiding principles on cybersecurity, and (d) summarising further standard development activities. SAE J3061 states that cybersecurity engineering requires an appropriate life cycle process, which is defined in correspondence to the process framework described in ISO 26262.

SAE J3061 recommends an initial assessment of potential threats (TARA - threat analysis and risk assessment, see also section 3.5) and an estimation of risks for systems that may be considered cybersecurity relevant or are safety-related systems, to determine whether there are cybersecurity threats that can potentially lead to safety violations.

Apart from that, no further recommendations on how to proceed with this estimated risk, set-up a security classification scheme or guidance for required protection mechanisms is given (Macher et al., 2017). We will therefore only explain how cybersecurity is processed in SAE J3061, which only comes back at the concept phase of creating a connected car, consisting of seven substeps, described below.

The first of the seven steps in the concept phase is the feature definition. Here the physical and trust boundaries of the system are described.

In the second step - initiation of cybersecurity lifecycle - the project is planned and documented with respect to the cybersecurity process.

Then comes the main activity in the concept phase: the threat analysis and risk assessment (TARA). More details about TARA are mentioned at section 3.5 where risk assessments are treated.

After the threats and risks are determined, a sub-step is taken called 'identify cybersecurity goals.' These goals can be stated in terms of what to avoid or the inverse of the threat system level. They are a high-level and concise descriptions of what should be avoided, detected or prevented. SAE J3061 does not mention specific requirements but lays out the process of determining these. Examples are 'prevent eavesdrop of wireless communication' or 'avoid unauthorised or unfinished software updates' (Schmittner et al., 2016).

Subsequently, cybersecurity concepts are stated in step 4. These include the high-level cybersecurity strategy that satisfies cybersecurity goals for identified threats. The strategy will be

refined to a technical strategy later in the production development phase.

Based on the high-level strategy, functional cybersecurity requirements are defined in the fifth step: identify functional cybersecurity requirements. These requirements are derived from the cybersecurity strategy that satisfies the cybersecurity goals (Schmittner et al., 2016).

The last two steps in the concept phase are the initial cybersecurity assessment and concept phase review. Initial cybersecurity assessment conducts an assessment of the level of security of the system. J3061 suggests that the initial assessment contains only the high-level cybersecurity goals, the risks, and open security issues. Concept phase review acts as a quality control gate that reviews the whole concept phase (Schmittner et al., 2016).

We noticed that the article of Walker (2018) mentions some downsides of SAE J3061. For instance, it is mentioned how there is not enough emphasis in the document on how the maintenance of adequate cybersecurity mechanisms could be achieved. Instead, only three sections of J3061 address the subject of post-production activities of connected cars, while the other processes focus on pre-production and production itself (i.e. the above described concept phase). This needs to be strengthened by looking at techniques to continually assess cybersecurity according to Walker (2018), especially in a future when connected cars continuously get new functions via software updates.

3.3.4 ISO 21434

SAE and ISO have joined their efforts to develop a new standard, ISO/SAE 21434, with the aim to establish an internationally accepted standard focusing on cybersecurity engineering, suitable for the automotive industry and with a risk based approach (Burzio et al., 2018). This standard is as of 2020 not available yet to the public. There is, however, already some information known about the goal of the standard and the scope.

The purpose of the standard to be created was to (a) define a structured process to ensure cybersecurity engineering of in-vehicle systems, (b) therefore reducing the potential for a successful attack and reducing the likelihood of losses, and (c) provide clear means to react to cybersecurity threats consistently across a global industry (Schmittner and Macher, 2019). Once again, the processes regarding cybersecurity are most important here.

In the standard neither specifics to cybersecurity technologies, solutions or measures are given. Furthermore, there are no unique security requirements for autonomous vehicles or road infrastructure given (Schmittner and Macher, 2019).

ISO 21434 focus areas are on cybersecurity engineering, considering all phases of the vehicle life-cycle, ranging from design and development, production, operation and maintenance to decommissioning. This is in contrast to the limited scope of SAE J3061 where mainly the concept phase was emphasised.

Once again, in the concept phase the item is defined with the help of TARA. In the next step during system specification requirements are refined and assigned to software and hardware. After the system concept is defined and during the development software and hardware phase, vulnerability analysis and risk assessment are used to ensure that no additional threats are introduced and the residual risk is acceptable. Guidance on implementation is for software mostly focused on secure software development and security functions and for hardware on the usage of hardware security functions. After the software and hardware phases are completed, verification and validation provide everything to release the system for production (Schmittner and Macher, 2019).

We conclude from the above two sections, that from a process point of view, the ISO 26262, SAE

J3061 and ISO 21434 can be used in order to develop a safe and secure connected product in the concept phase. Furthermore, after the feature definition and initiation of the cybersecurity lifecycle, a vulnerability analysis and risk analysis is executed. This step shows the importance of both RQ 2 and RQ 4.

In the section below, we move away from the most mentioned international standards and focus on individual aspects regarding security in connected cars and what requirements articles mention, starting with V2X communication.

3.3.5 Security Requirements of Connected Cars

In this section the security requirements regarding external (V2X) communication are described. These security requirements are converted to high level security requirements which we in turn use in our framework, in combination with the mentioned security requirements of European institutions (Chapter 4).

In the section below individual articles with suggestions to general requirements regarding security within (aspects of) connected cars are listed, starting with the article of Othmane et al. (2015). After that, the publication of Hu and Luo (2018) focuses on vehicle networks and their security requirements.

In the article of Othmane et al. (2015) a taxonomy of the connected car is mentioned. These aspects are:

- Data validity: data is information generated, manipulated, transmitted, and received by vehicles. Data include in- vehicle data, location data, and aggregated data. Data validity is mapped to authenticity.
- Identity and liability: binding an entity to a specific information or event. Identity refers to a characteristic of an entity, which distinguishes it from other entities. Liability refers to the ability to prove that a specific entity (vehicle, driver, and car owner) — or a set of entities — is responsible for a specific event or a set of events. The entity cannot repudiate the responsibility for a specified event. This aspect is mapped to non-repudiation.
- Access control (authentication): this aspects refers to enforcing rules for access or deny to certain functions or data for identified entities.

The security requirements for vehicle networks can be seen in Table 3.4 according to Hu and Luo (2018), including the CIA triangle. These are more general requirements which are not exclusive to the automotive area.

Table 3.4: Security Requirements of Vehicle Networks

Security Requirement	**Description**
Data origin authenticity	Ensures that the data received comes from a trustworthy source
Integrity	Data is not modified when transferring
Access control	Authorisation before the access to information
Freshness	Time information of related message
Non-repudiation	Actions of entity is undeniable
Confidentiality	Only authorised entities can get the information
Availability	The services provided are operational

3.3.6 V2X Communication

In this section, security requirements specifically regarding V2X are outlined. We only identified two publications about security requirements and V2X, both of which are outlined below. All the remaining publications focused on the security of the vehicle itself (e.g. internal architecture of ECU's).

In our literature review, we found one general article of Tbatou et al. (2017) describing security requirements mentioned in the next paragraph. After that, signal security (i.e. communication) is outlined in the publication of Macher et al. (2017).

The article of Tbatou et al. (2017) focuses on cybersecurity requirements of V2X communication. First, the communication channels need to be protected against data theft (confidentiality), and against manipulation (authenticity and integrity). Furthermore, the network interfaces need to prevent unauthorised access (authorisation).

In the network layer of a connected car, the most prominent security issues are with respect to the integrity and authentication of the data that is being transported in the network. Authentication refers to giving permission to access a connected car, not to be confused with authorisation, which is the access of a device to a network infrastructure.

The article of Macher et al. (2017) suggests a guideline for signal security in automotive industry. They argue that the realisation of a secure context in vehicle systems requires the coordinated application of different security technology best practices. Nevertheless, currently no standardisation for the coordination of security technology practices has been established and it is up to the manufacturers to decide how to provide a secure context (Macher et al., 2017). Therefore the authors propose a security classification scheme on the signal layer with five different security levels (SecL). Since the levels only focus on the signal level and not on the information security level, this classification only applies when handling wireless signals. Each security level must imply the security technology practices assigned to the lower levels. The levels can be seen in Table 3.5, with in brackets the corresponding high level security requirement(s).

Table 3.5: Security Signal Levels

Layer	**Attribute**
SecL0	No additional requirements
SecL1	Verify origin of message (non-repudiation, authentication) Verify integrity of message (integrity)
SecL2	Check volumes of messages (availability) Detect abnormal behaviour (availability, authorisation) Immutable device identification (non-repudiation, authentication) Intrusion detection (confidentiality, authorisation)
SecL3	Encrypted communication (Confidentiality) Data encryption (Confidentiality)
SecL4	Establishing of private communication channel Correct cycle detection Blocking of unapproved and inappropriate messages

If we analyse these security requirements, level 1 until 3 are the most common among (fu-

ture) V2I projects based on the functionalities and current state of security in these projects. These are therefore mapped to high level security requirements and taken into account for the framework, while level 4 is not.

In the first three security levels of Macher et al. (2017) the following requirements and amount of appearances are mapped: authentication 2, authorisation 2, availability 2, non-repudiation 2, confidentiality 3 and integrity 1.

The summary of all the above mentioned specific requirements and corresponding mapping can be seen in Table 3.6. In the middle column the general requirements regarding connected cars are listed, while in the right column V2X is specifically listed. No specific requirements for telematics were found.

As can be seen, regarding security requirements of connected cars in general, authentication is the most mentioned aspect, followed by non-repudiation, confidentially, integrity and availability (CIA). All these aspects are also mentioned at V2X communication, with data freshness as the outlier.

Table 3.6: All Identified Security Requirements of Connected Cars

Requirement	**Times Mentioned**	**V2X**
Authentication	5	3
Integrity	3	2
Freshness	1	
Non-repudiation	3	2
Confidentiality	3	4
Availability	3	2
Authorisation	1	3

3.4 Privacy Requirements

In this section, we answer RQ 1.3: 'what privacy requirements for connected cars and specifically V2X are discussed in literature?' We try to extract privacy requirements from existing publications. However, as it turned out, they are not explicitly mentioned in the publications we identified. This means this section does not contribute to the final framework in any form. Privacy as a general aspect is, however, being taken into account in the risk analysis in chapter 5 but the section below does not contribute to the input of the risk assessment. Therefore this section is included in this literature to describe what is mentioned about privacy and connected cars in general.

We identified three main themes regarding privacy and connected cars: data gathering, the description of GDPR and connected cars, and how permissions about data gathering are / should be arranged in connected cars. In the following sections we describe our findings regarding all of these three aspects.

3.4.1 Data gathering

As we mentioned before, modern connected vehicles are equipped with both telematics and V2X systems that make use of information of a vehicle's internal system. Modern vehicles are also equipped with infotainment systems that use non-vehicular information, providing drivers convenient onboard functions when driving. The information generated by these systems forms a source of consumer data which can be stored, processed and analysed. Vehicles log information can be related to the driver's behaviour, location, contacts and intended destinations (Akalu, 2018).

With this information, a driver profile may be developed that can be used for legitimate reasons such as providing emergency services and law enforcement, as well as a range of illegitimate reasons such as surveillance by employers, insurance companies or criminals. An example of this was when the satellite navigation company TomTom was caught selling customer GPS data to Dutch law enforcement for the purpose of creating speed traps in 2011 (Jaisingh et al., 2016). Therefore while wireless communication may offer significant benefits for safety, security and sustainability, they also raise considerable informational privacy risks since the data being shared is potentially accessible to a wider set of users (Akalu, 2018). Recipients of privacy-sensitive data are usually automotive manufacturers, suppliers and their service provider, e.g. car dealers, leasing companies, car rental companies, insurance companies, finance providers, etc (Nawrath et al., 2016).

The article from De Vries and Van Engers (2019) informs users about the data collection of their smart car and whether the owners are aware of this phenomenon. It turns out 79% of modern car owners from BMW, Tesla and Volvo indicate (disagree / partially disagree) that the transparency of the gathered data mentioned in Table 3.7 is not clear with the commissioning of the vehicle, while 70% disagree with the statement that their personal data is easy to see, and 12% indicate they have a clear image of where their personal data is being used for.

Currently car manufacturers and dealerships satisfy their privacy obligations to consumers by communicating information handling practices with users via user agreements, privacy statement and software terms (Akalu, 2018). De Vries and Van Engers (2019) lists a few aspects from privacy statements deducted from BMW, Volvo and Tesla, while Nawrath et al. (2016) lists eight categories / aspects in which privacy-sensitive data in cars are collected, deducted from in total 47 publications (Table 3.7).

Table 3.7: Gathered Data of Connected Cars

Aspects (De Vries and Van Engers, 2019)	**Aspects (Nawrath et al., 2016)**	**Description**
Operational data	Identification data, driver behaviour data, biometric and health data, location data	Location, speed, mileage, state of charge, fuel usage, weight of luggage in trunk, usage of belts, usage of motor, door status (open / closed), how often you have an emergency braking, number of passengers, how often you honk, etc
Environment	N.A.	Weather conditions, temperature, rain, road marking, road signs
Maintenance	Customer account data, vehicle health data	Vehicle ID number, software version, amount of fuel left, tire pressure, technical faults, etc.
Infotainment and communication	Infotainment data, personal communication data	Voice commands and gestures to control on board systems like personal assistants. Via Bluetooth connectivity the car gathers the following personal information: calendar, contacts, phone call history, email, messages, browser history, etc.

The reason for gathering these aspects of data is for (De Vries and Van Engers, 2019):

- Legislation purposes: in some countries black boxes to gather data about the car is mandatory, data for possible recall actions, informing users about changes in terms and conditions
- Product improvement: to improve performance, quality and safety of vehicle
- Marketing: inform users about new products, services and events and market research
- Comfort: service notifications, customer service, etc.

3.4.2 GDPR

In this section legislation is included due to its presence - in the form of GDPR -, in contrast to the cybersecurity requirements where legislation of cybersecurity for connected cars does not exist (yet). This is because GDPR plays a big role in the gathering, processing and distribution of personal data of companies operating in Europe, including connected cars.

GDPR can be seen as a more general guideline for all connected cars functions, with the following main points (Zallone, 2019):

- Privacy by design
- Definition of data retention period
- New standard for data security

The GDPR distinguishes data controllers: parties which offer goods or services, irrespective of whether a payment of the data subject is required or the monitoring of their behaviour takes places within the European Union. Currently, the operation of the connected car concerns many

actors, just like smartphones. Connected cars consist of mechanical as well as digital parts (hardware and software). This means involved parties are the manufacturer of the mechanical part, the digital HW manufacturer, the SW manufacturer, the provider of connectivity, etc. Most of these players will use the data that is collected when the car is in use. These data are personal data, in as much as they point to the use made by a natural person. With so many players involved in different roles, the very nature of connected cars makes it difficult to understand who the data controller will be (Zallone, 2019).

Another aspects Zallone (2019) touches upon is privacy by design. Here a controller must use all measures to mitigate the risks connected with the future processing of personal data. However, it is difficult to list all measure that may be taken to implement this principle, who may vary depending on the scope of the processing, the kind of data used, size and complexity of the IT infrastructure.

The last aspect is security. The GDPR does not have a list of security requirements, but simply uses one word: the security measures must be “adequate”. The adequacy of the security must be evaluated on the basis of very clear parameters, security measures must be adopted “taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing,” according to the GDPR.

However, this leads to questions as: what is the exact application of adequate: does a adequacy test mean that every system must be safe from all and any hacking? That loss of data must be impossible, and all measures have been taken to avoid these risks? These questions the GDPR does not specifically answer and therefore this law is only applicable to a smaller scope instead of mentioning specific (technical) requirements regarding the connected car, telematics and V2X.

3.4.3 Permission

We identified three publications focusing on the permission side of data gathering from the user perspective. First, Akalu (2018) mentions how current privacy policies are an individual matter: individuals give permission to collect, process and distribute their data. As a result, whether a privacy violation has occurred (or not) depends on whether a reasonable person would consider collection, use and disclosure of personal data appropriate in the circumstances.

The control of data cannot be considered meaningful when the individual is unable to assess the risk associated with disclosing personal information. Without a clear emphasis of what the individual is entitled to control, privacy rights can be presented in a way that provides individuals with no meaningful choice. This is achieved by assuming that the individual has agreed to the use of their personal data when a service is first provided.

Additionally, Akalu (2018) argues how so called ’identifiable information’ (information that is liked or reasonably linkable to (a) the vehicle from which the information was retrieved, (b) the owner of that vehicle or (c) the registered user using vehicle technologies and services associated with the vehicle from which the information was retrieved) both cover the personally identifiable information and business practices of the manufacturers. When data is shared among multiple recipients, it is appropriate that connected car companies provide information about their data sharing network and take responsibility for its conduct.

In the contrary, Walter et al. (2017) shows quantitatively how via a new usability focused user interface, users have a better sense of where they give permission to, stating that the transparency and intervenability required by the GDPR in connected vehicular services do not fulfill these requirements. Most users do not understand the implications of their privacy decisions, a statement in line with De Vries and Van Engers (2019). Therefore a usable approach is re-

quired that enables users to decide on their informational privacy in the connected car in a self-determined manner (Walter et al., 2017).

Lastly, the systematic mapping study from Ram et al. (2018) analyses research from multiple articles study and states what aspects where focused upon and which solutions were proposed. The principle of “privacy by design” is backed by as a safeguard against insecure system architecture. These privacy principles are, however, not adopted in dealing with concerns like privacy under “identity management.’ Instead, proposed solutions rely heavily on cryptography and pseudonyms. Only a couple of studies, according to Ram et al. (2018), argue for the need to address the insecure system design or infrastructure to safeguard privacy. Ram et al. (2018) conclude that in general many proposed (technical) solutions in the privacy-area are not empirically validated.

Instead, for V2X only 2 sources were found, while all the remaining publications focused on the security of the vehicle itself (e.g. internal architecture of ECU’s). It is stated by Tbatou et al. (2017) that ’in the network layer of a connected car, the most prominent security issues are with respect to the integrity and authentication of the data that is being transported in the network’, whilst confidentiality and authorisation are also mentioned as security requirements. The article of Macher et al. (2017) gives several security levels of which V2X can apply to, but is not bounded to. If those security requirements are to be analysed, level 1 until 3 are the most common among (future) V2I projects based on the functionalities and current state of security in these projects.

Summarised, we argued that in many proposed (technical) solutions in the privacy-area are not empirically validated. The amount of papers used for answering this RQ (7) is the lowest of any RQ, indicating the lack of available literature regarding this aspect. This is backed up by the fact that no information about privacy requirements about V2X infrastructure specifically was found. For further research, therefore, available guidelines on a European legalisation level combined with GDPR are more of value than solely focusing on literature. Therefore the privacy requirements were dismissed in this research when creating the framework.

3.5 Assessing Risks Regarding Cybersecurity

In the following section we answer RQ 2 and 2.1, in this order. We first look at the most mentioned aspects in frameworks, methods, best practices etc. regarding analysing cybersecurity and privacy are described. We do this in order to get a complete picture of these methods. This answers RQ 2: 'What is the current state-of-the-art in literature regarding analysing cybersecurity and privacy risks in the automotive area?'

Following that, we answer RQ 2.1: 'What is the most suitable framework for a risk analysis of V2I projects?' For future research, where risks are going to be analysed (regardless of focusing on telematics or V2X communication) this research question is important to answer. In this section, we identify two suitable risk assessment methods regarding V2X and therefore V2I. The other risk assessment methods are researched in order to create an accurate picture of the area of risk assessment in connected cars in general.

In general, risk estimation methods require the definition of attack likelihoods (or probabilities) and impacts (or severities) (Boudguiga et al., 2015), in line with definition we use of a risk (the probability of an event occurring $\times$ the impact of this event). Cybersecurity goals can be determined based on the results of the threat analysis and risk assessment. Cybersecurity goals may be stated in terms of what to avoid, or the inverse of the potential threat. For example, if a potential threat is 'malicious unintended steering', the cybersecurity goal for this potential threat may be 'avoid or prevent malicious unintended steering'. A single potential threat may have multiple cybersecurity goals, and multiple potential threats may have the same cybersecurity goals. The cybersecurity goals along with their associated risk are used to determine the high level strategy for achieving cybersecurity of the item or system (Walker, 2018). This means RQ 4 and RQ 2 are tied together: first the risks are determined before certain requirements can be defined, proactively or afterwards.

As explained in section 3.3, both ISO 26262 regarding (functional) safety and SAE J3061 regarding (cyber)security have a risk assessment protocol. However, different publications are critical on these processes and aim to improve upon them. For instance, Ando et al. (2018) argues that the used 5W elements in SAE J3061 (where, when, who, why and what) take too much time to confirm threats because for every aspects the possibilities are multiplied, quickly raising to 3000 or more threats. Therefore many publications propose their own risk assessment method, some of which we list below.

First, we analyse the risk assessment protocols of ISO 26262 and SAE J3061, after we list the identified individual risk assessments / frameworks, some of which elaborate on the risk assessment protocol of SAE J3061. The risk assessment framework of ISO 2662 is called the Hazard Analysis and Risk Assessment (HARA). The following definitions will come back often and are therefore listed here. Hazards (ISO 26262) and threats (SAE J3061) are defined as follows:

- Hazard: the potential source of harm to an asset due to unintended failure of the system. Note that the harm is typically restricted to humans or the environment.
- Threat: the potential source of harm to an asset due to attackers.

3.5.1 ISO 26262: HARA

In ISO 26262 HARA is prescribed. When conducting the HARA, faults, and reactions of security mechanisms must be considered as potential causes of hazards. This also includes attacks on the system that can be seen as foreseeable misuse and their handling by the planned security mechanisms. Hazards and their impact is assessed by three parameters: severity, probability

and controllability. Moreover, it also allows the systematical identification of non-safety related security threats based on the STRIDE approach.

STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges. The STRIDE threat model can be seen as the security equivalent to HARA.

ISO 26262 provides an automotive-specific risk-based approach for determining risk classes that describe the necessary risk reduction for achieving an acceptable residual risk, called automotive safety integrity level (ASIL), as mentioned in section 3.3. Integrity levels are an established method to indicate the required level of robustness associated with a risk mitigation solution. They have been specified in various standards such as IEC 61508 and ISO 26262 and are intended to be used throughout an engineering process to determine the level of robustness required and trace whether this level has been met by the final implementation (Beckers et al., 2016). The ISO 26262 standard does not concern threat analysis for malicious attackers or how to select appropriate security countermeasures (Beckers et al., 2016). This problem is tackled by using ISO 27001.

Mixing the safety aspect of ISO 26262 and security aspect of ISO 27001 into threat assessment and automotive controls is done by Beckers et al. (2016). Via Unified Modeling Language (UML) different safety goals of the car are mapped, focusing on the data integrity of the signals exchanged. Here the safety goals for ISO 26262 are determined, serving as input for risk assessment of ISO 27001, while e.g. relevant situations and reasoning is input for analysing threats. The technical aspects mapped via UML are not within the scope of this research and therefore excluded.

As mentioned above, threats in ISO 26262 can be based on the STRIDE approach of which the Security-Aware Hazard and Risk Analysis Method (SAHARA) collaborates mores (Islam et al., 2016). In the section below, we focus on SAHARA and explain how it relates to STRIDE and connected cars.

SAHARA

The SAHARA concept quantifies the security impact on dependable safety-related automotive system development at a system level. SAHARA was originally focusing on safety, but redesigned for security evaluation (Monteuuis et al., 2018). The SAHARA method is geared towards the needs of an analysis of security threats in the automotive domain at an early development phase, the concept level. The challenge is that the HARA at this preliminary stage is based on incomplete information. Furthermore, for analysis of remote cybersecurity attacks and attacks geared towards whole car fleets, the HARA threat quantification scheme is lacking in terms of measures for damage potential and affected users.

SAHARA classifies the security threats of an automotive system using the STRIDE approach and a special quantification scheme developed for automotive application.

An HARA analysis (right part of Figure 3.3) can be performed in a conventional manner. Attack vectors of the system can be independently modeled using the STRIDE approach (left part of Figure 3.3) by specialists of the security domain. The SAHARA method applies automotive safety integrity level (ASILs, see also section 3.3 and ISO 26262 above), to the STRIDE analysis outcomes. Threats are quantified similarly to ASIL quantification, according to the resources and know-how required to exploit the threat, and how critical the threat is. Security threats that might lead to a violation of safety goals can be handed over to HARA for further safety analysis (Macher et al., 2017).

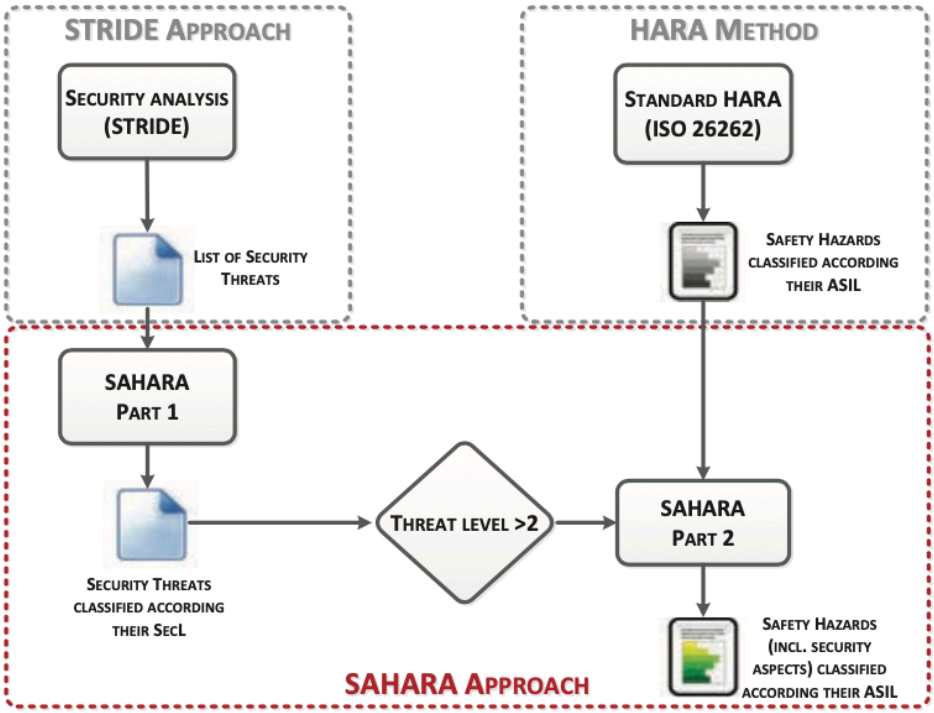

Figure 3.3: From HARA and STRIDE to SAHARA

Macher et al. (2016) mentions how SAHARA achieves easy classification of threats in combination with STRIDE threat modeling. The basic classification aligned with ASIL classification is therefore optimal for use in combined security and safety engineering processes. However, Monteuuis et al. (2018) argue that SAHARA does not allow interactions between security risks and safety metrics, although as explained in section 3.3.1, these concepts do have significant overlap. Furthermore, the threat model STRIDE is used, which does not consider authentic messages with false data attacks. Lastly, STRIDE fails to consider attacks with multiples security goals (Monteuuis et al., 2018). So although using SAHARA for a risk assessment could be done, the closed source documents its based upon (ISO 26262) forms the main reason not to use it in this research.

3.5.2 SAE J3061: TARA

The SAE J3061 and corresponding Threat Analysis and Risk Assessment (TARA) is described in the article of Schmittner et al. (2016). The objectives of the TARA is to identify potential threats and to assess the associated risks, which helps us to prioritise cybersecurity activities in terms of efforts and resources (Schmittner et al., 2016).

Specifically, during the TARA it must be examined whether planned safety mechanisms and the defined safe states could be exploited by an attacker, e.g. to influence the availability of assist functions negatively. Naturally, the possible impact of threats and associated attacks on functional safety must be checked as well. It should be noted here that there is no direct correspondence between the ASIL rating of a safety goal and the risk associated with a threat that can lead to a violation of this safety goal. This is because only the impact factor of the risk is influenced by the ASIL rating while the probability factor is independent of it (von Wedel and Arndt, 2018).

TARA is defined as ‘an analysis technique that is applied in the concept phase to help identify

potential threats to a feature and to assess the risk associated with the identified threats.' There are three steps involved in TARA (and risk analysis in general):

1. Threat identification
2. Risk assessment (includes classification of the risk associated with a particular threat)
3. Risk analysis, which ranks threats according to their risk level

The SAE J3061, however, does not give any restrictions on how to execute the TARA assessment. It is quoted how 'it is left to an organisation to determine which TARA method is appropriate for their purposes, and to determine what an acceptable level of risk means ...' Examples mentioned in SAE J3061 to execute the TARA assessment are the EVITA method, TVRA and attack trees (Macher et al., 2016). In the sections below, different methods to execute HARA are listed, starting with TVRA.

TVRA

Threat, Vulnerability and Risk Assessment (TVRA) classifies system assets based on their nature, complexity of construction and lifetime. This classification serves to assess the impact of harming an asset. Computing the attack severity S as the sum of an asset impact (Ai) and the intensity factor (I). TVRA defines 3 levels of asset impacts ranging from 1 to 3.

As such, TVRA final attack severity S is computed as S = Ai + I with a truncation to 3 if $S > 3$ (Boudguiga et al., 2015). Islam et al. (2016) argue that TVRA requires a good understanding of Common Criteria (which is a document of more than 400 pages as part of the ISO 15408), and is not aligned with any safety standards, which are downsides to the method. Lastly, TVRA is not exclusive to the automotive domain and only focused on telecommunication threats (Monteuuis et al., 2018). However, we did find other risk assessment methods like RACE elaborating on TVRA, therefore we chose to include the base of TVRA in this research.

The most mentioned (original European) risk assessment method we encountered in our literature review is EVITA, outlined below.

EVITA

EVITA defines attacks using attack trees where the attack goal is the tree root. This goal is reached through one or more attack objectives. The attack tree expresses all possible attack elements and provides both a logical approach and a visual means of identifying the threats and vulnerabilities by determining which event must be generated for an attack to be successful (Kong et al., 2018). Each objective is achieved by one or more attack methods which are composed of elementary attacks on system assets. Attacks on system assets serve to compute the attack probability (i.e. likelihood) while attack objectives are used to evaluate the attack impact (i.e. severity).

EVITA considers attack severity as a vector formed by the following components (Islam et al., 2016), (Macher et al., 2016):

- Safety: the safety component (SS) evaluates the attack damages to driver and passengers lives.
- Privacy: the privacy component is related to personal data exposure and vehicle identification and tracking.
- Financial: the financial component (SF) quantifies economical - direct or indirect - losses for users, car manufacturers or other stakeholders.

- Operational: the operational component - which has little or no safety or financial impact - describes the impact of the attack on vehicle performance, affecting manufacturer corporate image (for instance the loss of secondary functionalities such as cruise control, or comfort and entertainment systems such as music streaming or air conditioning.)

In addition, EVITA specifies five severity levels (S) for each tuple. An S level of 0 corresponds to no risk while an S level of 4 corresponds to a critical situation for many individuals or cars.

Macher et al. (2016) states that EVITA is a suitable approach for concept evaluation, but requires too many details for classification. These details are estimated based on concept design and therefore involve the disadvantage of a huge potential for discussion. The separation of functional, safety, privacy and operational severity adds further potential for discussion but does not result in a significant difference in the resulting risk level. There is too much classification effort based on estimations for the concept evaluation phase (Macher et al., 2016).

Islam et al. (2016) furthermore mentions how a detailed study of the different impacts in the attack severity is missing. Also, EVITA does not take legislation aspects into account, even though several laws regarding the environment and driver behaviour are already in effect, and there are threats that can potentially lead to the violation of those legislative requirements.

3.5.3 V2X

In this section, we describe two risk assessment methods we identified specifically regarding V2X communication. The first is described in the article of Sabaliauskaite et al. (2018) proposing of a framework with ISO 26262 and SAE J3061 in mind, while also taken into consideration EVITA, TVRA and RACE (listed below), focused on V2X communication. Sabaliauskaite et al. (2018) claims that 'to the best of the authors' knowledge' there are no international standards for designing V2X systems as of yet. Therefore the authors proposed an approach for safety and cybersecurity risk analysis in V2X, where the likelihoods (probabilities) and impacts (severities) have to be determined in order to estimate risks. The following steps are executed:

1. Attack potential:
    - Three levels of attackers' knowledge, K, are identified: 0 - attackers do not require prior knowledge of the V2X system. 1 - attackers need some basic knowledge or some basic understanding of the V2X system. Level 2 - attackers need comprehensive domain knowledge.
    - The equipment required to perform a successful attack, R, can also be assigned to three levels: 0 - no special equipment is needed. 1 - standard equipment is needed, which can be easily obtained. 2 - specialised, not easy to obtain equipment is required.
2. Attack severity (deducted from EVITA, mentioned above) (S): safety, privacy, financial and operational, with four severity levels ranging from 0 to 3.
3. Vehicle automation level (L): low (levels 1 and 2), medium (level 3), and high (levels 4 and 5).
4. Cybersecurity values: using the attacks' total severity S, potential P, and vehicle automation level L values, the cybersecurity Risk Level (CSRL) can be determined.

RACE

A risk assessment method for specifically V2X communication is described in Boudguiga et al. (2015), called Risk Analysis Method for Cooperative Engines (RACE). RACE is compatible

with TVRA. There are four aspects to be determined: a) attack description b) attack likelihood c) attack severity and d) the risk analysis.

A) Boudguiga et al. (2015) proposes to limit the attack methods choice to the following items, instead of following the Common Criteria (see TVRA):

- Communicate falsified communication: to lure an asset by sending it wrong information
- Disable equipment function: to exclude an asset by killing it, for example with a denial of service attack
- Execute unauthorised command: to run bad operations on an asset
- Modify equipment function: to change an asset behaviour e.g., by installing a malware or modifying a configuration file
- Recover unauthorised information: to retrieve driver or vehicle private data

B) The attack likelihood is computed as the inverse of the attack potential i.e., the difficulty of executing an attack, the same as EVITA and TVRA. The attack potential is the sum of the assigned values to the following factors (see also Figure 3.4):

- Knowledge factor: information gathering regarding an asset
- Time factor: the time needed by an attacker to identify and successfully realise an attack, ranging from a few hours to some months
- Expertise factor: the expertise of the attacker
- Opportunity factor: if the attack requires a special window of opportunity to be executed or it can be easily executed. The window of opportunity scales from unnecessary to none
- Equipment factor: indicates whether an attacker needs special equipment to realise an attack

RACE uses three levels to indicate the attack likelihood (A(I)) - from 1 to 3 - , matching with EVITA (mentioned before) and TVRA, see also Figure 3.5.

C) The attack severity consists of four levels, with the same attack severity as EVITA (safety, privacy, financial and operational), but made compliant with TVRA, resulting in four levels of attack impacts and corresponding meanings.

D) Lastly, in the risk analysis the final risk is calculated as follows: $R = C + S \times A(I)$. When the safety factor S is different from 0 (determined at the severity level), a controllability factor (C) is added to risk evaluation. The controllability quantifies the driver influence on avoiding a danger and so reducing the severity. C is classified from 1 to 4 where 1 corresponds to a possible reaction from the driver and so possible harm avoidance. Meanwhile, 4 corresponds to a hazardous situation which cannot be influenced by human response, all in correspondence with EVITA.

Although the method of Sabaliauskaite et al. (2018) could be used for our risk analysis, we chose for the RACE assessment method as our base, because it offers a more detailed implementation of several factors (time, expertise, knowledge, opportunity and equipment) when assessing the likelihood of an attack. However, both the frameworks use the attack severity classification of EVITA (safety, privacy, financial and operational), which strengthens our belief that this classification is generally accepted and can be used in our risk analysis.

Factor	Level	Description	Value
Elapsed time	1 day		0
	<1 week		1
	<1 month		4
	<3 months		10
	<6 months		17 (13)
	>6 months		19 (26)
	not practical		∞
Expertise	layman	no special knowledge in security	0
	proficient	familiar with security	3 (2)
	expert	mastering security	6 (5)
	many experts	collaboration of multiple experts	8
Knowledge	public	easy to recover	0
	restricted	Developer/company with NDA	3 (1)
	sensitive	Developing team	7 (4)
	critical	few individuals	11 (10)
Opportunity	unnecessary	window of opportunity not needed	0
	easy	(<1 day)+(assets number<10)	1
	moderate	(<1 month)+(assets number<100)	4
	difficult	(>1 month)+(assets number>100)	10
	none	window of opportunity is negligible	∞
Equipment	standard	Already available for the attacker	0
	specialized	Not available but easy to get	4
	bespoke	Expensive and not available	7
	multi-bespoke	Different types of bespoke are needed	9

Figure 3.4: Rating Values of Attack Potential Factors

Risk value	Description
[1,2]	**Minor** risk: no primary need for countermeasures
[3,5]	**Major** risk: likely to occur but not fatal, countermeasures should be applied
>6	**Critical** risk: should be minimized with highest priority

Figure 3.5: Classification of Risks using RACE

3.5.4 Privacy Assessment Framework

Regarding frameworks / assessments specifically focused towards privacy, we could not identify many publications, except for one article of Xiong and Lagerström (2019). This article focuses on the privacy extension of a security analysis of vehicle based on VehicleLang, which is a probabilistic modeling and simulation language for vehicular cyber attacks, and can be used to design vehicles IT infrastructure and analyse its weaknesses. Xiong and Lagerström (2019) argue that geo-location is the most valuable privacy sensitive data, more important than vehicular sensor data, biometrics data and behavioural data.

The article, however, does not propose a general risk assessment from a privacy perspective but rather a (technical) solution in the form of Local Differential Privacy based on the Meta

Attack Language, which is out of scope for this review. Lastly, the technical focus combined with the lack of focus on information security, makes this framework not practical to use for further research.

4 EUROPEAN SECURITY DOCUMENTATION

4.1 Organisations

This chapter will explain the existing European security documentation regarding V2X communication, therefore answering RQ 3: 'How does existing European documentation regarding security in V2I collaborates to the identified security requirements in literature?'

To answer this question, in total 10 organisations were analysed, which were selected based on the input of two experts in the connected car area. These organisations produce a diverse set of documents, ranging from standards to guidelines to recommendations / best practices.

Of these 10 organisations, only two provide direct relevant information regarding security requirements and V2I, also indicated in bold below: ETSI and CEN / TC 278, where the standards from CEN / TC 278 could unfortunately not be obtained because they are closed source. ETSI, ITU and UNECE are used as input for Chapter 5. We list all the 10 organisations below for reproducibility.

The other 6 organisations were out of scope by focusing on other aspects (EEA or CLEPA), did not have any overlap with security (ERTICO), was not focused towards V2X (ERTRAC), only mentions how security requirements could be implemented but not what they were (5GAA) or only processed focused how to achieve a secure automotive organisation (ACEA).

1. UNECE: United Nations Economic Commission for Europe. This organisation has a working party called GRVA regarding Automated/Autonomous and Connected Vehicles. This working party is divided into several subjects, where one is the 'Task Force on Cyber Security and (OTA) software updates.' The task force consisted of members of representatives from contracting parties and non-governmental organisations. The used security standard of UNECE does not focus solely on V2I but rather on the connected car as a whole, giving several 'cybersecurity principles' which can be used to demonstrate how organisations should implement cybersecurity over the lifecycle of the vehicle, used as a base for European regulation in order to achieve type approval of a vehicle. Since these specific security principles are not focused towards communication, they are not included in the analysis below. However, the documentation contains a list of vulnerabilities and measures which are used in this research.
2. EEA: European Environment Agency, an agency of the European Union. Monitors registrations of all European vehicles.
3. CLEPA: European Association of Automotive Suppliers, consisting of over 100 of the world's most prominent suppliers for car parts.
4. ERTICO – ITS Europe: a public-private partnership of 120 companies and organisations representing service providers, suppliers, traffic and transport industry. This organisation is goal-oriented towards future possibilities regarding Intelligent Transport Systems.

5. **ETSI**: European Telecommunications Standards Institute. Creates standards regarding ICT, including automotive. Officially recognised by the EU as a European Standards Organisation.
6. ERTRAC: European Road Transport Research Advisory Council. Define strategies and roadmaps regarding transportation in Europe.
7. 5GAA: 5G Automotive Association. Consists of over 130 organisations, including automotive manufacturers, suppliers, chipset/communication system providers, mobile operators and infrastructure vendors. Goal is to develop end-to-end solutions for future mobility and transportation services using 5G.
8. ITU: The International Telecommunication Union (ITU) is the United Nations specialised agency for information and communication technologies. The Study Groups of ITU's Telecommunication Standardisation Sector (ITU-T) assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of ICT. Also develop technical standards, including V2X communication. These are, however, not open source. We could find a public presentation containing information about vulnerabilities in V2X communication.
9. **CEN / TC 278**: Responsible for managing the preparation (but not creation) of standards in the field of Intelligent Transport Systems (ITS) in Europe. Works together with ETSI, ERTICO and ISO.
10. ACEA: European Automobile Manufacturers Association. Main standards group of the automobile industry in the European Union, including cybersecurity regarding connected cars.

Based on the documentation that we could obtain, high-level security requirements are deducted which in turn are merged into the already identified security requirements in the structured literature review in Chapter 3.

Security documentation are different from wireless communication standards in the sense that communication standards like ITS-G5 or 4G / 5G are enablers of the security documentation. There is, however, currently no wireless communication standard between intelligent roadside units and connected cars. Whichever technique will be used (e.g. 4G & 5G and ITS-G5), the picked security requirements are independent of this, leaving this discussion and future developments outside the scope of this research.

In the sections below, we will describe the security requirements we have identified extracted from the ETSI standards and why these are selected by matching it to V2I functionality. We also explain why CEN/TC 278 is relevant for this research but could not be used. Lastly, we explain the degree these requirements match the security requirements we identified in Chapter 3.

4.1.1 ETSI

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies (Ivanov et al., 2018). ETSI has in total six public technical specifications (TS) under the category security of Intelligent Transport Systems (ITS), listed below.

1. ETSI TS 102 731: ITS Security: Security services and architecture (2010)
2. ETSI TS 102 940: ITS Security: Communications security architecture and security management (2018)

3. ETSI TS 102 941: ITS Security: Trust and privacy management (2019)
4. ETSI TS 102 942: ITS Security: Access control (2012)
5. ETSI TS 102 943: ITS Security: Confidentiality services (2012)
6. ETSI TS 103 097: ITS Security: Security header and certificate formats (2017)

It is important to note that these technical specifications are not mandatory to be used by third parties. They are only approved by the technical committee of the organisation that created the standard in the first place.

The first five of these standards are analysed below in this research in order to extract relevant security requirements regarding V2I communication. Standard number 6 about security headers and certificates formats is specified towards technical implementation of how messages can be transmitted on a data level, which is out of scope of this research. The remaining standards of ETSI have overlap with each other. Therefore some standards may have less relevance or are shorter in this research, but individually analysed they are relevant to the topic of security in V2I communication.

4.1.2 CEN/TC 278

There are several relevant standards this institution develops, the most important regarding security and V2X are:

- CEN/TS 21177: Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices. This standard details how to set up session and sequence diagrams. Unfortunately, this standard is being published by the ISO and therefore closed source and could not be used in this thesis.
- CEN/TR 21186: Cooperative intelligent transport systems — Guidelines on the usage of standards, part 3: security. This document explains the necessary framework needed for deployment of secure ITS services, specifically the usage of the various technical security means (ITS-Station services) relevant for ITS, considering both the broadcast information dissemination (signing of messages) and unicast communications (sessions). This standard is at the moment of writing this research not yet publicly available but could be used in further research once available.

4.2 Security Requirements

There are different requirements stated by ETSI per application category of ITS. The first one is Cooperative awareness (see also Table 4.1) which has different use cases.

There are different categories, sub-categories, applications and use cases for V2I communication. On one hand, there are the strictly safety-related broadcasted messages, which is the message to be analysed here. These messages either are so-called Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Message (DENM). In Table 4.1 the categorisation, sub-categorisation and examples of use cases are outlined.

Many of the applications and services as mentioned in Table 4.1 are based on the transmission of broadcast messages which are intended to be viewed and processed by all recipients. Consequently, there are according to the ETSI standard no confidentiality requirements associated with these messages other than the protection of the sender's identity.

The confidentiality of transmitted information is protected primarily by the encryption of messages within an established security association such that it can only be decrypted by the re-

Table 4.1: Functions of V2I according to ETSI

Category	Sub-category	Use cases
Active road safety	Cooperative awareness (CAM)	• Emergency vehicle warning
	Static hazard warnings	• Wrong way driving warning (infrastructure based) • Signal violation warning
	Area hazard warnings (DENM)	• Stationary vehicle - accident • Stationary vehicle - vehicle problem • Traffic condition warning • Roadwork warning
Cooperative traffic efficiency	N.A.	• Regulatory/contextual speed limits notification • Curve warning (i.e. sharp bend coming up)

cipient to whom it is addressed. The true identity of the sender of broadcast ITS messages is kept confidential by ensuring that all such messages are sent pseudonymously.

Another message type is multicast. This a message sent to several specific vehicles, e.g. public transport information or point of interest notification. Finally, unicast is messages specific to one vehicle only, e.g. warning of collisions or theft-related services or traffic information. With multicast and unicast, applications are assumed to be offered by several providers and, possibly, to be commercially sensitive. Therefore, the requirements depend heavily on the specific application and the respective business model (ETSI, 2019). Furthermore, these messages will be created in order to give an incentive to gain commercial benefits. This means these type of messages are dismissed in this research.

ETSI mainly differentiates security requirements between authentication and authorisation, with an additional focus on confidentiality, if applicable. In below sections, the security requirements are categorised by kind of message, followed by the specific security requirements (indicated by bold font) and a description of how these requirements can be fulfilled according to the ETSI standards (ETSI, 2018).

The categorisation of messages linked to specific functionalities can be found in Table 4.1 below.

The security requirements per goal and sort of message are as follows (ETSI, 2018):

- Cooperative awareness (CAM)
  - **Authentication**: different levels of authentication may be needed depending on the application and the requirements for participation. Consequently, authorisation (below) may depend on status (e.g. vehicle priority) or properties (e.g. sensor equipment, vehicle type).
  - **Authorisation**: What different parties are allowed to do:
    - Basic CAM messages: linked to basic data such as speed, heading, acceleration and brake status of a vehicle. Granted to all enrolled ITS stations to enable participation in the basic ITS. For the basic communication structure of a CAM message, including the relevant communication parties, see also Figure 4.1. The orange colour means the exchanging of a message while the authorities involved in this process have all obtained a different colour.
    - Authorisation to claim priority rights for emergency vehicles:

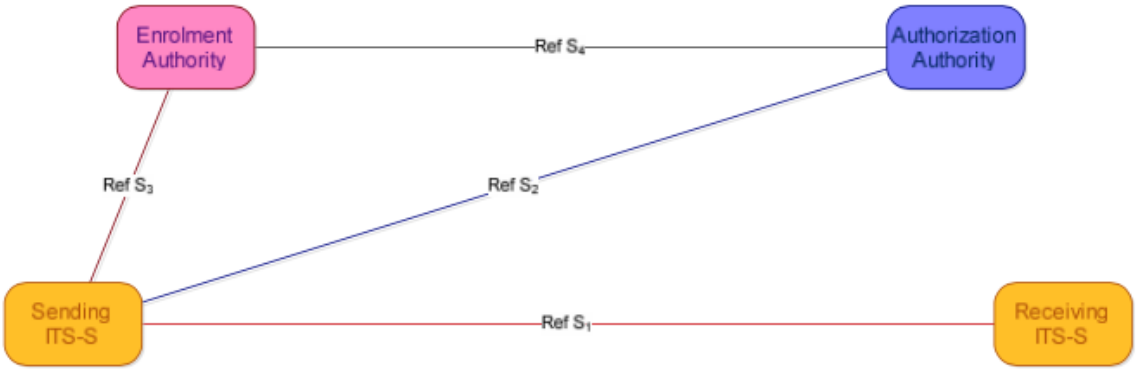

Figure 4.1: ITS Security Reference Model for CAM (ETSI (2018))

        - granted only to specially authorised emergency vehicles or public transport vehicles according to national legislation. Multiple layers of priority may be defined, for example priority for emergency vehicles and on a lower level authorisation to use a special lane reserved for public transportation
    - Authorisation to state regulatory orders such as speed limits and road closures
        - granted only to specially authorised ITS stations such as RSUs (Road Side Unit) and police vehicles
        - granted by a governmental organisation or its authorised proxy agency
  - **Confidentiality**
    - As CAMs are broadcasted to any possible receiver there are no confidentiality requirements
- Static local hazard warnings
  - **Authentication and Authorisation** have very similar properties as the CAM service with the exemption that they are sent by RSUs. For authentication and authorisation similar requirements as for CAM apply with the addition, that authorisation should be limited to the specific purpose, functionality, and location of the respective RSU.
  - **Confidentiality**
    - As the nature of the service is to broadcast and the sender is a static RSU, no confidentiality requirements apply
- Area hazard warnings (DENM)
  - **Authentication and Authorisation:** Authorisation for area hazard warnings could be granted on several levels depending on sensor equipment, sensor quality and processing capabilities of the ITS (can be both a station or a personal vehicle). Apart from that, similar requirements as for CAM apply.

    For the communication structure of DENM including the relevant communication parties see also Figure 4.2. The orange colour means the exchanging of a message, while the authorities involved in this process have all obtained a different colour.
  - **Confidentiality**
    - No confidentiality services are required

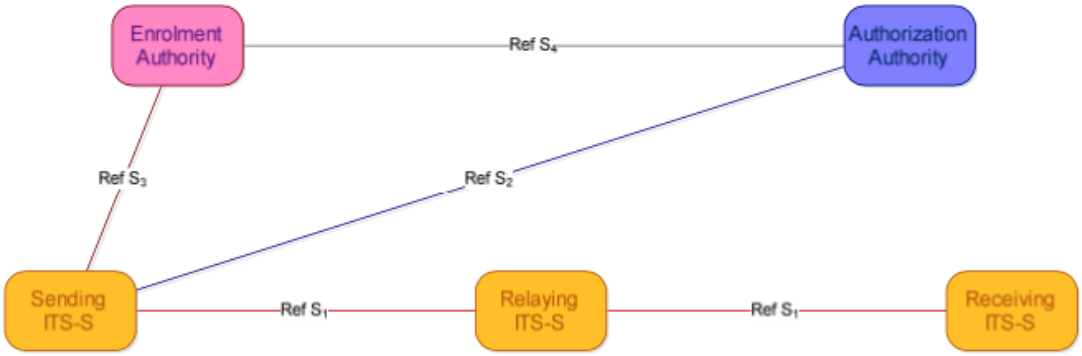

Figure 4.2: ITS Security Reference Model for DENM (ETSI (2018))

ETSI also describes how the authorisation process should be designed and implemented. All these techniques can be found in Appendix D.

Furthermore, the document of ETSI (2010) describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorisation. The information flows describing the reference architectures are included in Appendix E, e.g. obtain / update / remove enrolment credentials, obtain / update / remove authorisation, etc. This way specific V2I projects can be guided towards security requirements and the corresponding technical implementation if necessary.

4.3 Combining Security Requirements from Literature and European Security Documentation

In this section, the requirements of literature described in section 3.3 are compared to what ETSI stated. It is important to emphasise that literature does not specifically go into detail of security requirements regarding V2I. Instead, as we mentioned before, for V2X only 2 sources were found, while all the remaining publications focused on the security of the vehicle itself (e.g. internal architecture of ECU's).

To repeat, the security requirements in literature regarding V2I are:

- Confidentiality (4): e.g. protect communication channels against data theft
- Authentication (3): e.g. prevent manipulation of messages
- Authorisation (3): e.g. prevent unauthorised access to network
- Integrity (2): e.g. verify integrity of message against manipulation
- Availability (2), e.g. check volume of messages or detect abnormal behaviour of messages
- Non-repudiation (2): e.g. verify origin of message

The difference between literature and European documentation is shown in Table 4.2. Here with a '+' sign the presence of a security requirement is indicated, while with a '-' sign the absence is indicated.

The most obvious difference is that of the addition the importance of confidentiality. The reason confidentiality is mentioned the most in literature is because of the article by Macher et al. (2017) focusing on encryption and therefore protecting the confidentiality of received and send messages.

Table 4.2: Difference in Security Requirements between Literature and European Documentation

Requirement	**Literature**	**European Documentation**
Confidentiality	+	+
Authentication	+	+
Authorisation	+	+
Integrity	+	-
Availability	+	-
Non-repudiation	+	-

However, as seen in the above section, confidentiality is specific to certain messages. For instance, in V2I projects broadcasted messages meant for multiple vehicles (e.g. road works ahead or closed lane) send from the infrastructure to a vehicle, confidentiality is not important. However, if a message from an emergency vehicle to other personal vehicles to make way is send via infrastructure, the message should be encrypted in order to prevent spoofing attempts of that message.

Furthermore, integrity, availability and non-repudiation are not mentioned in the ETSI standards, but are, however, very important for V2I because of certain risks V2I projects are exposed to. These risks, mapped to the corresponding security requirements, are shown in section 5.2.

In general, it can be stated how the security requirements mentioned in literature form the base, upon which the European standards - in the form of the ETSI Technical Specifications - elaborate and specify upon.

The above security requirements will be used to map the corresponding vulnerabilities and form the base of the final framework of this thesis.

5 RISK ANALYSIS OF V2I PROJECTS

In this chapter, a risk analysis of V2I projects is executed. This is done by using the RACE framework as described in section 3.5 since we argued this is the most suitable framework regarding analysing V2I. With this risk analysis, we answer RQ 4: 'What are the most important risks an V2I project is exposed to regarding communication on a data level?'

The outcome of the risk analysis will be a quantitative list of most important risks to least important risks. These risks and corresponding risk values are used as input for the final framework.

In this chapter, we will execute a risk analysis, which is started by a risk assessment. As briefly mentioned in section 3.5, the difference between the two is that a risk assessment is a classification of the risks, while a risk analysis extents the assessment by ranking the vulnerabilities according to their risk level. In this chapter we will outline the process of the risk analysis.

As mentioned in the introduction, we view V2I as both communication between the roadside unit (RSU) and the vehicle itself and visa versa. This means risks between the RSU and vehicle affect both the vehicle and the RSU and therefore are not separated. In the classification below, risks are therefore not divided in vehicle or RSU, in contrary to some standards like ETSI 102 893 and the UNECE.

For example, if a denial of transmission is executed on the vehicle, prohibiting sending a message that the vehicle is standing still on a lane due to a mechanical failure, this affects the system of V2I as other vehicles also do not get that (potentially) critical message. This denial of transmission affects the system as a whole and not only the vehicle itself.

The other way around also holds true: if a DDoS attack is being executed on the roadside unit, prohibiting it sending any message to any vehicle, it cannot warn vehicles that a stranded car is in the middle of a lane, again affecting the whole system and not just the roadside unit.

We also noticed that in the analysed European documentation the term 'threat' was oftentimes used instead of a vulnerability. In this research, the following definitions are used. A threat is a party (an organisation, a person, a country) which can potentially misuse a vulnerability (a weakness in the system). The usage of these definitions are in accordance with ISO 27001.

5.1 Used Sources

Documents of UNECE, ETSI 102 893 and ITU are analysed and summarised, see also section 4.1. We briefly explain these three documents below.

5.1.1 UNECE

The working version of security standard document of UNECE as of December 2019 contains a list of vulnerabilities, possible mitigations and attack methods related to connected cars which we used as input. However, as noted within the document, new vulnerabilities and attach

methodologies emerge over time, making the list not exhaustive. Furthermore, since all meetings and documents of the working party are public, we determined this list has structurally not been changed since the middle of 2019 and could therefore be used.

5.1.2 ETSI

The document of TR (2017) contains a comprehensive overview of (high level described) vulnerabilities for an ITS system, including given values of executing a certain attack and a list of countermeasures.

5.1.3 ITU

In a public presentation of ETRI (see also 4.1) as part of working group 17 of the ITU given in 2017, several vulnerabilities per security requirement were outlined. One of the goals of this presentation were to provide security guidelines for V2X communication systems, lying within the scope of a V2I system (Lee, 2017). This document is in beneath section used to extract relevant vulnerabilities of V2I.

In the sections below, we first make a categorisation of the identified vulnerabilities. We do this by mapping the vulnerabilities mentioned in the document of UNECE to that of ETSI (TR, 2017). This categorisation as a whole can be found in Appendix G in the first two columns.

At the same time, with the categorised vulnerabilities, we map the corresponding attack methods. If an attack method is from the ITU this is mentioned within the brackets behind the relevant attack method.

Lastly, in our categorisation of vulnerabilities, we also map the security requirements mentioned in section 3.3 to the vulnerabilities and therefore corresponding attack methods. This way, the vulnerabilities are grounded from both European documentation and literature.

5.2 Categorisation of Security Requirements, Vulnerabilities and Attack Methods

The article of Ivanov et al. (2018) distinguishes three categories in which attacks of V2X can be placed:

1. Infrastructure domain: includes vehicle manufacturers (supply chain), service providers (emergency services, billing, etc.), and trust authorities (TA).
2. V2X domain: is representing all the V2X communications, such as the communication between vehicle on-board unit (OBU) and road-side units as well as the communication between neighbouring vehicles (V2V).
3. In-vehicle domain: consists of the trusted platform modules (TPM), application units (AU), and electronic control units (ECU).

In the risk analysis below, vulnerabilities of all three categories were encountered, although V2X communication at point number 3 is limited to V2I specifically. Furthermore, risks regarding the in-vehicle domain are important, but cannot be specified for every car since the details regarding risks differ per car.

In the document of UNECE, only two main relevant vulnerabilities were identified which we will use from this point onwards:

1. Vulnerabilities regarding back-end servers
2. Vulnerabilities to vehicles regarding their communication channels

Of these two main vulnerabilities, different so called 'sub-levels' of vulnerabilities are identified. These are the most important vulnerabilities for further reference in our framework, stated in the second column. The specific attack methods are described in the third and last column, and as mentioned, are based on both UNECE and ITU.

Table 5.1: Vulnerabilities regarding Back-end Servers

Security Requirements	**Vulnerability**	**Attack Methods**
Authorisation, Authentication	Back-end servers used as a means to attack a vehicle or extract data	• Abuse of privileges by staff (insider attack) • Unauthorised internet access (enabled for example by backdoors, unpatched system software vulnerabilities or other means) • Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server) • Attack on infrastructure: attack on infrastructure is attack when an attacker sends false malfunctions to innocent vehicles. This attack makes CA revoke permission for the innocent vehicle (ITU).
Availability	Services from back-end server being disrupted, affecting the operation of a vehicle	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on
Authorisation, Confidentiality	Data held on back-end servers being lost or compromised ("data breach")	• Abuse of privileges by staff (insider attack) • Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers • Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities or other means) • Unauthorised physical access to the server (conducted for example by USB sticks or other media connecting to the server) • Information breach by unintended sharing of data (e.g. admin errors)

Table 5.2: Vulnerabilities to Vehicles regarding their Communication Channels

Security Requirements	**Vulnerability**	**Attack Methods**
Non-repudiation, Authentication, Authorisation, Integrity	Spoofing of messages or data received by the vehicle	• Spoofing of messages by impersonation • Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road) (also mentioned by ITU) • Impersonation attack: Attacker can pretend to other entity by stealing other entity's ID information. Attacker can receive a message which is sent to another entity and attacker can send a message which is generated by a specific entity. For example, if attacker can pretend to an emergency vehicle, it can send a message like "I am an emergency vehicle, thus move away on my direction" to other vehicles. (ITU, also 11.2) • Credential manipulation: Credential manipulation means modifying the vehicle's private key or ID. Attacker can use other vehicle's credential information without authorisation (ITU).

Security Requirement	Vulnerability	Attack Method
Authorisation, Integrity, Confidentiality	Communication channels used to conduct unauthorised manipulation, deletion or other amendments to vehicle held code/data	• Communication channels permit code injection, for example tampered software binary might be injected into the communication stream • Communication channels permit manipulation of vehicle held data/code, i.e. sensor information manipulation: attacker modifies a physical address of the communication module or manipulates ECU sensor information such as a speed sensor (ITU). • Communication channels permit erasure of vehicle held data/code • Communication channels permit introduction of data/code to the vehicle (write data code)
Confidentiality, Non-repudiation, Authentication	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks / Messages received by the vehicle (for example V2X or diagnostic messages), or transmitted within it, contain malicious content	• Routing message manipulation attack: a malicious intermediate node modifies the message. Therefore vehicles can receive a forgery information. (ITU) (see also spoofing of messages) • Malicious diagnostic messages (i.e. of defect car creating false V2I message) via man in the middle attack/ session hijacking • Replay attack, attacker can intercept V2V message nearby vehicles and V2I message of RSUs. Later, attacker can replay those messages or information for the malicious purpose, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway (ITU)
Confidentiality, authorisation	Information can be readily disclosed	• Gaining unauthorised access to files or data (i.e. through allowing unauthorised access to sensitive files or folders) • Eavesdropping: Attacker can sniff V2V message nearby vehicles and V2I message of RSUs. Attacker can analyse traffic information by sniffing message (ITU)
Availability	Denial of service attacks via communication channels to disrupt vehicle functions	• Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner • Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
Authorisation	An unprivileged user is able to gain privileged access to vehicle systems	An unprivileged user is able to gain privileged access, for example root access, i.e. unauthorised access to credentials: attacker can access a private key and certificate without authorisation (ITU).

Note that the vulnerability 'Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks' (fourth last in the second table) and 'Messages received by the vehicle (for example V2X or diagnostic messages), or transmitted within it, contain malicious content' were merged into one instance. This is done because UNECE sees them separate because of the before mentioned separation of an RSU and vehicle. The merge is made because, as explained before, we see a vulnerability as a threat to the (functioning of) whole system, not to one of the individual instances itself. In addition, the two separate vulnerabilities were mapped to the same threat group in ETSI 102 893 with the same given values for executing this attack (see also Appendix G).

5.3 Risk Analysis

For the risk analysis, the framework called RACE (Risk Analysis Method for Cooperative Engines) will be used, as in correspondence with section 3.5.

In order to estimate a risk, we assume that an attack always succeeds. Theoretically speaking, a vulnerability is being used via an attack by a threat, as mentioned at the beginning of this chapter.

Also, for this risk analysis, it is assumed that all of the functions mentioned in Table 4.1 are applied in practice in order to estimate the potential risk, although this should not always be the case in real life V2I projects where often a subset of the potential functionalities of a V2I project has been chosen.

The proposed attack methods of Boudguiga et al. (2015) of the RACE framework will not be used, but are replaced by the vulnerabilities we identified in Tables 5.1 and 5.2.

In the sections below we will explain the process of the risk analysis, starting with how we used the RACE framework, followed by the quantification of risks by assessing the severity level, likelihood and impact of the available attack methods on a vulnerability.

5.3.1 Adjustments to RACE framework

When using the RACE framework of Boudguiga et al. (2015), several adjustments / improvements are made in order to specifically fit V2I projects.

First, the knowledge metrics (see Figure 3.4) of the RACE framework are not very fitting regarding V2I projects. Therefore we propose different criteria. For the factor 'opportunity' the number of assets is disregarded due to its irrelevance in estimating the time window needed for a potential attack. The following categories regarding the aspect 'knowledge' were proposed and used in this risk analysis:

- Knowledge
  - Public: knowledge to successfully execute attack can be easily found on the internet
  - Restricted: knowledge to successfully execute attack can only be found in specific documentation, e.g. literature or technical standards
  - Sensitive: knowledge to successfully execute attack can only be found at the corresponding parties, e.g. manufacturers
  - Critical: knowledge to successfully execute attack can only be found at the developing team, so only a few individuals have access

In addition, in our risk assessment the controllability factor (ranging from 1 until 4) is being taken out of account since this is primarily a safety factor (although security does have influence on safety, see section 3.3). However, the safety factor regarding vulnerabilities are not clear, since the vulnerabilities are described using terms as 'services from back-end server being disrupted, affection the operation of the vehicle' where it remains unclear what operation of vehicle means and therefore the corresponding safety value.

Lastly, 'easy' in the time aspect at the factor 'opportunity' is within one week in TVRA and 1 day in RACE. For consistency, we use here the definition of TVRA, which is one week.

5.3.2 Calculation of Risks

The RACE method contains four aspects to be determined: a) attack description b) attack likelihood c) attack severity and d) the risk analysis. The attack descriptions we have already created in section 5.2, so the other 3 items remain.

Severity Levels of Risks

First, we start with determining the attack severity of potential exploitation of vulnerabilities. The specific ratings of every vulnerability mentioned in Table 5.1 and Table 5.2 can be seen in Appendix F.

Table 5.3: RACE Severity Levels of Risks

Level	Safety	Privacy	Operational
0	No injuries	No unauthorised access to data	No impact on performance of V2I system
1	Light injuries	Access to anonymous or pseudonymous data	Impact not detected by driver, i.e. message is being delivered or sent without delay
2	Severe injuries, with survival	Identification of car or driver	Driver aware of performance degradation of V2I system, i.e. message is delivered or sent with noticeable delay
3	Life threatening, possible death	Driver or car tracking	Significant impact on performance, i.e. failure of V2I system directly connects to a life threatening situation

For the determination of the severity levels, only direct relations between the categories and the vulnerabilities are being assessed. Therefore the financial category is being left out since it is very difficult to quantify direct and indirect damage (both for potential solutions and reputation damage). The remaining severity levels and categories can be seen in Table 5.3.

Also when for instance the vulnerability is 'an unprivileged user is able to gain privileged access to vehicle systems' there are no direct consequences to that action. Only and if the attacker(s) decide to execute malicious actions the safety of a driver comes into danger, but this would differ per goal of the corresponding threat (e.g. white hat or black hat hacker, perhaps attackers only wants to gather information without manipulating functionality).

The outcome of our judgement of all the severity levels can be seen in Appendix F. Notably, all the (sub-levels) of vulnerabilities obtain a minimum value of 2, meaning according to RACE that 'attack damages are not negligible but are not critical for individuals.' In total 6 of the 9 vulnerabilities obtain a value of 3, meaning 'attack results are harmful and dangerous to individuals and cars', see also Table 5.3.

Attack Potential per Vulnerability

After the attack severity, the attack potential per vulnerability is determined. The factors of which the numbers are based can be seen in Table 5.4, with the above-described adjustments taken into account.

The metrics of several similar vulnerabilities stated in ETSI 102 893 are combined when estimating the risk, i.e. when DoS: Denial of Access to incoming messages is only roadside, but denial of access to outgoing messages does not exist roadside in ETSI 102 893. The final attack potential numbers per factor we gave to every vulnerability can be seen in the third column

of Appendix G in the brackets behind every factor. The values are accumulated to the attack potential (column 4). The given numbers are based upon the risk analysis from ETSI TS 102 893 and adjusted where necessary.

Table 5.4: Rating Values of Attack Potential Factors

Factor	Level	Description	Value
Elapsed time	< 1 day		0
	< 1 week		1
	< 1 month		4
	< 3 months		10
	< 6 months		13
	> 6 months		26
	not practical		26 >
Expertise	Layman	No special knowledge required in security	0
	Proficient	Familiar with security	2
	Expert	Mastering security	5
	Many experts	Collaboration of multiple experts	8
Knowledge	Public	Knowledge to successfully execute attack can be easily found on the internet	0
	Restricted	Knowledge to successfully execute attack can only be found in specific documentation, e.g. literature or technical standards	1
	Sensitive	Knowledge to successfully execute attack can only be found at the corresponding parties, e.g. manufacturers	4
	Critical	Knowledge to successfully execute attack can only be found at the developing team, so only a few individuals have access	10
Opportunity	Unnecessary	Window of opportunity not needed	0
	Easy	< 1 week	1
	Moderate	< 1 month	4
	Difficult	> 1 month	10
	None	Window of opportunity is negligible	10 >
Equipment	Standard	Already available for the attacker	0
	Specialised	Not available but easy to get	4
	Bespoke	Expensive and not available	7
	Multi-bespoke	Different types of bespoke are needed	9

Adjustments of the values of ETSI was often done since the vulnerabilities ETSI describes are differently formulated than that from UNECE. For instance, where UNECE describes a DDoS attack as one vulnerability, hindering availability of a service, ETSI separates this into two specific vulnerability groups, also giving different attack values for knowledge required to execute this attack. The values given in this research are based upon the attack methods corresponding to the vulnerabilities described in UNECE, in correspondence to what is used in Chapter 5. In most cases the adjusted values only were changed to one category above or below, in order to accurately represent the identified attack methods of the vulnerabilities.

An example of the need to adjust the given values to a vulnerability is that of the vulnerability 'services from back-end server being disrupted, affecting the operation of a vehicle.' Here, the time required to the attack is reduced to less than a day (value 0) instead of a week (value 1), since now a days a DDoS can easily be purchased on the web.

However, the vulnerability 'denial of services via communication channels to disrupt vehicle

functions' has been rated a 5 (expert) regarding the required knowledge. This is because of the scalability of the attack and different types of vehicles and used communication channels differ per car, and therefore the attack would have to be adjusted.

In general, it can be seen that all attacks can be executed relatively easily regarding the window of opportunity, except two vulnerabilities: communication channels used to conduct unauthorised manipulation, deletion or other amendments to vehicle held code/data, and unprivileged users is able to gain privileged access to vehicle systems. This is because these attacks are car specific. Therefore psychical access to a car should be obtained to estimate how the vehicles can be manipulated or deleted, increasing the opportunity an attacker would need to successfully execute an attack.

Attack Likelihood

The third step is the calculation of the attack likelihood, based upon the attack potential values, as explained in Table 5.7. Here it can be seen that the higher a high attack potential is, the lower the attack likelihood. This means that if the attack potential is high, for instance, 21 for the vulnerability of 'an unprivileged user is able to gain privileged access to vehicle systems' this means that due to the accumulation of the given attack potential values, the lower the attack likelihood will be. This is because of the higher attack potential, the more difficult it is to execute an attack, decreasing the likelihood of this attack, resulting in a lower number of the attack likelihood.

Table 5.5: Determining Likelihood of Attack

Accumulated value	**Description**	**Attack likelihood**
[0,2]	Basic	3
[3,6]	Enhanced basic	3
[7,14]	Moderate	2
[15,26]	High	1
> 26	Beyond high	1

Outcome of Risk Assessment

If we combine all of the above information and quantification of vulnerabilities, we come to a risk assessment as shown in Table 5.6. This table lists the attack potential (Appendix G), attack likelihood (Appendix F) and the corresponding categorisation of risks, all coupled to the relevant vulnerability.

The final number of the risk is calculated by multiplying the number mentioned in the likelihood column times the number mentioned in the impact column. In brackets, the risk itself is described according to the classification used by RACE, see Table 5.3. The risks are sorted from critical to minor. These risks in this order, along with the values, are directly used in Chapter 7 for the final framework.

Table 5.6: Attack Potential, Likelihood and Quantified Risk of V2I Projects

Vulnerability	Attack potential	Attack likelihood	Impact	Risk
Spoofing of messages or data received by the vehicle	11	2	3	6 (Critical)
Communication channels permit untrusted / unreliable messages to be accepted or are vulnerable to session hijacking / replay attacks / Messages received by the vehicle or transmitted within in, contain malicious content	11	2	3	6 (Critical)
Information can be readily disclosed (i.e. interception of information / eavesdropping)	2	3	2	6 (Critical)
Denial of service attacks via communication channels to disrupt vehicle functions	14	2	3	6 (Critical)
Data held on back-end servers being lost or compromised (data breach)	10	2	2	4 (Major)
Services from back-end server being disrupted, affecting the operation of a vehicle	11	2	2	4 (Major)
Communication channels used to conduct unauthorised manipulation, deletion or other amendements to vehicle held code/data	18	1	3	3 (Major)
An unprivileged user is able to gain privileged access to vehicle systems	21	1	3	3 (Major)
Back-end servers used as a means to attack a vehicle or extract data	15	1	2	2 (Minor)

The used categorisation for the risk as shown in Table 5.7 is used, ranging from minor risks to critical risks. The colours above represent every category: red is a critical risk, orange a major risk and green a minor risk.

Table 5.7: Classification of Risks using RACE

Risk value	Description
[1,2]	Minor risk: no primary need for countermeasures
[3,5]	Major risk: likely to occur but not fatal, countermeasures should be applied
> 6	Critical risk: should be minimised with highest priority

In our risk assessment, we encounter 4 critical risks, 4 major and 1 minor risk. The critical risks mean, once they are exploited, they should be minimised with the highest priority possible, if they are applicable to a V2I project.

6 MAPPING OF ATTACK METHODS TO SECURITY REQUIREMENTS VIA MEASURES

In this chapter RQ 5 'How can potential measures in V2I projects be mapped to specific security requirements?' is answered. This is being done by several steps.

First, we take each individual attack method, belonging to a vulnerability (see Tables 5.1 and 5.2). For each attack method, we map one or more relevant measures to prevent the attack methods from being exploited. After that, we map the identified security requirements to every individual attack method and combine all of these aspects in one table. These security requirements are needed to see which requirement is fulfilled by implementing certain measures.

As could be seen in Tables 6.1 and 6.2, we already mapped the vulnerabilities to security requirements. This chapter, however, goes more in depth of which security requirements belong to which attack method.

We did the mapping of the security requirements to the vulnerability / attack methods independent of each other, which means we did not look at the security requirements of the vulnerabilities before mapping them to the attack methods. This way we 1) double-check if the attack methods belong to the vulnerability via the security requirements and 2) could check whether the potential mitigation / measure belongs to the mapped attack method (and therefore vulnerability). This also means that every mentioned security requirements belonging to an attack method is a subset of the security requirements belonging to the vulnerability of the attack method.

After this process, only two security requirements in the 9 vulnerabilities were missing, namely:

- Vulnerability: communication of external infrastructure / vehicle permit untrusted or malicious messages to be accepted. Here, the missing security requirement was confidentiality. This was resolved by adding the measure 'digitally sign each message using a PKI-like system'
- Vulnerability: communication channels are used to conduct unauthorised manipulation, deletion or changes, to change the content of vehicle's messages. Here, the missing security requirement was also confidentiality and again resolved by adding the measure 'digitally sign each message using a PKI-like system'

The measures we describe are mainly derived from ETSI (TR, 2017). However, we did not put all measures into the table. For instance, measures like 'Implement ITS G5A as a CDMA/spread-spectrum system or base ITS on 3rd Generation mobile' or 'Implement frequency agility within the 5,9 GHz band.' These measures can be seen as standard bounded measures and are therefore beneficial for certain companies involved in this standard, while measures like 'Implement frequency agility within the 5,9 GHz band' or 'Plausibility checks on incoming messages' are too general compared to other measures mentioned in TR (2017). We, therefore, excluded these measures.

Furthermore, we complement the measures described by ETSI from documentation of both

UNECE and ITU. The mitigations are referred to as follows: if a [1] is behind a certain mitigation, it originates from ETSI 102 893, if a [2] is behind a mitigation, it originates from UNECE. If an attack is followed by [3], it originates from ITU (Lee, 2017).

Again, the tables are separated by the main two vulnerabilities: vulnerabilities regarding back-end servers and vulnerabilities to vehicles regarding their communication channels.

Note that no double attack methods are listed appearing at the same sub-level, i.e. abuse of privileges by staff and several examples of unauthorised access mentioned at 'back-end servers used as a means to attack a vehicle or extract data' are just mentioned once in Tables 6.1 and 6.2.

In both tables, the vulnerabilities as used in Chapter 5 are indicated with italic. The corresponding attack methods are listed below that, with potential mitigation(s) in the second column, followed by the specific security requirement.

6.1 Mapping of Measures from UNECE and ETSI to Security Requirements

Table 6.1: Attack Methods Mapped to Vulnerabilities Regarding Back-end Servers

Attack Method	Potential Mitigation	Requirement
Back-end servers used as a mean to attack a vehicle or extract data		
Abuse of privileges by staff (insider attack)	Security controls shall be applied to back-end systems to minimise the risk of insider attack [1]	Authorisation
Unauthorised internet access to the server	Security controls shall be applied to back-end systems to minimise unauthorised access [1]	Authorisation
Unauthorised physical access to the server	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data [1]	Authorisation
Attack on infrastructure: attack on infrastructure is attack when an attacker sends false malfunctions to innocent vehicles. This attack makes CA revoke permission for the innocent vehicle [3]	Digitally sign each message using a Kerberos/PKI-like token system [2]	Authentication, Integrity
Services from back-end server being disrupted, affecting the operation of a vehicle		
Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on.	Security controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage [1] / Reduce frequency of beaconing and other repeated messages [2]	Availability
Data held on back-end servers being lost or compromised		
Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	Security controls shall be applied to minimise risks associated with cloud computing [1]	Confidentiality
Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)	Security controls shall be applied to back-end systems to prevent data breaches [1]	Authorisation

Table 6.2: Attack Methods Mapped to Vulnerabilities to Vehicles regarding their Communication Channels

Attack method	Potential mitigation	Requirement
Spoofing of messages or data received by the vehicle		
Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	The vehicle shall verify the authenticity and integrity of messages it receives [1] / Limit message traffic to V2I/I2V and implement station registration [2] / Implement differential monitoring on the GNSS system to identify unusual changes in position [2]	Authentication, Integrity, Non-repudiation
Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road [3]	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules) [1], Include a non-cryptographic checksum of the message in each message sent [2]	Non-repudiation, Authentication, Integrity
Impersonation attack: Attacker can pretend to other entity by stealing other entity's ID information. Attacker can receive a message which is sent to another entity and attacker can send a message which is generated by a specific entity [3]	Limit message traffic to V2I/I2V and implement station registration [2], Digitally sign each message using a Kerberos/PKI-like token system [2]	Authentication, Integrity
Credential manipulation: Credential manipulation means modifying the vehicle's private key or ID. Attacker can use other vehicle's credential information without authorisation (ITU).	Digitally sign each message using a Kerberos/PKI-like token system [2]	Authentication, Non-repudiation
Communication channels accept untrusted/unreliable messages / Messages received / send are malicious		
Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. routing message manipulation attack: a malicious intermediate node modifies the message. Therefore vehicles can be received a forgery information [3] (see also spoofing of messages)	Digitally sign each message using a Kerberos/PKI-like token system [2], Include a non-cryptographic checksum of the message in each message sent [2]	Authentication, Integrity
Malicious diagnostic messages (i.e. of defect car creating false V2I message) via man in the middle attack/ session hijacking	The vehicle shall verify the authenticity and integrity of messages it receives [1] / Include an authoritative identity in each message and authenticate it [2], Digitally sign each message using a Kerberos/PKI-like token system [2] / Use broadcast time (Universal Coordinated Time - UTC - or GNSS) to timestamp all messages [2] / Implement differential monitoring on the system to identify unusual changes in position [2]	Authentication, Integrity
Replay attack, attacker can intercept V2V message nearby vehicles and V2I message of RSUs [3]	Use broadcast time (Universal Coordinated Time - UTC - or GNSS) to timestamp all messages [2] / Digitally sign each message using a Kerberos/PKI-like token system [2] / Include a sequence number in each new message [2]	Confidentiality, Authentication, Integrity
Communication channels execute unauthorised manipulation, deletion or other changes to vehicle held data		
Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	The vehicle shall verify the authenticity and integrity of messages it receives [1]	Integrity, Authentication
Communication channels permit manipulation / erasure / introduction of data/code of vehicle held data / code	Access control techniques and designs shall be applied to protect system data/code [1], Digitally sign each message using a Kerberos/PKI-like token system [2]	Integrity, Authentication

Attack method	Potential mitigation	Requirement
Information can be readily disclosed		
Interception of information / interfering radiations / monitoring communications	Confidential data transmitted to or from the vehicle shall be protected [1] / Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle [2]	Confidentiality
Gaining unauthorised access to files or data	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data [1]	Authorisation
Eavesdropping: Attacker can sniff V2V message nearby vehicles and V2I message of RSUs. Attacker can analyse traffic information by sniffing message [3]	Encrypt the transmission of personal and private data [2], use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle [2]	Confidentiality
Denial of service attacks via communication channels to disrupt vehicle functions		
Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner [3]	Measures to detect and recover from a denial of service attack shall be employed [1] / Add source identification (IP address equivalent) in V2V messages [2], maintain an audit log of the type and content of each message sent from and received by an ITS-S [2], include a source identity in each ITS message [2]	Availability
Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles	Measures to detect and recover from a denial of service attack shall be employed [1], limit message traffic to V2I/I2V and implement station registration [2] / digitally sign each message using a Kerberos/PKI-like token system [2] / Include a source identity in each ITS message [2]	Availability
An unprivileged user is able to gain privileged access to vehicle systems		
A unprivileged user is able to gain privileged access, for example root access [3]	Measures to prevent and detect unauthorised access shall be employed [1]	Authorisation

As was the case in Chapter 5, this mapping from attack methods to measures to requirements and visa versa is direct input for our final framework.

7 FRAMEWORK

In this chapter, we put all of the aspects we described and analysed so far together. The security requirements, vulnerabilities, measures and risk analysis all go into the framework, our final product of this thesis. In this chapter we therefore answer RQ 6: 'How can the identified security requirements, risks and measures contribute to a scalable and up-to-date guideline for V2I projects regarding security requirements?'

7.1 Goal of Framework

The goal of the framework is to help security companies, like Northwave and V2I projects with parties like Rijkswaterstaat or municipalities, check whether new / existing V2I projects of all kinds of functionalities are as secure as possible, for both automotive vehicles and external infrastructure.

The goal of the framework is that both companies working with the framework (i.e. a consulting security company) and corresponding parties of a V2I project (i.e. government, municipality, infrastructure administrators or other parties responsible for security) can work in an accessible and clear way in order to determine where the risks are. Also, they should be aware of how to tackle these risks in order to have a secure V2I system as possible, for both automotive vehicles and external infrastructure.

Furthermore, although the framework is aimed to managers concerning security, they should be able to appropriately delegate work to corresponding parties, along with being able to interpret the information about security and V2I projects and keep track of security within both current and future projects.

In order to do that, specific security requirements should be met. How these security requirements are fulfilled (i.e. authentication, access control, non-repudiation, confidentiality, integrity and availability) differs per relevant risk. Therefore our framework should describe in an orderly and conscious way which vulnerabilities and risks are applicable, attack methods and the corresponding security requirements and high-level descriptions of how to mitigate these risks along with a few examples to have a more practical perspective in this framework.

Stakeholders in this framework are security companies like Northwave and corresponding parties of a V2I project. Therefore it has to be made sure that the framework is for all stakeholders accessible and clear. We do this by analysing the interviews we had with 4 Northwave consultants.

It is important to note that this framework is a living document and due to changes in the future when new vulnerabilities are discovered and new functionalities of V2I projects are implemented in practice.

First, the results of the interviews held at Northwave B.V. are described. This is followed by the creation of the framework itself and the choices that were made, including the fulfilment of

specific measures.

7.2 Results of Interviews

In the following section, the main results of the four interviews will be elaborated upon and several examples will be given. Also, the main takeaways for the final framework of this thesis based on the results will be listed. The interview questions can be found in Appendix H.

In the interviews we omitted question five ('Do you combine existing frameworks in practice?'), since the goal of the question is too broad and the feedback of the answers could not be applied to the framework of this thesis (see Appendix I).

The four interviewed consultants all indicated they have working experience with standards / best practices methodologies / guidelines in their daily work. The most used standard is ISO 27001 regarding cybersecurity since this standard can be certified by a client. This certification process is a service Northwave offers. Other examples of standards being used by consultants in practice are the BIO (Baseline Informatiebeveiliging Overheid), which is an extension of the ISO standard for government organisations, ISO 27002 for the implementation of ISO 27001, COBIT (Control Objectives for Information and Related Technology), cloud control frameworks, best practice guidelines, along with standards / guidelines which are published from research organisations, e.g. NIST (National Institute of Standards and Technology) or SANS Institute which are more market-focused towards guidelines / best practices. In the two sections below the main results along with examples will be stated.

7.2.1 Knowledge of client

One of the main results of the interviews is that when a consultant assesses a specific document (being a guideline, methodology or framework) if this is suitable for usage in practice, the consultants focused on what he or she knows about a client. This general theme was mentioned 12 times in the interviews. Aspects which fall within this theme 'knowledge of a client' are, according to the interviews: 1) the requirements a client has when choosing certain documentation 2) maturity of the client 3) size of the client and 4) how to gather this knowledge, namely via a risk-based analysis. The coding of all these aspects can also be seen in Appendix J.

All consultants state they reason from a client first perspective in order to determine what standard / framework they pick, if relevant. If, for instance, an ISO certification is asked by the client, the corresponding ISO standard is of course used.

However, the goal of reasoning from a client first perspective is less important for this guideline, since the scope is relatively small and therefore focused on the same kind of V2I projects which are currently being trailed in practice and the future. Moreover, there are currently no other methodologies regarding security and specifically V2I. This means that the knowledge about a client from a consultant perspective when choosing a suitable framework regarding V2I and security is very limited: the framework fits or it does not, and other documentation is used. However, the maturity, size and corresponding risks of a client should still be taken into account in the feedback loop in order to see if the designed artefact fits with multiple kinds of organisations.

7.2.2 Framework should be descriptive, not prescriptive

The main outcome assessing if a framework is content-wise suitable for usage, is that a guideline / standard / template should be directive instead of prescriptive. All consultants agreed to this aspect. In total it was mentioned 7 times.

The descriptiveness is preferred by the consultants because every client is different. Detailed information is required from documentation / standards because the client wishes this. This aspect is being mentioned 3 times. This aspect also holds a close relationship with the documentation being directive and not prescriptive, since too much detail can lead to ending up having the danger you end up with something not fitting for the organisation' as consultant 3 mentions. Consultant 1 adds that she likes detail but 'every client is different, and the ISO 27002 (how to implement ISO 27001) does leave space for interpretation of every specific client, without being prescriptive.' Consultant 2 says situations are not always 0 or 1, or black or white, which makes the exact text of a standard or guideline less important. Again, knowledge of the client is important here.

Consultant 2 sees the aspect of giving examples / outlying situations as one of the most differentiation factors between standards / frameworks and guidelines / best practice guides: standards / frameworks are certain fixed frames within you can operate and how you fulfil this is up to the client, while guidelines / best practice guides outline a certain amount of steps which have to be followed in order to achieve something. For the final framework of this research examples of how some security requirements can be fulfilled will be, if applicable, included.

Consultant 3 also distinguishes between prescriptive and descriptive documentation: prescriptive is necessary when implementing a management system, while on an operational level (i.e. our framework) descriptive is preferred because prescribing all measures is too specific to apply for every client.

Lastly, the risks a client are exposed to is also 3 times mentioned to determine which framework is being picked in order to mitigate the risks. Consultant 1 mentions how risks can be used to determine where a client can improve on security and therefore what the focus areas of Northwave will be in order to mitigate these risks.

In summary, there are three main takeaways for the final framework as a result of the interviews. These are listed below:

1. Risk-based as a start of the framework, which also correlates with knowledge about an organisation and what to tackle first
2. Framework should be descriptive and not prescriptive, leaving some interpretation per client if possible
3. Framework with examples of how something can be implemented are being experienced as useful, in order to complement above takeaway

7.3 Creation of Framework

In beneath sections, the definitive framework will be presented. The mapping of all the parts of the framework is already done in previous chapters, leaving the framework mainly as a combination of all those aspects, with a few additions. For instance, we included where relevant a fulfilment per measure. Furthermore, we updated the description of the vulnerabilities to match this more closely with V2I projects.

First, as in line with the first takeaway from the interviews, we will take the vulnerabilities stated in section 5.2 as our starting point. The descriptions of these vulnerabilities have been made more clear compared to Chapter 5, by specifying it to V2I and giving examples where possible.

There are 9 vulnerabilities in total, of which we executed a risk analysis. The vulnerabilities are ranked from highest to lowest risk, along with the corresponding values.

Our framework consists of two tables. The first table outlines the vulnerabilities along with the risk assessment and requirements. In the second table, the mapping from security requirements to their mitigations is shown, along with examples of how these measures can be implemented.

In the first table, the first column consists of the vulnerability + corresponding attack methods, while in the 3 columns after that the values of the risk assessment are displayed, followed by the corresponding security requirements.

In the second column, the attack likelihood from Chapter 5 is shown, within brackets the value of the likelihood, extracted from the RACE framework. The higher the value of the likelihood, the higher a theoretical chance of a potential attack of a threat. 3 means a basic attack and therefore higher chance of being executed, 2 moderate and 1 a highly advanced attack, and therefore less likely to be executed.

In the third column, the highest number of the attack impact is shown, within brackets the category this highest value appears in. These values can be found in Appendix G, along with the category of where the impact of the vulnerability is the highest. The explanation for the impact of the attack is extracted from the RACE framework.

In the fourth column, the value of the risk can be found, which is the outcome of the attack likelihood multiplied by the attack impact. With this number, the order of the vulnerabilities is displayed.

Table 7.1: Vulnerabilities, Attack Methods, Values of Risks and Security Requirements

Vulnerability + Attack Methods	Attack Likelihood	Attack Impact	Value	Security Requirements
Spoofing of send messages or data received by the vehicle *Attack methods:* • Impersonation: attacker can receive a message which is sent to another entity and attacker can send a message which is generated by a specific entity. For example, an attacker can pretend to be an emergency vehicle, by sending a spoofed message pretending to be such vehicle in order to claim right of way to other vehicles • Sybil attack: in order to spoof other vehicles as if there are many vehicles on the road • Credential manipulation: modifying the vehicle's private key or ID. Attacker can use other vehicle's credential information without authorisation	2 (Moderate)	3 (Operational: significant impact on performance)	6 (Critical)	• Non-repudiation • Authentication • Authorisation • Integrity
Communication of external infrastructure / vehicle permit untrusted or malicious messages to be accepted *Attack methods*: • Routing message manipulation attack: a malicious intermediate node modifies the message. Therefore vehicles can receive forgery information • Malicious diagnostic messages: i.e. creating false V2I of defect car via man in the middle attack / session hijacking • Replay attack: attacker can intercept V2V message nearby vehicles and V2I message of RSUs. Later, attacker can replay those messages	2 (Moderate)	3 (Operational: significant impact on performance)	6 (Critical)	• Confidentiality • Non-repudiation • Authentication

Vulnerability + Attack Methods	Attack Likelihood	Attack Impact	Value	Security Requirements
Send / received messages can be disclosed by eavesdropping *Attack methods:* • Interception of information / monitoring communications: attacker can sniff V2I message and analyse traffic information by eave dropping / sniffing messages. Example: tracking of specific (emergency) vehicles • Gaining unauthorised access to files or data	3 (Basic)	2 (Privacy: identification of car or driver)	6 (Critical)	• Confidentiality • Authorisation
Denial of service attacks via communication channels disrupts ability of vehicle and infrastructure to send or receive messages *Attack methods:* • Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner • Black hole attack: in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles	2 (Moderate)	3 (Operational: significant impact on performance)	6 (Critical)	• Availability
Services from back-end server of infrastructure being disrupted *Attack method*: • Attack on back-end server stops it from functioning. Example: vehicle cannot receive messages anymore or infrastructure cannot send messages to vehicle	2 (Moderate)	2 (Operational: driver aware of performance degradation)	4 (Major)	• Availability

Vulnerability + Attack Methods	Attack Likelihood	Attack Impact	Value	Security Requirements
Data held on back-end servers being lost or compromised *Attack methods:* • Insider attack: abuse of privileges by staff • Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers • Unauthorised internet access to the server. Example: backdoors or unpatched system software vulnerabilities • Unauthorised physical access to the server. Example: by USB sticks or other media connecting to the server • Information breach by unintended sharing of data. Example: admin errors	2 (Moderate)	2 (Privacy: identification of car or driver)	4 (Major)	• Authorisation • Confidentiality
Communication channels are used to conduct unauthorised manipulation, deletion or changes to change content of vehicle's messages *Attack methods:* • Communication channels permit code injection. Example: tampered software binary might be injected into the communication stream • Communication channels permit manipulation of vehicle held data/code, i.e. sensor information manipulation. Example: attacker modifies a physical address of the communication module or manipulates ECU sensor information such as a speed sensor	1 (High)	3 (Operational: significant impact on performance)	3 (Major)	• Authorisation • Integrity • Confidentiality

Vulnerability + Attack Methods	Attack Likelihood	Attack Impact	Value	Security Requirements
An unprivileged user is able to gain privileged access to vehicle systems *Attack methods:* • An unprivileged user is able to gain privileged access, for example root access, through unauthorised access to credentials like private keys or certifications. This could lead to e.g. reading the content of send messages or change the interpretation of received messages in built in vehicle systems	1 (High)	3 (Privacy: driver or car tracking / Operational: significant impact on performance)	3 (Major)	• Authorisation
Back-end servers of infrastructure used to attack a vehicle *Attack methods:* • Insider attack: abuse of privileges by staff • Unauthorised internet access to the server. Example: backdoors or unpatched system software vulnerabilities • Unauthorised physical access to the server. Example: by USB sticks or other media connecting to the server • When an attacker sends false malfunctions to innocent vehicles. This attack could make certification authority revoke permission for the innocent vehicle	1 (High)	2 (Privacy: identification of car or driver)	2 (Minor)	• Authorisation • Authentication • Integrity

7.3.1 Vulnerabilities and Corresponding Measures

In the second table of the framework, the vulnerabilities are once again outlined and examples of mitigations are given, where applicable with examples. These examples are also extracted from Chapter 4 where specific fulfilments per kind of V2I message are outlined.

Once again, the security requirements are included in order to have the base of this framework present. The requirements are, however, more specific and are a subset of the vulnerabilities. In bold, the corresponding vulnerability is stated to make clear about which specific vulnerability the attack / measures belong to.

We also add more detail to some mitigations. When a potential mitigation only describes what should be done, e.g. 'security controls should be applied...' or 'access control should be used...', how this mitigation can be implemented is not clear. Therefore, where relevant, we extracted the implementation from Chapter 4 or from the ISO 27002 standard. This is because this standard, as identified in the interviews with Northwave (see Appendix I) and mentioned in Beckers et al. (2016), is used to describe measures in information security, including connected cars. When a measure is described from a European standard how to implement a mitigation, this is indicated with a [1]. If not, [2] indicates the control of ISO 27002 which is selected.

Table 7.2: Mitigations per Attack Methods, including Fulfilment and Corresponding Security Requirements

Attack Method	**Potential Mitigation + Fulfilment**	**Security Requirements**
Spoofing of send messages or data received by the vehicle		
• Impersonation	• The vehicle shall verify the authenticity and integrity of messages it receives • Limit message traffic to V2I/I2V and implement station registration • Implement differential monitoring on the positioning system to identify unusual changes in position	• Authentication • Integrity • Non-repudiation
• Sybil attack	Security controls shall be implemented for storing cryptographic keys *Fulfilment:* • Use of hardware security modules • Include a non-cryptographic checksum of the message in each message sent	• Non-repudiation • Authentication • Integrity
• Credential manipulation	Digitally sign each message using a PKI-like token system *Fulfilment:* • By using different authorities belonging to cryptographic algorithms (i.e. enrolment authorities, authorisation authorities and certification authorities) a process can be created in order to make a secure PKI token system. For more detailed information see attachment PKI	• Authentication • Non-repudiation

Attack Method	Potential Mitigation + Fulfilment	Security Requirements
Communication of external infrastructure / vehicle permit untrusted or malicious messages to be accepted		
• Routing message manipulation attack	• Digitally sign each message using a Kerberos/PKI-like token system (see attachment) • Include a non-cryptographic checksum of the message in each message sent	• Authentication • Integrity • Confidentiality
• Malicious diagnostic messages	• The vehicle shall verify the authenticity and integrity of messages it receives • Include an authoritative identity in each message and authenticate it • Digitally sign each message using a Kerberos/PKI-like token system (see attachment) • Use broadcast time (Universal Coordinated Time - UTC) to timestamp all messages • Implement differential monitoring on the system to identify unusual changes in position	• Authentication • Integrity • Confidentiality
• Replay attack	• Use broadcast time (Universal Coordinated Time - UTC) to timestamp all messages • Digitally sign each message using a Kerberos/PKI-like token system • Include a sequence number in each new message	• Authentication • Integrity • Confidentiality

Attack Method	Potential Mitigation + Fulfilment	Security Requirements
Send / received messages can be disclosed by eavesdropping		
• Interception of information / monitoring communications	• Confidential data transmitted to or from the vehicle shall be protected *Fulfilment:* – Usage of cryptographic algorithm, see attachment • Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle	• Confidentiality
• Gaining unauthorised access to files or data	Through system design and access control, it should not be possible for unauthorised personnel to access personal- or system critical data *Fulfilment:* • Formal user registration and de-registration process should be implemented to enable assignment of access rights [2]	• Authorisation
Denial of service attacks via communication channels disrupts ability of vehicle and infrastructure to send or receive messages		
• Sending a large number of garbage data to vehicle information system	• Measures to detect and recover from a denial of service attack shall be employed • Add source identification (IP address equivalent) in V2I messages • Maintain an audit log of the type and content of each message sent from and received by an ITS-S • Include a source identity in each ITS message	• Availability

Attack Method	Potential Mitigation + Fulfilment	Security Requirements
• Black hole attack	• Measures to detect and recover from a denial of service attack shall be employed • Limit message traffic to V2I/I2V and implement station registration • Digitally sign each message using a PKI-like token system (see attachment) • Include a source identity in each ITS message	• Availability
Services from back-end server of infrastructure being disrupted		
• Attack on back-end server stops it from functioning	Security controls shall be applied to back-end systems *Fulfilment:* • Where backend servers are critical to the provision of services, there are recovery measures in case of system outage • Reduce frequency of beaconing and other repeated messages	• Availability
Data held on back-end servers being lost or compromised + Back-end servers of infrastructure used to attack a vehicle		
• Insider attack • Unauthorised internet access to the server	Security controls shall be applied to back-end systems to minimise the risk of insider attacks / unauthorised access, respectively *Fulfilment:* • Formal user registration and de-registration process should be implemented to enable assignment of access rights [2]	• Authorisation

Attack Method	Potential Mitigation + Fulfilment	Security Requirements
• Loss of information in the cloud	Security controls shall be applied to minimise risks associated with cloud computing *Fulfilment:* • Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets should be agreed with the supplier and documented [2]	• Confidentiality
• Information breach by unintended sharing of data	Security controls shall be applied to back-end systems to prevent data breaches *Fulfilment:* • Groups of information services, users and information systems should be segregated on networks [2]	• Authorisation
Communication channels are used to conduct unauthorised manipulation, deletion or changes to change content of vehicle's messages		
• Communications channels permit code injection	The vehicle shall verify the authenticity and integrity of messages it receives • Digitally sign each message using a PKI-like token system	• Integrity • Authentication
• Communications channels permit manipulation of vehicle held data/code	Access control techniques and designs shall be applied to protect system data/code *Fulfilment:* • A formal user registration and de-registration process should be implemented to enable assignment of access rights [2]	• Integrity • Authentication

Attack Method	Potential Mitigation + Fulfilment	Security Requirements
An unprivileged user is able to gain privileged access to vehicle systems		
• An unprivileged user is able to gain privileged access	Measures to prevent and detect unauthorised access shall be employed *Fulfilment:* • A formal user registration and de-registration process should be implemented to enable assignment of access rights	• Authorisation
Back-end servers used as a mean to attack a vehicle or extract data		
• Unauthorised physical access to the server	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data *Fulfilment:* • Formal user registration and de-registration process should be implemented to enable assignment of access rights [2]	• Authorisation
• When an attacker sends false malfunctions to innocent vehicles	Digitally sign each message using a PKI-like token system, focusing on the enrolment and authority parts in order to make sure no unauthorised parties can send false malfunctions to vehicles (see attachment)	• Authentication • Integrity

8 VALIDATION OF FRAMEWORK

In this chapter, the obtained results of the validation of the framework via the expert opinion validation method will be presented. We will, therefore, answer RQ 7: 'How can the proposed framework be applied and evaluated for the Dutch market?' As explained in section 2.3, a survey was spread to several employees in the Concorda project. The survey as a whole can be seen in Appendix K, while the methodology of it can be read in section 2.3.2.

In the sections below, we will first present the participants of the validation, accompanied by the case description. After that, we present the results of the survey for every section of the framework, followed by recommendations for future improvements of the framework based on the input of the experts. Lastly, we describe the limitations of the validation process of the proposed framework.

8.1 Case Study Participants

As mentioned in section 2.3, Concorda exists of multiple parties working together in order to set up and test trial environments regarding V2X communication. For this case study, we surveyed several security experts involved in Concorda. We also state the vendor they belong from. Rijkswaterstaat is seen here as the managing party, while a vendor can be e.g. Qualcomm, V-Tron, Swarco or any other vendor working together with Rijkswaterstaat at Concorda. In order to obtain anonymity, we do not mention the specific vendor a respondent is involved with.

Table 8.1: Participants of Survey

Participant No.	Function	Role in Project	Experience with Security	Experience with V2I
Participant 1	Developer of Road-Side Unit (RSU)	Vendor	20 years	4 years
Participant 2	In-car service provider	Rijkswaterstaat	18 years	10 years
Participant 3	Security architect	Vendor	3 years	1 year

Participant 1 is involved in the implementation of ETSI TS 103 097 about security of Intelligent Transport Systems (ITS), specifically security header and certificate formats, a relatively technical standard with several security profiles per type of message. The second participant is involved in Praktijkproef Amsterdam. The third and last participant is involved in the development of secure V2I and V2V communication.

8.2 Case Description

Concorda is a temporary project in which multiple trials regarding V2X and V2I are run in the Netherlands, Belgium, Germany, France and Spain. The project in the Netherlands is run by the Rijkswaterstaat, the maintainer of the roads in the Netherlands. Rijkswaterstaat works together

with third parties in order to develop solutions in order to make traffic as efficient and safe as possible. Concorda is part of this goal, by targeting autonomous cars and their communication with external infrastructure as well. Concorda is developed in order to know what an autonomous car should do when a certain situation on the road occurs (PraktijkproefAmsterdam, 2020).

The technical manager of an ITS Corridor as part of Concorda elaborates on the relationship between Rijkswaterstaat and vendors. He states that vendors work for Rijkswaterstaat: Rijkswaterstaat instructs the vendors to create certain functionality, both in-car systems as well as road-side units. In this process, Rijkswaterstaat leaves the technical specification of the prescribed functionalities to the vendors, they are free to choose their implementation and way of development.

There are different working parties which work in different kind of projects in different areas. Areas where trails are run in the Netherlands are Brabant, the region Rotterdam - The Hague and the region of Amsterdam. The best-known example of a project is that of Praktijkproef Amsterdam, where a connected car is notified when for instance:

- A car is stationary in the same lane your car is travelling and how this car should react to that
- A car is nearing a closed lane
- A car is nearing a connected traffic light to determine which speed should be maintained in order to get as efficient as possible through the traffic light
- What a connected car should do when a temporary speed limit is set due to e.g. road works

An example of a test setup, where the connected car receives a notification of a closed lane due to a stationary car via a smartphone, can be seen in Figure 8.1. Praktijkproef Amsterdam runs it trails on the A5 and A9, along with the regional roads N205 and N201 nearby Schiphol. On these places the necessary communication hardware is already in place, for example on the N205 six intersections are fitted with connected traffic lights (PraktijkproefAmsterdam, 2020). On the Dutch roads, Concorda started its first trails in February 2019 and it is planned to execute the last test in 2020 (PraktijkproefAmsterdam, 2020).

8.2.1 Security in Concorda

There is little public documentation on how security is managed within Concorda. The technical manager of Concorda gives us a bit more information. He states that normally Rijkswaterstaat asks an independent department called CVI (Centrale informatievoorziening, i.e. central information supply) to create a plan for the architecture of the project. In this architecture there should also be attention to security. However, the manager indicates that CVI is not always able to supply the necessary knowledge regarding security. Furthermore, since Concorda is in a concept-phase, the involvement from CVI is currently limited. Individual projects are, however, free to implement security if they want to, e.g. a PKI structure, according to the manager.

In addition, in our survey, some participants gave information on this matter. For instance, participant 2 mentions how security at Concorda is always implemented in the end, while it would be better to start with security by design. Participant 2 also adds security can be a killer for enabling functions. These functions combined with security are not working either not properly or not at all, which makes security sometimes difficult to implement. Lastly, participant 3 mentions how European cooperation is the bigger challenge regarding security because different interests of different parties play a part in developing V2I projects. What this means for Concorda in the Netherlands specifically remained, unfortunately, unclear.

Figure 8.1: Example of Praktijkproef Amsterdam Test Setup

8.3 Results of Survey

In this section, we will describe the results of the filled-in surveys. The methodology of the survey can be found in section 2.3.2, while the whole survey can be seen at Appendix K.

We questioned the main aspects of the framework from different perspectives, as explained in section 2.3.2. In summary, the main 6 aspects of the survey are: the overview of vulnerabilities and risks, measures, security requirements, attack methods, the mapping between all these parts and the overall usefulness of the framework. Of these 6 aspects, we asked different perspectives to be judged, e.g. the mapping between different aspects or the inclusion of certain aspects.

In the section below we will present and discuss the results of every main aspect of the framework. The results are presented in the order of the survey, which means first we explain whether the questioned aspect is used / documented in Concorda and if so how, followed by the results of the multiple-choice with the 5 options (from strongly disagree to strongly agree) where we ask the participants to judge the aspect on perspectives like relevance or clarity. The results of all the participant of the multiple-choice questions of all the main aspects of the framework can be seen in Appendix L. After that, we present the results of the open questions where we ask the participants if they agree with the presented content of the relevant aspect of the framework. Furthermore, we give recommendations on future improvements regarding this framework. Lastly, we state the limitations of the validation.

8.3.1 Vulnerabilities and Risks

When asked about the general current processes regarding security in projects of Concorda, all participants indicated that security risks have not been documented when designing / implementing current projects within Concorda.

Furthermore, participant 1 explains that the current security implementation of Concorda project is based on the ETSI 103 097 standard. This standard does prescribe the design regarding the security implantation. Furthermore, participant 1 indicates there are 'two important European Commission policy documents giving a clear description of the dos and dont's regarding security implementation.' However, as far as we are aware, these documents do not provide an overview of security risks regarding V2I, which our framework does.

Participant 2 states he was not involved in the project startup phase. However, once he joined the Praktijkproef Amsterdam, security was mentioned as a project goal. This goal was followed and implemented by working out the created impact analyses for the transition between PKI-structures, according to participant 2. Participant 3 adds that a new risk / threat assessment always has value, even if other documentation is used for that goal.

Table 8.2: Valuation of Vulnerabilities and Risks

Aspect of Vulnerabilities / Risks	**Strongly disagree**	**Disagree**	**Do not disagree, but also not agree**	**Agree**	**Strongly Agree**
Vulnerabilities relevance			[1]	[2] [3]	
Attack levels relevance			[1]	[2] [3]	
Impact level relevance			[1] [2]	[3]	
Priority of risks relevance			[1] [2]	[3]	

2 of the 3 participants agree that the presented vulnerabilities and attack levels are relevant for current and future projects within Concorda, while the other participant answered 'do not disagree, but also not agree.' Regarding the impact levels and shown priority of the risks, 2 participants do not disagree but also not agree whether these aspects are relevant for current and future projects within Concorda, while 1 participant agrees to the relevance. The results can also be seen in Table 8.2.

Regarding the presented 9 vulnerabilities of V2I, the participants state how they agree with them, while participant 2 adds the vulnerability of 'power failures' which could give false data by default. Participant 3 also adds some specific attack methods and measures, which we put into the corresponding sections below.

Lastly, using the vulnerabilities as a starting point - determined by the interviews with the consultants of Northwave (section 7.2) - is agreed upon by all three respondents, without any addition.

8.3.2 Attack Methods

All participants state that, like security risks in the above section, have not been documented specifically for Concorda projects. Participant 3 adds that the overview of attack methods would add value to project in Concorda.

2 of the 3 participants indicate that they agree with the clarity of the description of the attack methods. The result can also be seen in Table 8.3.

Table 8.3: Valuation of Attack Methods

Aspect of attack method	**Strongly disagree**	**Disagree**	**Do not disagree, but also not agree**	**Agree**	**Strongly Agree**
Attack method clear			[1]	[2] [3]	

Participant 1 says that the attack methods mentioned in the framework are 'already in ETSI documents', while participant 2 adds that the possibility of radio communication frequency jamming is a missing attack method. Participant 3 states that the black hole attack description is not fitting since 'it doesn't block messages.'

8.3.3 Measures

2 of the 3 participants answer that security measures have been documented for projects within Concorda. Participant 1 says this is being done with ETSI and European Commission documentation, while participant 2 says that measures have been documented as an impact analysis for the PKI structure. Also, functionalities of other working parties of other projects have been reused who had a dedicated job documenting measures. Participant 3 mentions that the overview of measures presented in the framework does add value.

Table 8.4: Valuation of Measures

Aspect of Measures	**Strongly disagree**	**Disagree**	**Do not disagree, but also not agree**	**Agree**	**Strongly Agree**
Security measures relevance			[1]	[2]	[3]
Security measure clear			[1]	[2] [3]	

1 participant strongly agrees with the presented security measures and its relevance to current and future projects within Concorda, 1 agrees and 1 does not disagree, but also not agree. 2 of the 3 participants agree with the statement that each security measure is clearly described, while one does not disagree, but also not agree. The results can also be seen in Table 8.4.

Participant 3 mentions how data validation can be implemented by combining several sources. 'It is no longer possible to trust only one data source.' The combining of multiple data sources could also act like a fall-back, as well as data validation. Participant 3 adds that this type of security is not issued at this moment. Participant 2 gives a tip to work with an identifier per vulnerability and attack methods to improve readability of the framework.

8.3.4 Security Requirements

Of the 3 respondents, 2 say that security requirements have been documented in Concorda, while one states they are not. Collaborating on that, participant 1 says that in the ETSI 103 097 there is a 'detailed design description' of how to securely implement messages. Participant 2 adds that for specific projects this is easier to answer, but for Concorda as a whole, not. Furthermore, participant 2 says that in his / her project it was only being told that PKI had to be used without a reason why.

Table 8.5: Valuation of Security Requirements

Aspect of Security Requirements	**Strongly disagree**	**Disagree**	**Do not disagree, but also not agree**	**Agree**	**Strongly Agree**
Security Requirements relevance Table 1			[1]	[2] [3]	
Security Requirements relevance Table 2			[1]	[2] [3]	

2 of the 3 respondents indicate that they agree with the relevance of the security requirements presented in Table 1 and Table 2 of the framework, while 1 respondent does not disagree, but also not agrees. The results can also be seen in Table 8.5.

When asked about the inclusion of the security requirements in the framework in general, participant 1 says this is already done in the ETSI framework, participant 2 agrees, while participant 3 say that they are on a high level and are not 'really requirements' because they do not state how these requirements can be complied upon.

8.3.5 Mapping between all the Parts

Table 8.6: Mapping of Aspects of Framework

Mapped aspects	**Strongly disagree**	**Disagree**	**Do not disagree, but also not agree**	**Agree**	**Strongly Agree**
Relevance of mapping between vulnerabilities and attack methods			[1]	[2] [3]	
Mapping between vulnerabilities, attack methods and measures is clear			[1] [2]	[3]	
Mapping between vulnerabilities and requirements in Table 1 is clear			[1] [2]	[3]	
Mapping between vulnerabilities and requirements in Table 2 is clear			[1] [2]	[3]	

The results of the mapping between vulnerabilities and attack methods regarding current and future projects within Concorda show us that 2 participants agree with this mapping, while one does not disagrees, but also not agrees.

Regarding the clarity of the mapping between vulnerabilities, attack methods (both Table 1 of the framework) and the corresponding security measures (Table 2 of the framework), 2 of the 3 participants say that they do not disagree, but also not agree, while 1 participant agrees.

When the participants were asked about the mapping of vulnerabilities to security measures, and between the mapping of attack methods and security measures, participant 1 says this work has already been done by ETSI, while the other two participants say that they indeed agree with the mappings.

The clarity of the mapping between vulnerabilities and security requirements in Table 1 and Table 2 shows different results: here two participants state they do not disagree, but also not

agree while only one participant agrees with the clarity of the mapping.

All of the above results can be seen in Table 8.6.

8.3.6 Usefulness of the Framework

The final aspect of the framework we questioned the participants is the usefulness. This aspect consisted of a few multiple-choice questions and one open question. These results are presented in the section below.

At the first question, about the usefulness of a comprehensive overview regarding cybersecurity when working with current and future projects in Concorda, participant 1 says that this is already available at the ETSI framework, participant 2 says it would be but at the current state, Concorda is not a complete project with day-to-day project management. This makes the usage of such an overview less necessary. Participant 3 answers that a comprehensive overview would help in managing a project more adequately.

At the second question about a potential positive impact of the proposed framework on current or future projects within Concorda, participant 1 says again this is irrelevant, participant 2 says it would have a positive impact on both current and future projects while participant 3 differs and states this only holds true at future projects.

The final multiple-choice question about the usefulness of the framework, is if the participant would consider incorporating a security framework similar as proposed in this research in projects of Concorda. Participant 1 again states this question is irrelevant due to the presence of the ETSI 103 097 document, participant 2 he / she would only do this at future projects, while participant 3 has the same opinion.

The last question of the survey is how relevant the proposed framework as a whole is, regarding security in V2I projects. Participant 1 says that the ETSI frameworks are leading regarding V2I projects. Participant 2 says that he / she thinks it can help to start different security processes but a complete risk assessment needs to be done prior. Participant 3 says in Concorda projects security needs to be understood better, instead of consultants who only create fear and misunderstanding. Security is not an issue, according to participant 3, if a framework is used from the beginning and with a clear function in mind.

8.4 Future Improvements of Framework

In this research, we will not process the feedback of the participants into an improved version of the framework. Instead, we will describe the points participants indicated could be improved, so this can be taken into account for further research.

First, it is important to emphasise the iterative process the development of such a framework should go through. Functionalities of V2I projects will differ a few years from now on, which could lead to new vulnerabilities. The framework is by no means an exhaustive list of vulnerabilities, attack methods, measures and security requirements. A periodic check in order to update the framework where necessary according to the latest developments is therefore advised.

Looking at the specific content of the current version of the framework, participants indicated that the attack method 'frequency jamming' was missing. This attack method could be added to the vulnerability 'Denial of service attacks via communication channels disrupts ability of vehicle and infrastructure to send or receive messages.'

Lastly, a participant stated how a fixed pointer via a unique identifier per vulnerability or attack method would improve the readability of the framework. This would also improve the clarity

of the mapping from requirements to measures and vulnerabilities since via the identifier the requirement can be traced to a specific measure, which in turn can be mapped to the corresponding measure.

8.5 Discussion

In this section, we will discuss the above results of the validation of the framework. First, we point out some general remarks about the validation, before moving to specific results and comments the participants have made.

First, we notice that participant 1 does not belong to the proposed target group of the people, i.e. managers of security. Instead, participant 1 is a developer. This means participant 1 primarily focuses on what he or she can actually apply, while this framework mainly is meant to constitute to decisions about security being made without being bothered how this can be achieved. Participant 1 therefore oftentimes mentions how in ETSI 103 097 all the information the framework is already there, neglecting the combination of vulnerabilities, measures, attack methods and requirements from multiple sources.

An explanation for these answers could be the fact that participant 1 is convinced that many aspects of my framework can already be found in the ETSI 103 097 standard. For instance, regarding the inclusion of the vulnerabilities itself, participant 1 states that vulnerabilities are 'okay', but that these are 'already in the ETSI 103 097' when they are, at least not explicitly, mentioned. This theme comes back when answering the question about starting with vulnerabilities in the framework when participant 1 says 'this work has been done already.' This sentiment could be strengthened by the fact that participant 1, assessing his / her role in Concorda, is the only developer and the framework is not meant to be relevant for developers itself but rather targeted for managing security.

Also, participant 1 only filled in the middle option 'do not disagree but also not agree' if asked about any of the main aspects of the framework. This does not indicate a proper insight into the framework as we already discussed in section 9.3, where we identify the limitations of the framework which can also be seen without the corresponding background information.

Since participant 1 is not part of our targeted audience, the negative results are less important than the other 2 participants who are more aware of the target of the proposed audience of the framework. Participant number 2 does show some deviation of his / her answers. For instance, while the option 'agree' is most often used, when something was not clear - the mapping between requirements and measures - the respondent lowered the level to 'do not disagree, but also not agree.' This was also the case for participant number 3.

Zooming in on specific answers of participant 2 and 3, we observe generally positive sentiment towards the main aspects of the framework. The most positive feedback was obtained at the presented security measures, where we obtain the only 'strongly agree' from participant number 3. This is followed by the vulnerabilities, attack levels of the risks and the security requirements with all obtaining a result of 2 participants agreeing of the degree of relevance for Concorda and one does not agree, but also not disagree.

However, the most critical feedback of the open questions was regarding the (high level) security requirements. Participant 3 states they are not 'really requirements' because they do not state how these requirements can be complied upon. This implies that the participant sees the requirements as not properly connected to corresponding measures and vulnerabilities. This should be therefore improved in a future version of the artefact. Also, the mapping between security requirements and vulnerabilities is not made explicit in the framework.

We expected the participants to question the choices being made. However, this was not the fully the case, as two participants state they do not disagree, but also not agree with the statement that the mapping between vulnerabilities (Table 1) / measures (Table 2) and security requirements is clear.

The results of the security requirements also show us that security requirements can be useful to the participants. Participant 2 says that in his / her project it was only being told that PKI had to be used without a reason why. Determining security requirements and linking that to the vulnerabilities beforehand, would help speed up this process of prioritising resources in a V2I project before determining how to fulfil the requirements.

Compared to the other multiple-choice question about the mapping between aspects, we do notice a slight decline in positive feedback since on average two respondents do not disagree, but also not agree with the clarity of the mapping of the aspects. The only exception is the mapping between vulnerabilities and attack methods, which received two agreements regarding the clarity of the mapping. These results are to be expected: the vulnerabilities and attack methods are put into the same box, which makes the direct relationship between vulnerabilities and attack methods the clearest. Meanwhile, the other aspects of the framework do not possess this direct relationship since they are not put into the same box or - in the case of the mapping between vulnerabilities and corresponding security measures - even the same table of the framework.

Regarding the usefulness of the framework, we notice how 2 of the 3 participants agree with the statement that a framework similar to in this research would help future projects in Concorda. This is because the framework is made to manage security, something which is not done daily in current Concorda projects. For instance, a participant of the case study mentions how Concorda is not a complete project with day-to-day project management, which makes the usage of such an overview as the framework is currently less necessary. This is inevitable considering the current state and limited availability of V2I in practice (see also section 9.3).

Lastly, we observe a difference in answers of what main aspects of our framework have already been documented within Concorda and which are not. For instance, 2 of the 3 participants indicate that measures within projects have been documented and one denies this. This could be because of the different projects the participants where involved in and different working procedures. The same holds true regarding the overview of security requirements in the framework.

8.6 Limitations

Naturally, the above-described validation process has some limitations. In this section, we describe the limitations and how this could potentially influence the results of the validation process. The limitations mainly stem from the fact that V2I has not been deployed on mass as of yet, making it impossible to find a mature environment to validate the framework in.

The first limitation is that V2I as a whole is not mature enough to be analysed in an environment where all aspects like functionality and security are deployed. The participants consequently had to imagine the framework being deployed in a fully operational environment which can cause some bias. This especially holds true regarding the questions about future projects in Concorda, since one the goals of the framework is to be up-to-date and scalable to both current and future projects, where currently we cannot predict the future regarding V2I, functionalities and security.

An expert in the field of security in V2I mentions how Concorda does not have a permanent operational environment to which the developed framework can be verified. Furthermore, Concorda's goal is not to develop towards mass deployment. Concorda is a temporary environment where different parties, i.e. vendors and Rijkswaterstaat, test different V2X and V2I configura-

tions to be primarily compared on performance. Security is not neglected in this regard since to be able to adequately judge the performance of V2I projects, security needs to be implemented as well. In practice, according to the expert, this means setting up security only on a communication level (sending and receiving messages) and not on an organisation level. This means certain measures we mention in our framework, like access control via formal user registration and de-registration to enable assignment of access rights to prevent insider attacks or abuse of privileges, will by definition not be applicable to Concorda.

The second limitation is an elaboration of the first: since security is not a primary focus in Concorda, there were no security experts in a managing role found to fill in the survey. The respondents of the survey were primarily security experts and not in charge of managing security as a whole. This is also because Rijkswaterstaat can ask an independent department of their organisation to set up an architecture for a project in which security is also taken into account. However, since this department is not always involved in Concorda due to its infancy, this was not always the case which makes security, in general, more an afterthought in Concorda, something a participant of the case study also indicated.

The third limitation lies in the choice of creating and sending a survey to the experts. Therefore we could not ask for feedback or clarification of answers since the survey is anonymous. For instance, participant 3 only mentions how security is a bigger challenge on the level of European cooperation because different interest play a role here. What this means for Concorda specifically remained unclear.

Also, according to participant 2, a black hole attack does not block messages. However, a black hole attack by definition is denial of service attack because one of the sending nodes is being skipped, causing it to drop messages instead of sending them. Therefore we mapped this kind of attack to the category of 'Denial of service attacks via communication channels disrupts the ability of vehicle and infrastructure to send or receive messages.'

Another limitation originates from the second limitation: since security is not a primary focus of Concorda, we could only obtain three people at least involved in some role with security in Concorda. Three people are too few to draw certain conclusions regarding the validation of our framework, it is only indicative. More people involved in security should be obtained to give the framework a thorough validation.

The last limitation lies within the fact that we chose deliberately not to explain the framework to the experts before filling in the survey since the framework was aimed to be self-explanatory. However, since the experts were briefed via a third party, we cannot be sure which information about the goal and creation of the framework was given to the participants.

9 CONCLUSION AND DISCUSSION

Every research question answered in this research has resulted in several outcomes. In this chapter, the answers to all the research questions are therefore presented and discussed. After that, the limitations of this research are described, followed by potential further research. We also give recommendations to other researchers in this area, closed by our contribution to theory and practice.

9.1 Conclusions

The primary goal of this research was to answer the following main research question:

> **How can current and future V2I projects deal with security requirements regarding communication with connected cars?**

To answer this question, several sub-questions have been formulated. In the section below, the outcomes of all of the seven sub-questions are shown, starting with RQ 1.

9.1.1 RQ 1: Functions, Security and Privacy Requirements of Connected Cars

In this RQ we discuss both functions of connected cars and more importantly, the security and privacy requirements of connected cars.

RQ 1.1: Functions of Connected Cars

We first conclude from the mapping of functions of connected cars that there are two categories: telematics and V2C communication. In our research, we focused on V2X communication, specifically V2I.

V2X is dependent on external communication and infrastructure and therefore more difficult to implement due to the variety of stakeholders. V2X consists of four general categories: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Home (V2H) and Vehicle to Environment (V2E) communication. Features focus on three categories: traffic safety, traffic efficiency, and convenience and interaction.

Secondly, we conclude that in literature we could not find any overlap between the functionalities of connected cars and security. This overlap, was, however, found in European documentation (see below).

RQ 1.2: Security Requirements

From a process point of view, the ISO 26262 and SAE J3061 can be used to develop a safe and secure connected product in the concept phase. After the feature definition and initiation of the cybersecurity lifecycle, a vulnerability analysis and risk assessment are executed. This step shows the overlap between RQ 2 and RQ 4.

Regarding the identified security requirements, we found in total 6 security requirements in the literature regarding V2X communication. Confidentiality is the most mentioned aspect, followed by authentication, authorisation, integrity and availability. All these aspects are also mentioned at connected cars in general, with data freshness as the outlier.

However, for this categorisation regarding V2X, only 2 usable sources were found, because all the remaining publications focused on the security of the vehicle itself (e.g. internal architecture of ECU's).

RQ 1.3: Privacy Requirements

Regarding privacy requirements we have not identified any requirements in the studied literature. In contrast, literature about connected cars and privacy-focused on three areas: data gathering, GDPR and giving permission. Therefore we dismissed the privacy aspect in our final framework.

9.1.2 RQ 2: Analysing Risks of Connected Cars

In total we identified 12 risk assessment methods, of which only two are specific to V2X, one to privacy, none to telematics, and the remaining 9 to the automotive area in general. This means that the general risk assessment methods about the automotive areas should be scaled to the required specific scope, in this case telematics and V2X, if they want to be useful.

Only one risk assessment method, RACE, offered a detailed implementation of several factors (time, expertise, knowledge, opportunity and equipment) when assessing the likelihood of an attack and was therefore preferred. We did notice the step from SAE J061, where a process of threat and vulnerability analysis (TARA) is described to specific implementations of this process in the form of EVITA / TVRA, and how the RACE framework builds upon both.

9.1.3 RQ 3: Security Requirements in European Standards

The most obvious difference between literature in the identified security requirements in European standards is that of the addition of confidentiality. The reason confidentiality is mentioned the most, is because of the article by Macher et al. (2017) focusing on encryption and therefore protecting the confidentiality of received and send messages. However, as seen in the above section, confidentiality is specific to certain messages. For instance, in V2I projects broadcasted messages meant for multiple vehicles (e.g. road works ahead or closed lane) send from the infrastructure to a vehicle, confidentiality is not important.

However, if a message from an emergency vehicle to other personal vehicles to make way is send via infrastructure, the message should be encrypted in order to prevent spoofing attempts of that message. Furthermore, integrity, availability and non-repudiation are not mentioned in the ETSI standards, but are, however, very important for V2I because of certain risks V2I projects are exposed to. These risks, mapped to the corresponding security requirements, are shown in section 5.2.

In general, it can be stated that the security requirements mentioned in literature form the base for our framework, upon which the European standards - in the form of the ETSI Technical Specifications - elaborate and specify upon.

9.1.4 RQ 4: Risk Analysis

For our risk analysis we used an adjusted version of the RACE framework, as identified as the most suitable risk assessment method in RQ 2. The elements we changed were the knowledge

metrics necessary to successfully exploit a vulnerability. Also, we dismissed controllability factor since this is primarily a safety factor. Lastly, 'easy' in the time aspect at the factor 'opportunity' is within one week in TVRA and 1 day in RACE. For consistency, we used the definition of TVRA, which is one week.

The values of the risks assessment were primarily based on ETSI TS 102 893 and where necessary adjusted for V2I projects, while the attack methods are extracted from multiple sources, i.e. ITU, ETSI and UNECE.

Also, the attack methods belonging to the vulnerabilities were extracted from two sources, namely UNECE and ETSI.

In total only two main vulnerabilities were identified:

- Vulnerabilities regarding back-end servers
- Vulnerabilities to vehicles regarding their communication channels

These two main vulnerabilities are divided by 9 sub-vulnerabilities, given values to the attack potential (as can be seen in Appendix G), attack impact (as can be seen in Appendix F) and therefore the final value risk as can be found in Table 5.6.

9.1.5 RQ 5: Mapping of Measures to Security Requirements

The combined security requirements from literature and European standards were used to map to vulnerabilities. This way the security requirements form the base of the final framework.

The next step was mapping the security requirements per vulnerability to the corresponding measures. The outcome of this mapping can be seen in Table 6.1 and Table 6.2. These tables are categorised with the same two main vulnerabilities as described above.

9.1.6 RQ 6: Creation of Framework

The security requirements, vulnerabilities, attack methods, risk values and measures were all put into the framework: an overview consisting of two tables aiming to help security consultants and project managers of V2I projects to make an as secure V2I system as possible. To achieve this, first four interviews with security consultants of Northwave B.V. were held in order to gather requirements for the final framework regarding usability. The outcomes of the interviews were as follows:

1. Risk-based as a start of the framework, which also correlates with knowledge about an organisation and what to tackle first
2. Framework should be descriptive and not prescriptive, with leaving some interpretation per client if possible
3. Framework with examples of how something can be implemented are being experienced as useful, in order to complement the above statement

This input was used to create the framework, consisting of two related tables. The first table outlines the vulnerabilities of V2I projects together with the attack methods and a risk analysis, consisting of the risk impact, likelihood and final value. The vulnerabilities were also mapped to a set of security requirements which formed the base of the second table. In this second table, the measures per vulnerabilities including fulfilment are presented. These measures are primarily based on ETSI standards, but complemented by the ISO 27002 when applicable. The tables can be seen in section 7.3.

9.1.7 RQ 7: Validation of Framework

To validate the final artefact, a survey was sent to several project managers involved in V2I projects, namely Concorda. This survey focused on a total of 6 aspects of the framework to be judged. Of these aspects, none were received negative, while the measures were received as the most positive aspects to be included in the framework.

We did observe, however, that the security requirements did not contribute to the usability of the framework due to the mapping relatively not being clear between the requirements, measures and vulnerabilities.

The framework in general was perceived to be most useful at future projects within Concorda since the framework could then be implemented by management. This is because of the immature state of current V2I projects, which consist of trails being run and the lack of day-to-day management, according to one of the respondents.

9.2 Discussion

In this section, the findings obtained in the previous chapters will be discussed and interpreted. The discussion will focus on the above conclusions, especially the obtaining and usage of security requirements as a base for the final framework for practitioners in current and future V2I projects.

9.2.1 RQ 1.1: Functions of Connected Cars

In this research, all literature regarding connected cars and security was analysed, automatically including V2I. The move from connected cars as a whole to specifically V2I was to get a clearer picture of what literature already stated about the connected car in general, while also taking V2X (and therefore V2I) into account. The mapping from connected cars to V2I is unconventional but necessary, considering the lack of literature about specifically V2I or even V2X. This meant we could not build upon specific literature about V2I. This missing documentation in this research means that the chosen methodology is open to interpretation and subjectivity. Throughout this research, several steps have been made to prevent bias and subjectivity as much as possible, which also will be explained below.

The initial aim for listing the functionalities of connected cars was to see whether there is a relationship between specific functionalities and security requirements. In the executed literature study, no such relationship was discovered or mentioned. The articles of functionalities of connected cars often focused on hypothetical functions and how to implement these, without focusing on security. Therefore this research question proved afterwards to be the least valuable regarding security and connected cars.

For instance, regarding telematics, there are two categories: convenience functions and functionally enablers. The distinguishing between those categories, however, does not contribute to the final framework since there could be no link found between in-car functionalities and security requirements in connected cars (section 3.3).

In contrary, the categorisation and examples regarding V2X are taken into account for the final framework where applicable. The categorisation regarding functions in V2X - traffic safety, traffic efficiency and convenience functions - are mentioned in the current functions of V2I in Table 4.1. However, categories like V2H and V2E are not being tested in practice at the moment. Furthermore, given examples like 'finding free parking spots' or 'automatic parking' are merely theoretical examples and did not come back regarding which type of messages can be dis-

tributed between vehicles and infrastructure, therefore making it impossible to link into certain security requirements.

RQ 1.1 does, however, reflect upon the state of literature and the reflection upon current and future functions of connected cars / V2X communication. It also made clear that from a car first perspective, functionalities can differ vastly per brand / model and therefore it is difficult to make generalisations about the security of such connected cars, for now and in the future.

9.2.2 RQ 1.2: Security Requirements

For the collection and identification of relevant security requirements, first the security requirements were identified in literature. Later on, these were combined with existing European standards. This process is discussed below.

Throughout the systematic literature review a few aspects became clear. No empirical research of a V2X project from the perspective of a connected car has so far been done with the focus on an information security level. In contrary, research is rather focused towards the architectural / structure of devices.

In order to bridge this gap, our proposed framework focuses on requirements regarding cybersecurity from a Vehicle to Infrastructure (V2I) data and external communication point of view, matched with a connected car. This scope rules out the connections between other nodes of the network or the connection from the backend of a third party (i.e. government) to other internal systems of the infrastructural party.

Identification of Security Requirements

As mentioned before, the security requirements derived from both literature and European standards form the base of the final artefact of this research. This approach means that the security requirements are a guide throughout the framework, giving it a scientific backing while combining it with practice.

Security requirements like confidentiality or authorisation tend to be a high-level description of a certain state and susceptible to interpretation. Therefore these requirements were linked to security requirements mentioned in current existing European documentation. This process of linking the in total 6 security requirements has the necessary interpretation, mainly originating in lack of literature specifically about V2I. To counteract this observation, literature from V2X - of which V2I is part of - was used to derive security requirements. However, only two suitable articles focused on V2X describing necessary security requirements were found in the literature study (see section 3.3).

This potential bias towards only two sources was partly mitigated by looking at other identified security requirements in the connected car area to see if they differentiated too much. This was, however, not the case. At the same time, this could lead us back to the start of this section: security requirements tend to be a high-level description of a certain state, making it potentially easy to match connected cars to V2X and to V2I. By taking only the security requirements of V2X this mapping process has been made as accurate as possible while keeping in mind the open nature of these requirements. Lastly, throughout the structured literature research (section 2.1 the review protocol was followed in order to decrease the subjectivity as much as possible and increased the degree of repeatability.

9.2.3 RQ 1.3: Privacy Requirements

The aim of the literature study was, beside identifying security requirements, identifying privacy requirements regarding connected cars. Notably, only 7 relevant papers could be found, where no significant overlap between subjects could be identified within the publications. The subjects of the papers varied from what data connected cars gathers and uses them for, the influence of GDPR on connected cars, and how permissions of sharing data should be arranged, instead of focusing on specific (technical) requirements how privacy should be obtained in connected cars in general, or even V2X. Therefore the privacy aspect was taken out when creating the final framework, although it was taken into account when doing the risk analysis. This is because a vulnerability or attack method can cause a privacy risk and the aim of the risk analysis is to expose all security-related risks, even if this has an overlap with privacy (see also Appendix F). The lack of literature regarding privacy requirements in connected cars is something to be studied in further research (section 9.4 below).

9.2.4 RQ 2 + 4: Risk Analysis

Risk Analysis Framework

Regarding the final risk analysis being executed in section 5.3, only two frameworks of the many stated in section 3.5 were about V2X. We chose for the RACE framework. RACE takes multiple sources in the form of TVRA and EVITA and combines / simplifies them. This simplification is beneficial when executing a risk analysis but also categorising risks into a few amount of broad categories.

In RACE, only three categories of risks can be obtained: minor, major and critical. This is because the categorisation from values being given about the attack likelihood (see appendix G) is reduced from originally 5 as is the case with ETSI / TVRA, to only three categories. Although this methodologically has no implications for our research, it could lead to a less accurate analysis for when practitioners want to differentiate risks on a more detailed level.

Execution of Risk Analysis

When executing the risk analysis in section 5.3, multiple values regarding multiple factors had to be determined (see Appendix G). These values were derived from ETSI, although changed when this was applicable, as explained in section 5.3. However, these values are always a judgement call and therefore contain assumptions of the author. Values can differ vastly with different amount of knowledge about certain vulnerabilities, especially regarding such a new and novel research area as V2I. Therefore, where possible, ETSI was used as the benchmark. However, in the document itself,they do not explain their reasoning for assigning values, leaving room for interpretation. However, the mapping process of vulnerabilities of UNECE (used as a base) from ETSI gives us the flexibility to compare multiple vulnerabilities and their corresponding values by ETSI and combine them to one, while also taking into account the knowledge of current projects of V2I and the corresponding vulnerabilities. However, no inside knowledge of current projects could be taken into account in the risk analysis. A tool where the parameters could be adjusted would therefore be helpful for practitioners. More about this in section 9.4 below.

9.2.5 RQ 3: Difference between Literature and Standards

Notably, the literature focused much towards existing standards like ISO 26262 and SAE J3061. These standards are primarily about safety and not so much about (cyber) security. Unfortunately, none of these two closed source standards could be obtained. However, several articles

(see section 3.3) were used to analyse the content of these two standards in order to create an accurate picture as possible of the current state of literature about security requirements and connected cars. ISO 21434 does focus on cybersecurity from a car point of view but is not yet available. Therefore these three standards proved not to be valuable to the final framework. Also, they analyse and recommend the process of making a safe and secure car from a process / management point of view, which parts were focused most upon in the publications found about these three standards. This research, on the contrary, focuses more on the combination of management and technical side.

In order to get more a more complete picture of security requirements, European documentation was therefore analysed. These European standards only focused on security requirements on messages and not the system as a whole. This is the reason a requirement like availability was not mentioned in the European documentation because you cannot require a message to be available, but only the system itself (i.e. sending and receiving party). Therefore the mapping from literature to European standards could not be done one-to-one. Another example of the different scope of literature and the European documentation was shown with confidentiality. This requirement was mentioned in literature but in the European standard documentation it only turned out confidentiality is only required with specific messages, i.e. when vehicles receive a message only for them. However, as can be seen in section 4.2, confidentiality according to ETSI is not necessary for any functionality of V2I messages which was included in this research. We did include confidentiality in the final framework as a security requirement, because as can be seen in the literature study, confidentiality still helps with intrusion detection and data theft, both of which could potentially lead to several attack methods mentioned in the framework like routing message manipulation attack or sending false diagnostic messages.

9.2.6 RQ 5: Mapping of Measures to Security Requirements

As mentioned in Chapter 6, we mapped the security requirements to the vulnerability / attack methods independent of each other. For this mapping, the direct relationship between the attack methods, corresponding measures and security requirements was studied. The independent mapping of security requirements to both vulnerabilities and attack methods proved to be beneficial for checking whether we had missed any security requirements regarding the 9 vulnerabilities: we only missed two requirements in the end. Furthermore, it gave us more assurance that the attack methods belonged to the corresponding vulnerability, since we added measures ourselves in the form of ISO 27002, UNECE and ITU and did not only rely on ETSI which we took as the base. It should be noted, however, that this mapping still is the interpretation of the author of this research and could therefore be biased.

9.2.7 RQ 6: Framework

The framework consists of multiple processes of which the most important will be discussed below, starting with the categorisation of vulnerabilities, followed by the categorisation of attack methods, mapping from security requirements to vulnerabilities via measures and finally the identified measures.

Categorisation of Vulnerabilities

The first important step is to make a list of vulnerabilities regarding V2I. For this, there were two sources combined. The main issue here is that both sources - UNECE and ETSI - do not solely focus on V2I but more from a V2X or even vehicle perspective. This shows in the categorisation of vulnerabilities in the ETSI standards, which are split between vehicles and roadside units.

In this research, it was chosen to combine these measures (for the explanation why, see the start of Chapter 5) and map them to the general vulnerabilities UNECE listed. As mentioned before, the document of UNECE where these vulnerabilities are listed are still in a working document and not made definitive yet as of current publication of this research. However, since the list with the in total nine vulnerabilities has appeared three times largely unchanged in several meetings of the working group of UNECE, it was assumed no big changes were due for this list and therefore used as a base for the vulnerabilities.

By combining the two lists and specifying them for specifically V2I in the final framework, we believe this is the most accurate way of creating a list of vulnerabilities without any practical knowledge of existing projects. Furthermore, no documentation or known attacks on V2I are public because this is such a novel area. The list of vulnerabilities is, therefore, a first version and not exhaustive and due to change in the future, even if functionalities of V2I change to specific vehicle function: this will imply both a change to security requirements (e.g. confidentiality) and vulnerabilities to be explored.

Categorisation of Attack Methods

Hand in hand with the list of the nine vulnerabilities go the attack methods. Again, a mapping from multiple sources in the form of UNECE, ETSI and ITU was made in order to align the attack methods with the (more high-level) vulnerabilities. These attack methods are very specific in the sense that they give an indication of how a vulnerability could be exploited by an attacker.

It was, however, never the intention of the framework to describe how this attack could be executed itself. If, for instance, the vulnerability is 'back-end is used as a mean to attack a vehicle' and the vulnerability is 'abuse of privileges by staff' how this staff could abuse its privileges is left open. Otherwise, this list would be unexhaustive and not complete since such a detailed overview of exploitation of vulnerabilities could lead to over completeness and the danger of missing some attack methods of which we currently have no knowledge.

Therefore it is important to emphasise that the list of attack methods is as complete as possible with the used three sources. We spotted also overlap between the sources when suggesting attack methods which strengthen the fact that the scope of the proposed attack methods was the same, i.e. V2X (and therefore V2I).

Mapping from Security Requirements to Vulnerabilities via Measures

Another important step was to map the identified security requirements to the vulnerabilities (and therefore measures at the same time).

The mapping of measures to security requirements was done independently of the mapping of vulnerabilities to security requirements. This was done to check whether the measures were actually related to the mapped vulnerabilities. Also, we could check if we had missed any security requirements in the mapping between vulnerabilities and requirements. In only two of the nine vulnerabilities this was the case. This means the initial mapping of security requirements to vulnerabilities was in 7 of the 9 vulnerabilities accurate and that the security requirements we mapped to the attack methods are also accurate since the attack methods belong to a certain vulnerability.

Measures

When selecting the measures, ETSI and UNECE were once again used as the main sources. In this process, it appeared that some measures were very high-level and not suitable for (direct) implementation for an organisation. An example of too high-level measure is: 'the vehicle

shall verify the authenticity and integrity of messages it receives.' Here no specific (high-level) fulfilment was identified in the used sources. Another example is the measure 'Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data' or 'Security Controls shall be applied to back-end systems.'

These too general measures were where necessary mitigated by 1) inserting a section called 'fulfilment' in the final framework where a direction / example was given of how this measure could be implemented and 2) using the information security standard ISO 27002. This standard gives high-level descriptions of how areas of the ISO 27001 can be implemented. An example is access control, of which ISO 27001 states this is an area that a company should look at, while ISO 27002 states 'A formal user registration and de-registration process should be implemented to enable assignment of access rights' while leaving it up to the organisation itself to assess how this claim can be fulfilled. We believe that with the addition of ISO 27002 we have mitigated the high-level measures in order to be as practical as possible for practitioners involved with security in V2I projects, because of the lack of other documentation regarding mitigating risks in V2X communication in general.

9.3 Limitations

9.3.1 Literature Review

This mapping study adhered to the research protocol that was systematically developed following several well-established guidelines in Kitchenham and Charters (2007), Bandara et al. (2015), Webster and Watson (2002) and Okoli (2015). However, keywords used for retrieving primary studies can still present a potential limitation. Synonyms used for "connected cars" such as "intelligent transport", "intelligent transportation" and "intelligent vehicle", were not used to specifically focus on the car and not transport in general, potentially missing primary studies regarding functions, security, privacy or risk assessment methods.

Furthermore, in contrary to what Okoli (2015) recommends, only one author was involved in the process of picking relevant papers. This introduces bias in the selection of papers, although the inclusion and exclusion criteria were created to counteract this bias as much as possible. To reduce this bias in future literature reviews more authors checking each other is recommended.

In addition, there is (personal) bias in the used backward citation where only the title was scanned and interpreted as relevant / not relevant. If deemed relevant to the subject of connected cars, via Scopus the importance of the paper was assessed by looking at the number of citations. It should be taken into account that citations do not indicate the 'popularity' or 'quality' of a publication. A publication can demand a subscription and is, therefore, less likely to be cited than an open-access publication. This process could therefore be executed more systematically in a future literature review.

Lastly, we notice in general a lack of literature about specifically V2I communication and security. This low amount of usable literature is mainly because of the novelty of V2I communication or even V2X, let alone security in these areas. We also explain this issue in section 3.1.1.

For instance, regarding security requirements and V2X communication - which is more general than V2I - only two articles could be found. Therefore we used grey literature in the form of European documentation to specify security requirements as much as possible towards V2I.

The same holds true for identifying suitable risk assessment frameworks for V2I: again, only two articles regarding assessing risks in V2X were identified. We tailored the most suitable (RACE) framework to V2I as much as possible though, to counteract for this lack of literature.

9.3.2 Framework

It is important to notice that the created framework is 1) only based on existing sources and no practical knowledge about existing projects and 2) these sources were not exclusively about V2I and therefore some mapping is done. As explained above, this mapping is done in a structural way but still leaves the subjectivity of the researcher into play. It is therefore important to remember that the final framework is not the only truth but only a guide for practitioners. With more knowledge about V2I, a better judgement could be made about the vulnerabilities and specific measures that could be (realistically) implemented.

Also, the problem arose that some standards like from CEN/TC 278 turned out to be very relevant (see section 4.1.2) but closed source and could not be obtained, even after asking the Rijkswaterstaat itself. If these standards could be included, the security requirements as a base could be even stronger and more easily verifiable, instead of relying on only two sources as in this research.

Furthermore, general standards like ISO 27001 and CIS (Critical Security Controls) are fully not taken into account regarding measures. Only ISO 27002 was consulted when a implementation of a too high-level measure was necessary. Standards like ISO 27001 and CIS are set up to broadly in scope that they can be applicable for V2I but in this research it was chosen not to in order to be as specific as possible.

In addition, the argumentation to include high-level security requirements derived from literature is not directly clear. The security requirements were about V2X and not V2I itself. This is, however, a limitation of literature itself and we tried to complement the security requirements with European standards / guidelines. However, for practitioners, the inclusion of security requirements could hold limited value since they do not see this process in the framework itself.

9.4 Further Research

Our framework lays the base for further research regarding V2I. There are, however, some gaps which still can be filled in with future research. This section will outline some possibilities regarding further research.

The first is that our framework is based solely on theoretical knowledge. Once more practical knowledge is obtained about V2I projects and their functionalities / equipment, more adequate measures can be designed. This knowledge could be obtained by analysing existing projects of V2I and the possibilities regarding security.

Also, in the interviews with Northwave, it appeared that in practice, a framework can be used to obtain a certain baseline / minimum security requirements after you have done the first risk analysis, after which you start tackling this baseline first before implementing all measures. Such a distinction in security requirements and measures has not been made in this framework. Rather, it is assumed that all requirements and measures have to be complied to in order to obtain a secure V2I system as possible. This distinction between security requirements and corresponding risks could be taken into account for further research.

Following this reasoning, the vulnerabilities in the final framework are presented from critical to minor risks. This order of these vulnerabilities is subject of change and dependent on several parameters being filled in to the best of knowledge of this researcher. However, to be as specific as possible for every project, a separate risk analysis should be held. When this risk analysis is done and quantified, this input can be used in order to identify corresponding measures and security requirements. A tool or template where these specific parameters can be put in order to match the specific functionalities of V2I projects is therefore a logical step for future research.

In addition, the security requirements could be made more specific, once research would describe specific aspects of V2I projects and which specific requirements correspond to that, instead of only the high-level requirements we used in this research. This would help the framework in being more specific on how security requirements contribute to the prevention of vulnerabilities being exploited.

Lastly, regarding literature, we identified a lack of research regarding both security and privacy requirements in V2X (or even V2I). This gap in literature, especially regarding privacy requirements, could be due to further research in order to process privacy in a future version of the framework.

9.5 Recommendations

In such a new and unexplored research area of V2I, there are many unknowns. However, history teaches us a few things regarding security. One is that, when developing a new product, the principle of 'security by design' is often forgotten in order to ship a product quickly to the market and develop from there. This is also confirmed by one of the participants of the case study. Our framework aims to prevent this trap, by giving project managers / security companies a handle of where to look when developing or analysing new / future V2I projects.

The novelty of V2I also implies that many functions are still due to development. This could also influence the vulnerabilities and therefore the framework as a whole, as discussed before. Therefore this framework purely serves a base of the current knowledge about how trials with V2I are executed and functionalities which can be safely predicted to be rolled out in the coming years. After that, it is unsure what cars can send / receive to infrastructure and the other way around, and the framework could be completely redundant by that time. It is therefore recommended to closely look at the beginning of each project / added functionality what the implications are regarding security, and how this could be mitigated. This research also gives a base of how this can be done and with which tools this can be done without any practical or real-life knowledge about a (future) project. This way security can always be taken into account in V2I.

Furthermore, there was no specific V2I literature regarding security found as when this research was made. This is, however, subject to change when projects get more mature and rolled out in practice instead of only being trials. Literature serves as a base for this framework and new insights in research should always be taken into account.

When using this framework, the broad applicability should also be taken into account. This is done by design but still leaves interpretation of how a certain vulnerability affects a V2I project - if at all - and which values correspond to that. Therefore it is recommended to fit the scope of a V2I project to the specific vulnerabilities and how important they are and use the proposed attack methods / measures as a guide of what aspect could be considered and not as an all-inclusive list.

The same holds true regarding standards and the synthesising of these standards. This framework merged several vulnerabilities, measures and attack methods into one overview. However, a change in one of the used sources could lead to changes in the framework as a whole. Also, the mapping process could be heavily influenced by this if certain measures comply with other security requirements for instance. This process is unpredictable and should also be closely watched in the future.

9.6 Contribution to Theory and Practice

The contribution of this research is multifold, divided by contributions to theory and practice. In this section, the contributions of this research are outlined and explained, starting with the contribution to practice.

9.6.1 Practice

By answering all research questions, there are in total 5 main contributions to practitioners of V2I projects, as listed below:

1. List of 9 vulnerabilities specific to V2I projects, extracted and mapped from UNECE and ETSI.
2. List of attack methods corresponding to these vulnerabilities, extracted and mapped from UNECE, ETSI and ITU.
3. Risk analysis of the vulnerabilities, including attack impact and attack likelihood.
4. Security requirements - extracted from both literature and European documentation by analysing a total of 10 organisations - corresponding to the vulnerabilities and measures.
5. Measures originating from UNECE and ETSI mapped to the attack methods, mapped to the vulnerabilities and supplemented by ISO 27002 where necessary.

The framework is designed for practitioners involved in either security, V2I or both and gives an overview of the most important vulnerabilities in V2I projects via a risk analysis, complemented by measures. This framework is a comprehensive overview of all of these aspects, without being prescriptive. This enables the stakeholders of this framework to adjust the framework were necessary but potentially using this framework as their main guide throughout the security of V2I projects.

For the first two contributions, it is the first time the above-mentioned sources are 1) combined and 2) made specific to V2I projects. Furthermore, the risk analysis is useful as a base for V2I projects to work upon if resources / knowledge are not available for a specific risk analysis of the project.

It is also the first time that security requirements from both literature and European documentation are matched and combined and used as a base for our framework. This means that managers involved in security always are aware of why a certain mitigation / vulnerability matters to their project on a high level. Furthermore, the measures we identified and mapped to the 9 vulnerabilities and corresponding security requirements, can be used as a baseline to manage security in V2I projects, without having the technical implementation stated. This way managers can use these measures to discuss with vendors.

9.6.2 Research

As mentioned before, there is no research available specifically aimed at V2I and security. This research addresses this gap. Much existing research focuses on a specific (theoretical) solution of how internal communication in connected cars can be handled, while research about external communication and security is scarce. This holds true to both security and privacy requirements as well as the risk assessment frameworks (see also Chapter 3). Our research can therefore be seen as an overview of what literature is available regarding both connected cars and V2X communication specifically, where the gaps are and how research can contribute to security in V2I. This research lays the base for this process.

Secondly, the combination of existing knowledge in the form of several European standards / documentation (practice) and literature (theory) contributed to the final framework, which is verified in the Dutch market by a case study. The reason for including these security requirements was to lay a scientific research-based layer beneath the final framework and to form a bridge between literature and practice. This approach is something not often seen or explicitly shown in current security / information security standards like the ISO standards. Our approach shows that bridging the gap between literature and practice in security in V2I projects is possible with a mapping process.

Lastly, this research shows that current literature is lacking in regards to security and V2I projects. This is mainly because of the lack of existing V2I projects but the principle 'security by design' also forces researchers to look ahead of what is coming instead of waiting for market developments to be worldwide spread. This research sets up a base of general V2I projects of which further work can elaborate instead of only relying on grey literature (see also section 9.4 on further research).

Bibliography

Ahmadi, S. (2019). Chapter 7 - vehicle-to-everything (v2x) communications. In S. Ahmadi (Ed.), *5G NR*, pp. 789 – 843. Academic Press.

Akalu, R. (2018). Privacy, consent and vehicular ad hoc networks (vanets). *Computer law & security review 34*(1), 37–46.

Ando, E., T. Kawauchi, N. Komoda, and T. Fujiwara (2018). Security risk assessment supporting system in connected car systems. pp. 389–394. cited By 0.

Axelrod, C. W. (2017). Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. In *2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT)*, pp. 1–6. IEEE.

Bandara, W., E. Furtmueller, E. Gorbacheva, S. Miskon, and J. Beekhuyzen (2015). Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support. *Communications of the Association for Information Systems 37*, 154–204.

Beckers, K., J. Dürrwang, and D. Holling (2016). Standard compliant hazard and threat analysis for the automotive domain. *Information 7*(3), 36.

Boudguiga, A., A. Boulanger, P. Chiron, W. Klaudel, H. Labiod, and J.-C. Seguy (2015). Race: Risk analysis for cooperative engines. In *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5. IEEE.

Burzio, G., G. F. Cordella, M. Colajanni, M. Marchetti, and D. Stabili (2018). Cybersecurity of connected autonomous vehicles: A ranking based approach. In *2018 International Conference of Electrical and Electronic Technologies for Automotive*, pp. 1–6. IEEE.

Coppola, R. and M. Morisio (2016). Connected car: technologies, issues, future trends. *ACM Computing Surveys (CSUR) 49*(3), 46.

CROW (2019). Stappenplan ivri: Handreiking voor wegbeheerders. `https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/verkeersregelinstallaties/stappenplan-ivri`. Accessed: 10-04-2020.

Darvish Rouhani, B., M. Mahrin, F. Nikpay, R. Ahmad, and P. Nikfard (2015, 02). A systematic literature review on enterprise architecture implementation methodologies. *Information and Software Technology 62*.

De, S. (2018). Next-gen business models for the automotive industry for connected cars and services. Technical report, SAE Technical Paper.

De Vries, D. and T. Van Engers (2019). Privacy on wheels. *Jusletter IT* (February). cited By 0.

Deichmann, J. (2019). The race for cybersecurity: Protecting the connected car in the era of new regulation. `https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/`

the-race-for-cybersecurity-protecting-the-connected-car-in-the-era-of-new-regulation. Accessed: 06-02-2020.

Dynniq (2019). Volkswagen golf supports car2x via its-g5, but the eu member states are still divided on which c-its standard to use: how to move forward? https://dynniq.com/volkswagen-chooses-its-g5-in-new-golf/. Accessed: 28-02-2020.

Ebert, C. (2017). Risk-oriented security engineering. *Automotive-Safety & Security 2017-Sicherheit und Zuverlässigkeit für automobile Informationstechnik*.

ETSI (2012). Etsi ts 102 942 v1.1.1: Intelligent transport systems (its); security; access control.

ETSI (2018). Etsi ts 102 940: Intelligent transport systems (its); security; its communications security architecture and security management.

ETSI, T. (2010). 102 731 v1.1.1, intelligent transport systems (its); security; security services and architecture.

ETSI, T. (2019). Etsi ts 102 941 v1.3.1: Intelligent transport systems (its); security; trust and privacy management.

Harmsen, A. (1997, 1). *Situational Method Engineering*. Ph. D. thesis, University of Twente.

Hong, J., J. Shin, and D. Lee (2016). Strategic management of next-generation connected life: Focusing on smart key and car–home connectivity. *Technological Forecasting and Social Change 103*, 11–20.

Hu, Q. and F. Luo (2018). Review of secure communication approaches for in-vehicle network. *International Journal of Automotive Technology 19*(5), 879–894.

Inayat, I., S. Salim, S. Marczak, M. Daneva, and S. Shamshirband (2015). A systematic literature review on agile requirements engineering practices and challenges. *Computers in Human Behavior 51*, 915–929.

Intercor (2020). About intercor. https://intercor-project.eu/homepage/about-intercor/. Accessed: 05-08-2020.

Islam, M. M., A. Lautenbach, C. Sandberg, and T. Olovsson (2016). A risk assessment framework for automotive embedded systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, pp. 3–14. ACM.

Ivanov, I., C. Maple, T. Watson, and S. Lee (2018). Cyber security standards and issues in v2x communications for internet of vehicles.

Jaisingh, K., K. El-Khatib, and R. Akalu (2016). Paving the way for intelligent transport systems (its): Privacy implications of vehicle infotainment and telematics systems. In *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, pp. 25–31. ACM.

Kitchenham, B. and S. Charters (2007, 01). Guidelines for performing systematic literature reviews in software engineering.

Kong, H.-K., M. K. Hong, and T.-S. Kim (2018). Security risk assessment framework for smart car using the attack tree analysis. *Journal of Ambient Intelligence and Humanized Computing 9*(3), 531–551.

Lee, S.-W. (2017). Itu-t sg17 work on its security – x.1373 and x.itssec-2. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Documents/S2-Lee.pdf. Accessed: 28-06-2020.

Macher, G., E. Armengaud, E. Brenner, and C. Kreiner (2016). Threat and risk assessment methodologies in the automotive domain. *Procedia computer science 83*, 1288–1294.

Macher, G., H. Sporer, E. Brenner, and C. Kreiner (2017). An automotive signal-layer security and trust-boundary identification approach. *Procedia Computer Science 109*, 490–497.

Möller, D. P. and R. E. Haas (2019). *Guide to Automotive Connectivity and Cybersecurity: Trends, technologies, innovations and applications.* Springer.

Monteuuis, J.-P., A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien (2018). Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, pp. 3–14. ACM.

Mourad, A., S. Muhammad, M. O. Al Kalaa, H. H. Refai, and P. A. Hoeher (2017). On the performance of wlan and bluetooth for in-car infotainment systems. *Vehicular Communications 10*, 1–12.

Nawrath, T., D. Fischer, and B. Markscheffel (2016). Privacy-sensitive data in connected cars. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 392–393. IEEE.

Nederhoed, P. (2015). *Helder rapporteren: een handleiding voor het opzetten en schrijven van rapporten, scripties, nota's en artikelen*. Bohn Stafleu van Loghum.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems 37*(1), 879–910.

Othmane, L. B., H. Weffers, M. M. Mohamad, and M. Wolf (2015). A survey of security and privacy in connected vehicles. In *Wireless sensor and mobile ad-hoc networks*, pp. 217–247. Springer.

PraktijkproefAmsterdam (2020). Primeur in europa: C-v2x uitgerold en getest op testtrack concorda amsterdam. `https://www.praktijkproefamsterdam.nl/actueel/nieuws/primeur-europa-c-v2x-uitgerold-en-getest-op-testtrack-concorda-amsterdam`. Accessed: 05-08-2020.

Ram, P., J. Markkula, V. Friman, and A. Raz (2018). Security and privacy concerns in connected cars: A systematic mapping study. In *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, pp. 124–131. IEEE.

Rijkswaterstaat (2020). Concorda: introducing self-driving cars and a hybrid communication infrastructure. `https://www.rijkswaterstaat.nl/english/mobility/projects/concorda/index.aspx`. Accessed: 04-08-2020.

Sabaliauskaite, G., J. Cui, L. S. Liew, and F. Zhou (2018). Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. In *2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS)*, pp. 723–728. IEEE.

Schmittner, C., G. Griessnig, and Z. Ma (2018). Status of the development of iso/sae 21434. In *European Conference on Software Process Improvement*, pp. 504–513. Springer.

Schmittner, C., Z. Ma, C. Reyes, O. Dillinger, and P. Puschner (2016). Using sae j3061 for automotive security requirement engineering. In *International Conference on Computer Safety, Reliability, and Security*, pp. 157–170. Springer.

Schmittner, C. and G. Macher (2019). Automotive cybersecurity standards-relation and overview. In *International Conference on Computer Safety, Reliability, and Security*, pp. 153–165. Springer.

Siegel, J. E., D. C. Erb, and S. E. Sarma (2017). A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas. *IEEE Transactions on Intelligent Transportation Systems 19*(8), 2391–2406.

Socrates2 (2020). About socrates 2.0. `https://socrates2.org/about/our-mission`. Accessed: 06-08-2020.

Svangren, M. K., M. B. Skov, and J. Kjeldskov (2017). The connected car: an empirical study of electric cars as mobile digital devices. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pp. 6. ACM.

Tbatou, S., A. Ramrami, and Y. Tabii (2017). Security of communications in connected cars modeling and safety assessment. In *Proceedings of the 2nd international Conference on Big Data, Cloud and Applications*, pp. 56. ACM.

TR, E. (2017). Etsi tr 102 893: Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra). *Intelligent Transport Systems (ITS)*.

Traffic, T. (2019). Gebruikers flitsmeister krijgen nu ook zicht op verkeerslichten. `https://www.talking-traffic.com/en/news/gebruikers-flitsmeister-krijgen-nu-ook-zicht-op-verkeerslichten`. Accessed: 10-04-2020.

Vékony, A. (2016). Speech recognition challenges in the car navigation industry. In *International Conference on Speech and Computer*, pp. 26–40. Springer.

Verhoeven, N. (2007). Wat is onderzoek. *Praktijkboek methoden en technieken voor het hoger onderwijs*.

von Wedel, J. K. and P. Arndt (2018). Safe and secure development: Challenges and opportunities. Technical report, SAE Technical Paper.

Walker, A. (2018). Cybersecurity in safety-critical systems. *Journal of Software: Evolution and Process 30*(5), e1956.

Walter, J., B. Abendroth, and N. Agarwal (2017). Pricon: self-determined privacy in the connected car motivated by the privacy calculus model. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia*, pp. 421–427.

Ward, D. and P. Wooderson (2016). Automotive cyber-security integrity levels.

Webster, J. and R. Watson (2002, 06). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly 26*, xiii–xxiii.

Wiebering-Losse, M. (2009). *Onderzoeksvaardigheden voor docenten: methoden en technieken voor het uitvoeren en begeleiden van praktijkonderzoek*. Boom uitgevers Den Haag.

Wieringa, R. (2014). *Design science methodology for information systems and software engineering*. Springer. 10.1007/978-3-662-43839-8.

Wolfswinkel, J., E. Furtmueller, and C. Wilderom (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems 22*(1), 45–55.

Xiong, W. and R. Lagerström (2019). Threat modeling of connected vehicles: A privacy analysis and extension of vehiclelang. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1–7. IEEE.

Zallone, R. (2019). Connected cars under the gdpr. In *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, pp. 1–6. IEEE.

A NOTES PER SEARCH ENGINE

Notes for every search engine in order to ensure reproducibility

- Scopus: standard procedure (title, abstract, keywords)
- ScienceDirect: does not support wildcards
- IEEEExplore: both title and abstract searched
- Springer: searches for match in both title and all other fields in advanced search. Therefore decided to get the most accurate matches to only search in all resources + automotive or connected car in the title, instead of matching all terms with the title since many matches got lost in that process
- ACM Digital Library: same principle as above: searched for automotive or connected car in the title and in the abstract for all the stated terms via booleans. However, the fields beneath each other DO NOT serve as a OR statement but are rather merged via an AND statement

B AMOUNT OF PUBLICATIONS PER SEARCH ENGINE AND SEARCH TERMS

N.B: numbers displayed are after year filter!	*Source*				
RQ1	**Scopus**	**ScienceDirect**	**IEEExplore (only abstract + title)**	**Springerlink**	**ACM Digital Library**
"Connected car*" AND (features OR possibilities)	53	5	8	24	27
("Connectivity features" OR "Connectivity functions") AND automotive	3	0	0	0	0
("Infotainment system*" OR Telematics) AND "Connected car*"	27	2	10	0	27
"Connected car*" AND "Vehicle communication system*"	0	0	1	0	3
RQ2					
"Cyber security" AND (Automotive OR "Connected Car*")	138	5	26	2	1
"Cyber security" AND ("ISO 26262")	15	2	1	0	0
"Cyber security" AND ("ISO 21434")	0	0	0	0	0
"Cyber security" AND ("connected car*" OR automotive) AND (standard OR framework)	46	2	11	0	28
RQ3					
"Connected Car*" AND (Privacy OR GDPR)	49	3	22	1	13
"Connected Car*" AND ("data gathering" OR "big data")	33	2	12	0	13
"Connected Car*" AND "privacy requirement*"	0	0	0	0	0
"Privacy" AND "Connected car*" AND ("standard*" OR "framework*")	9	0	1	0	0
RQ4					
("Risk Analysis" OR "Risk Assessment framework" OR "Classification Framework") AND (Automotive OR "connected car*" OR "Connected vehicle*")	130	11	0	X	10
("Cyber Security Assessment" OR "Cyber security analysis") AND (Automotive OR "connected car*" OR "Connected vehicle*")	0	0	8	X	2
("Privacy analysis" OR "Privacy Assessment") AND (Automotive OR "connected car*" OR "Connected vehicle*")	4	0	1	X	2
	507	32	101	27	126

Figure B.1: Amount of Publications per Search Engine and Search Terms

C QUALITY ASSESSMENT RQ 1 AND RQ 2

Outcome of quality assessment of RQ 1.1 until 2.1, exported from an Excel sheet. Strikethrough means paper dismissed. This is also the case for the other appendixes of the quality assessment.

		Research aim / objective			*Context research*			*Findings*			*Diversity perspective / context*			*Valuable*	
Article	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	1	0.5	0
Strategic management of next-generation connected life: Focusing on smart key and car–home connectivity	X				X		X			X				X, the outcomes of possibilities are fictional and not practically focused, however, some outcomes are claimed to be market-based	
On the performance of WLAN and Bluetooth for in-car infotainment systems	X			X			X			X				X, the primary focus of the study was on measuring bluetooth performance, not on connected car applications	
Speech Recognition Challenges in the Car Navigation Industry		X			X		X			X				X, only examples of section 2/3	
Guide to Automotive Connectivity and Cybersecurity		X		X				X		X				X, some very technical chapters and some not	
~~BlueID: Enabling Robust In-car Localization and On-demand Personalization Using Bluetooth~~															X, research is by Samsung and a theoretical one, so paper dismissed
Connected Car: technologies, issues, future trends		X		X			X			X			X, very		
Connected Car Overview: Solutions, Challenges and Opportunities		X			X		X				X		X, focus on V2X		
Vehicle-to-Everything (V2X) Communications (Ch. 7)		X			X		X			X				X, focus on technical aspect of 3GPP for V2X communication, but with some examples and use cases and used protocols	
The Connected Car: An Empirical Study of Electric Cars as Mobile Digital Devices	X				X			X		X				X, case study on connected cars with households	
~~"Connected Car"-Based Customised On-Demand Tours: The Concept and Underlying Technologies~~	X				X			X				X		X, only focuses on a specific part of connected cars namely on demand tours but this is only theoretical and therefore dismissed	
Introducing Connected Vehicles			X		X		X			X			X, focus on V2X		
RQ 1.2															
~~Automotive Vehicle to Everything (V2X) Communication Using IOT~~			X		X				X			X			X, paper dismissed
														X, very high level and theoretical	
RQ 1.3															
~~An Smart Key-initiated Multiple Operating System for Personalized Connected Cars~~	X, article exluded to only being theoretical and not practical				X				X						
Next-Gen Business Models for the Automotive Industry for Connected Cars and Services	X				X		X			X				X, calculations of business models are not relevant but given examples of features in connected cars are	
A Survey of the Connected Vehicle Landscape— Architectures, Enabling Technologies, Applications, and Development Areas	X			X			X			X			X, very, third paper of excellent relevance		
Security of communications in connected cars Modeling and safety assessment	X				X			X			X			X, focus more on V2X communiocation and high level requirements regarding cyber security. Therefore moved to RQ2 literature	
Added Afterwards															
Cybersecurity Challenges of Systems-of-Systems for Fully-Autonomous Road Vehicles		X		X				X		X			X, the examples given in tables are very useful to identify features of cars, while the main focus of the article is to emphasize the consequences of lack of standards, which can be useful to answer RQ2 as well		
RQ1 Backward citation															
Opportunities and Challenges of Vehicle-to-Home, Vehicle-to-Vehicle, and Vehicle-to-Grid Technologies		X			X			X		X				X, marginally, completely other direction with charging of EV's but with connected perspective in this	
Digital networks in the automotive vehicle			X		X	X				X				X, only for introductory purposes	

Figure C.1: RQ 1.1 Quality Assessment

		Research aim / objective			*Context research*			*Findings*			*Diversity perspective / context*			*Valuable*	
Article	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	1	0.5	0
Automotive cyber security integrity levels	X					X		X		X				X, focus on existing risk analysis methods and standards which are useful along with a mapping of these different standards	
Challenges and Mitigation of Cyber Threat in Automated Vehicle: An Integrated Approach	X			X				X		X				X, focus on both organisation and technical aspects of threats in connected cars	
Cybersecurity of Connected Autonomous Vehicles	X					X	X				X		X, focus on existing activiteis from regulatory bodies like the European Union which gives a accurate picture of the political / regulatory side of connected cars		
Review of secure communication approaches for in-vehicle network	X				X		X			X				X, although technical paper, current standards for in-car networks are described	
~~Towards Secure and Safe Appified Automated Vehicles~~															X, paper excluded due to theoretical perspective and no practical values are described, even not in the introduction
Highly Available, Self-Defending, and Malicious Fault-Tolerant Systems for Automotive Cybersecurity		X			X			X		X				X, mainly focus on theoretical improvements of existing standards but therefore of party value to answer RQ2	
An Automotive Signal-Layer Security and Trust-Boundary Identification approach	X			X			X				X			X, focus on signal layer based on Hardware-software layer (HSI) but elaborate description of existing standards	
An Automotive Signal-Layer Security and Trust-Boundary Identification approach		X			X			X		X			X, practical and recent overview of used standards by different OEMS		
Safe and Secure Automotive Over-The-Air Updates	X			X				X		X				X, very specific focus on OTA updates	
Risk-Oriented Security Engineering		X			X				X		X			X, only the overview of existing standards is useful, the main contribution of this paper not so	
Car hacking: Navigating the regulatory landscape	X				X		X			X			X, explains the need for regulations in connected cars, so useful for introduction of RQ2 along with an overview of current regulations		
Safe and Secure Development: Challenges and Opportunities	X				X		X			X			X, goal is to give examples of syngeries and dependencies between ISO 26262 and SEA J3061		
Cybersecurity in safety−critical systems		X				X		X			X			X. high level explanation of the SAE J3061 cybersecurity standard, can thefore be used as short introduction into this standard	
Other															
~~Design of a Framework for Security Enhancement in Telematics Control Units (TCUs)~~															X, technical implementation
A Study on Secure Protocol Techniques Supporting TCUs in a Telematics Environment			X		X			X			X			X, some detailed information about communication protocols and corresponding standards can be found in this article	
Automotive SPICE, Safety and Cybersecurity Integration	X				X			X		X			X, practice and theory meet each other in the SOQRATES working group, which combine functional safety from ISO 26262 and cyber-security requirements from SEA J3061 into the SPICE assessment model (see also article above)		
ISO 21434															
Status of the Development of ISO/SAE 21434		X		X				X		X			X, ISO 21434 is not published yet but useful to know what the standard focuses on and what is therefore expected		
Automotive Cybersecurity Standards - Relation and Overview	X			X			X				X		X, even more specific information about ISO 21434		
In Search of Synergies in a Multi-Concern Development Lifecycle: Safety and Cybersecurity	X			X				X		X				X, potential syngergies between the ISO 26262 and the first working draft of the ISO 21434 are investigated	
Backwards citation															
A Survey of Security and Privacy in Connected Vehicles	X				X		X			X				X, the taxonomy mentioned in this article can be used to create table and match other articles to it	
Cybersecurity: Best Practices for Modern Vechicles		X		X			X			X				X, here the practical side of the United States department of Transporation can be compared to the theoretical frameworks identified before	
Framework for Security and Privacy in Automotive Telematics															

Figure C.2: RQ 1.2 Quality Assessment

		Research aim / objective			*Context research*			*Findings*			*Diversity perspective / context*			*Valuable*			
Article	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	1	0.5	0		
Connected Cars under the GDPR		X		X					X		X			X, GDPR in connection to connected cars is explained but more on a high level			
Privacy on wheels	X			X			X				X			X, more useful for introduction for need / awareness of privacy in connected cars			
Privacy, consent and vehicular ad hoc networks (VANETs)		X			X			X						X, here also the relation between privacy and connected cars is explained, along with a technical proposal in VANETS to be privacy friendly			
Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things		X			X			X		X				X, the technical proposal for Vehicular networks is not useful but the introduction and examples in relation to privacy are			
Paving the Way for Intelligent Transport Systems (ITS): Privacy Implications of Vehicle Infotainment and Telematics Systems	X				X		X			X			X, many aspects and examples of privacy in connected cars are described				
Privacy-Sensitive Data in Connected Cars	X				X				X			X		X, classification of collected data can be used but paper is very short on details			
Connected Cars: Automotive Cybersecurity and Privacy for Smart Cities			X		X			X		X				X, high level requirements for privacy are described in a subsection of this chapter			
~~PRICON: Self-determined privacy in the connected car motivated by the privacy calculus model~~															X, only theoretical user interface		
Security and Privacy Concerns in Connected Cars: A Systematic Mapping Study	X			X			X			X			X, a comprehensive overview of existing literature regarding mainly security but also privacy, so paper can be used for answering both RQ's. Also the proposed solutions from researchers to mitigate threats are mapped here				
The GDPR and the Internet of Things: a three-step transparency model		X		X				X		X			X, the GDPR and guidelines to implement this in Iot are described with connected cars as a case study				
RQ3.2															X, only theoretical solution		
~~GS1 Connected car using EPCIS-ONS system~~																	
Other																	
Connected Vehicles: A Privacy Analysis	X				X			X			X		X, recent and high level overview of data being collected by cars, along with a sample				
Can privacy concerns for insurance of connected cars be compensated?	X				X		X				X		X, gives a granual importance of privacy against financial compensation				
Backwards citation																	
Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation	X				X		X			X				X, an overview with projects with connected / autonomous cars is given. The rest of the paper is detailed in technical communications between cars and therefore not much of use to answer RQ3			

Figure C.3: RQ 1.3 Quality Assessment

		Research aim / objective			*Context research*			*Findings*			*Diversity perspective / context*			*Valuable*	
Article	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	1	0.5	0
Frameworks															
AVES – Automated Vehicle Safety and Security Analysis Framework	X				X			X		X				X, focused towards automated vehicles but cyber security is consisered in the proposed framework called AVES Framework, targeted towards whole lifecycle of a car	
In Search of Synergies in a Multi-Concern Development Lifecycle: Safety and Cybersecurity	X			X				X		X			X, potential syngergies between the ISO 26262 and the first working draft of the ISO 21434 are investigated		
A Framework to Assess Value of Information in Future Vehicular Networks	X			X				X			X				X, very technical paper about value of information and corresponding framework to estimate this per aspect
Detailed Analysis of Security Evaluation of Automotive Systems Based on JASO TP15002	X				X		X						X, explanation and suggested improvement of the standard JASO TP15002		
A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context	X			X			X			X			X, review of available threat analysis methods and recommendations of SAE J3061 regarding threat analysis and risk asssessment method (TARA) are given		
Threat Modeling and Security Issues for the Internet of Things	X			X					X	X					X, only described on high level and connected car part is not much mentioned
Other															
Using SAE J3061 for Automotive Security Requirement Engineering	X				X		X			X			X, focus on SAE J3061 and the Threat Analysis and Risk Assessment (TARA)		
Backward citation															
A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems		X			X			X		X			X, a quantitative risk analysis, to target balancing costs and security risks. Remains to be seen if this method can be used in further research		

Figure C.4: RQ 2 Quality Assessment part 1

		Research aim / objective			*Context research*			*Findings*			*Diversity perspective / context*			*Valuable*	
Article	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	Yes	Partially	No	1	0.5	0
Research on Information Security Test Evaluation Method Based on Intelligent Connected Vehicle	X			X				X		X				X, Technical evaluation of security of connected cars, used for multiple aspects of the car, but theoretical framework with layers can be of use	
On threat analysis and risk estimation of autmotive ransomware		X		X			X			X				X, risk analysis for ransomware, so very specific to this aspect	
Security Risk Assessment Supporting System in Connected Car Systems	X				X		X				X		X, risk asssment based on SAE J3061 is created here		
Standard Compliant Hazard and Threat Analysis for the Automotive Domain	X				X			X		X			X, both ISO 27001 and ISO 26262 are used to create threat analysis for malicious attackers or how to select appropriate security countermeasures		
RACE: Risk Analysis for Cooperative Engines	X				X		X				X		X, (only) Risk analysis method for specifically V2X communication, no risk mitigations are mentioned		
A Risk Assessment Framework for Automotive Embedded Systems	X			X			X			X			X, a quantitatife risk analysis method for automotive, based on ISO 26262, also using different threats and potential impacts		
Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems	X			X				X		X			X, a quantitatife risk analysis method called HARA for automotive, also mentioned in the article above (including comparison). Also focus on functional safety		
Security risk assessment framework for smart car using the attack tree analysis		X			X		X			X			X, security risk assessment framework based on the security risk analysis model ISO 13335, using an attrack tree		
Threat and Risk Assessment Methodologies in the Automotive Domain	X			X			X			X			X, presents an overview of existing threat and risk assessments, so can be used as a reference for other analyis methods		
Using STPA in an ISO 26262 Compliant Process		X			X			X		X				X, in this article the STPA is processed into the ISO 26262 and also compared to the Hazard Analysis and Risk Assessment (HARA) of ISO 26262	
Case Study for Defining Security Goals and Requirements for Automotive Security Parts Using Threat Modeling			X		X			X			X			X, some models for threat modeling are described but not much in detail and also quantifiable	
Integrated Safety and Cybersecurity Risk Analysis of Cooperative Intelligent Transport Systems	X			X			X			X			X, propsal of a framework with ISO 26262, SAE J3061, US2, Evita, TVRA and RACE (mentioned before) in mind, but focused on V2X communication		
SARA: Security Automotive Risk Analysis Method	X			X				X		X			X, systematic threat analysis and risk assessment framework, SARA		
Security Risk Assessment for Connected Vehicles Based on Back Propagation Neural Network	X				X		X				X			X, technical paper with risk assessment based on neural network, but the introduction and used aspects are useful	
Privacy															
Threat Modeling of Connected Vehicles: A privacy analysis and extension of vehicleLang		X				X			X		X				X, technical paper of existing Vehiclelang language with privacy extension. Very specific.

Figure C.5: RQ 2 Quality Assessment part 2

D ELEMENTS OF PKI STRUCTURE

In this appendix, we explain how security requirements can be implemented according to ETSI TS 102 941, where trust and privacy management are described via the description of several parties involved in the process of encryption via a PKI structure.

Cryptographic algorithms are used to provide the V2X ITS security requirements. These algorithms rely on symmetric or asymmetric keys. Public key certificates and Public Key Infrastructure (PKI) are used to establish and maintain trust between the ITS-S and other ITS-S and authorities. To use asymmetric keys, a ITS station has to contact a trusted Certification Authority (CA) to get a certificate (Ivanov et al., 2018).

There are several functional element roles of the PKI, stated in Table D.1.

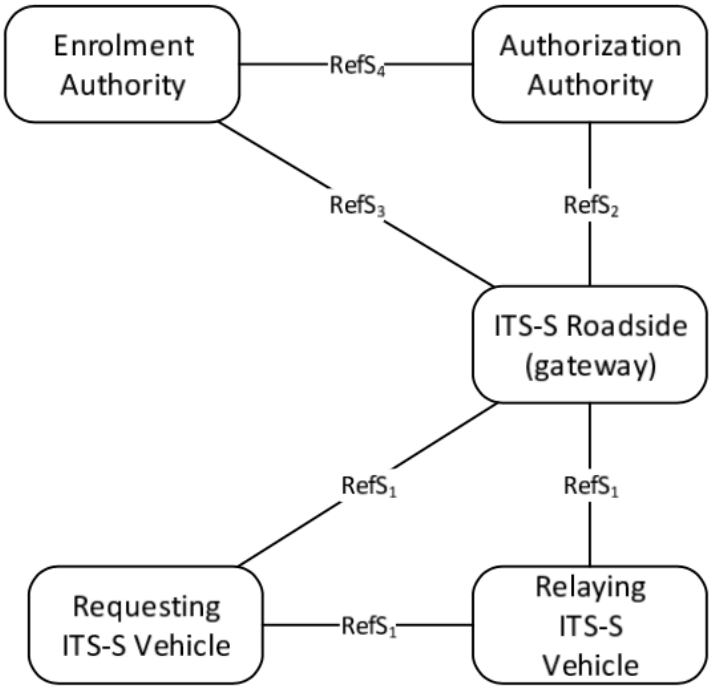

Figure D.1: Functional Elements of PKI Structure

In Figure D.1, the model specified in ETSI (2018) is refined by considering one ITS-S sending the certificate request message, one roadside ITS-S for relaying the message via the infrastructure network to the recipient Certificate Authority and the receiving Certificate Authority (EA or AA).

ETSI (2012) adds two specific examples of how authorisation and authentication requirements can be implemented. Authentication and authorisation information (permissions) for CAMs should be encoded in authorisation certificates. CAM messages shall include both of the following:

Table D.1: Communication with PKI using a V2I connection

Functional element	Description
Root Certification Authority	The Root Certification Authority (CA) is the highest level CA in the certification hierarchy. It provides Enrolment Authority (EA) and Authorisation Authority (AA) with proof that it may issue enrolment credentials, respectively authorisation tickets.
Enrolment Authority	Security management entity responsible for the life cycle management of enrolment credentials. Authenticates an ITS-S and grants it access to ITS communications. An Enrolment Authority (EA) issues a proof of identity to ITS-S identifier by delivering an enrolment certificate and then the station requests its authorisation certificates from an Authorisation Authority (AA) using the received enrolment credentials. AA verifies ITS-S enrolment credentials with EA before responding with authorisation certificates (Ivanov et al., 2018).
Authorisation Authority	Security management entity responsible for issuing, monitoring the use of authorisation tickets. Provides an ITS-S with authoritative proof that it may use specific ITS services.
Distribution Centre (optional)	Provides to ITS-S the updated trust information necessary for performing the validation process to control that received information is coming from a legitimate and authorised ITS-S or a PKI certification authority by publishing the (Certificate Trust List) CTL and Certification Revocation List (CRL).
Sending ITS-S	• Acquires rights to access ITS communications from Enrolment Authority • Negotiates rights to invoke ITS services from Authorisation Authority • Sends single and relayed broadcast messages
Relaying ITS-S	• Receives broadcast message from the sending ITS-S • Forwards them to the receiving ITS-S if required
Manufacturer	Installs necessary information for security management in ITS-S at production
Operator	Installs and updates necessary information for security management in ITS-S during operation

- The destination port number: ensures that the message is routed to the appropriate processing element in the receiving ITS-S
- The associated authorisation certificate or an unambiguous reference to it: demonstrates to the receiving ITS-S that the sending ITS-S is authorised to invoke the sending of the received message type.

E INFORMATION FLOWS OF SPECIFIC SECURITY REQUIREMENTS

In this appendix specific information flow regarding the design of authorised parties and the process of authorisation in a ITS is described.

Enrolment credentials

Obtain enrolment credentials The Obtain Enrolment Credentials is used by an ITS-S to enrol with an enrolment authority.

Following functional entities:

- In the ITS-S
  - Invoke enrolment
  - Enrolment request
  - Process authentication
- In the ITS infrastructure
  - Enrol station
  - Authenticate station

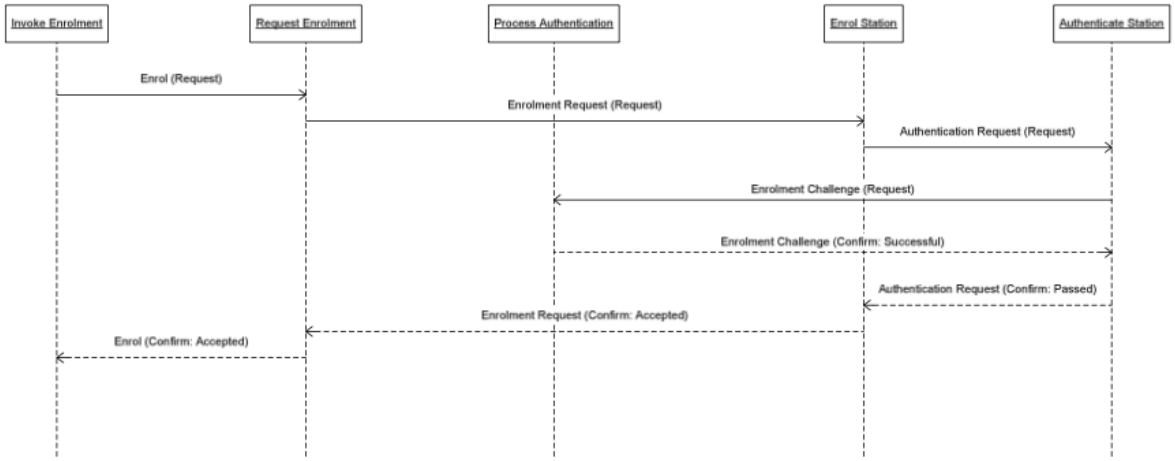

Figure E.1: Successful acquisition of enrolment credentials

Update enrolment credentials Upon request from an ITS-S the Update Enrolment Credentials security service is able to update its enrolment credentials.

Following functional entities:

- In the ITS-S
  - Update enrolment credentials
- In the ITS infrastructure
  - Request enrolment credentials
  - Issue enrolment credentials

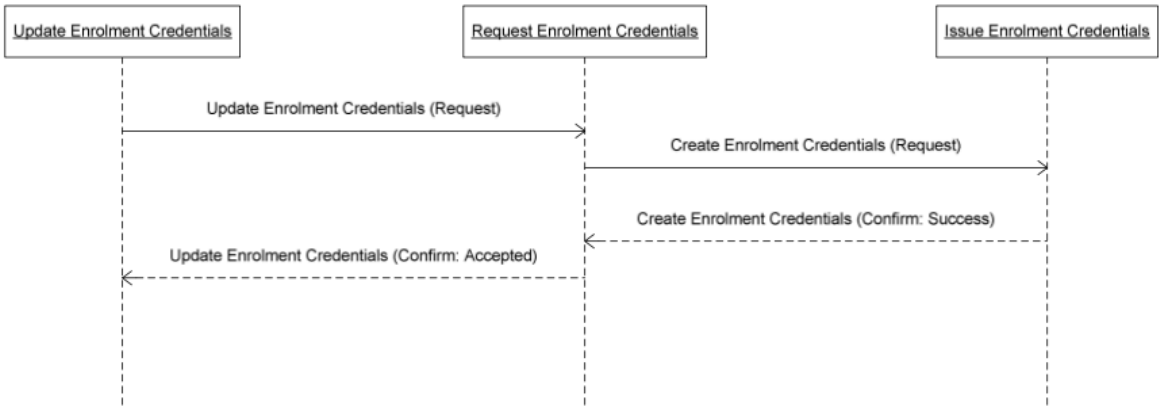

Figure E.2: Successful update of enrolment credentials

Remove enrolment credentials The Remove Enrolment Credentials security service provides the ITS network with the capability of removing the enrolment of a previously enrolled ITS-S thus nullifying any information currently in use by the ITS-S for communication with other ITS stations. For the removal to be effective, the enrolment authority and authorisation authority shall on a regular basis exchange enrolment credential and authorisation status information. It is particularly important for the enrolment authority to keep the authorisation authority updated at all times to ensure an accurate publishing of authorisation status updates.

Following functional entities:

- In the ITS-S
  - Remove enrolment credentials
- In the ITS infrastructure
  - Invoke enrolment credentials removal
  - Revoke enrolment credentials
  - Distribute enrolment revocation information

Authorisation tickets

Obtain authorisation tickets The Obtain authorisation Tickets service is used by an ITS-S to request and download authorisation tickets from one or more authorisation authorities.

Following functional entities:

- In the ITS-S

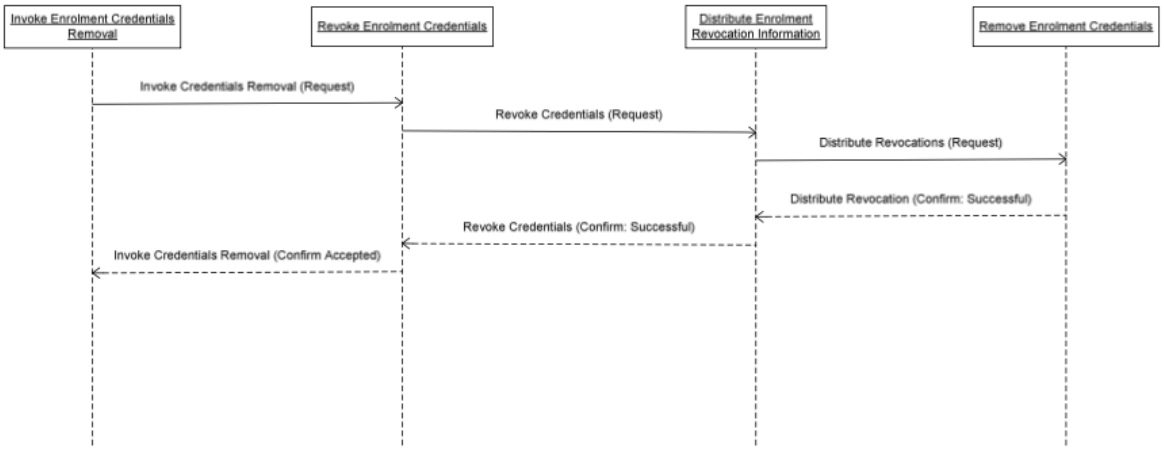

Figure E.3: Successful removal of enrolment credentials

  - ITS station agent
  - Station authorisation manager
- In the ITS infrastructure
  - A-ticket distributor
  - Enrolment credentials verifier

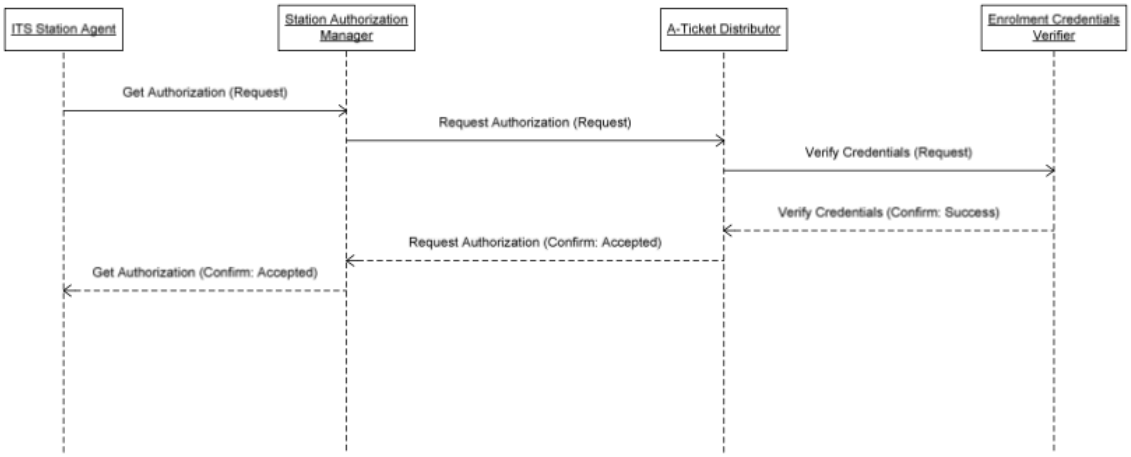

Figure E.4: Successful authorisation tickets request

Update authorisation tickets Authorisation tickets are restricted in number and time and shall be updated regularly. The update interval is ITS application dependent and not specified in this document. The Update Authorization Tickets security service handles all kinds of A-tickets update.

Following functional entities:

- In the ITS-S
  - ITS station agent
  - Station authorisation manager

- In the ITS infrastructure
  - A-ticket distributor
  - Enrolment credentials verifier

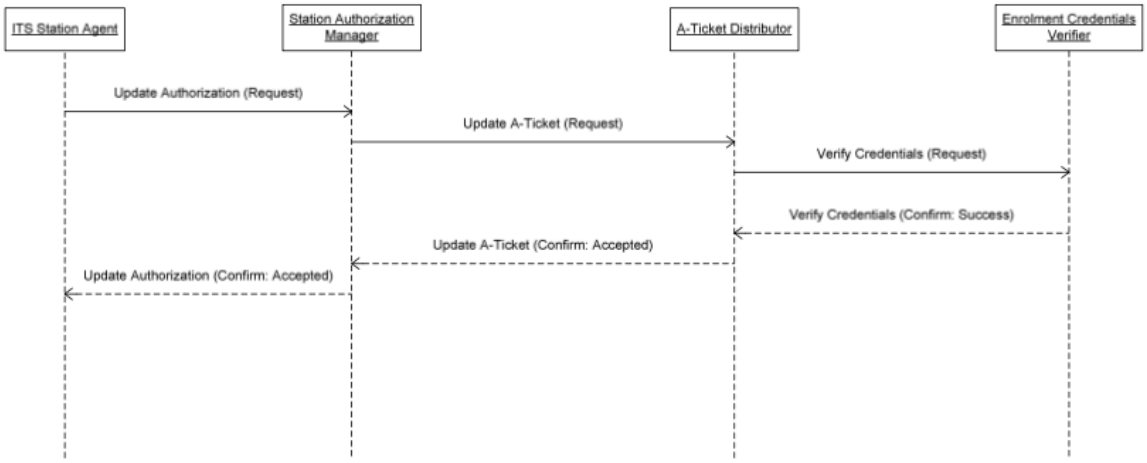

Figure E.5: Successful update of authorisation tickets

Publish authorisation status The Publish Authorisation Status security service sends authorisation status information from the ITS infrastructure either on request from an ITS-S or when determined by any authoritative entity in the ITS network to be necessary. Authorisation status is used to mark particular ITS-S as misbehaving or otherwise not trustworthy or accountable in terms of either temporary disabling authorisations or removing authorisations altogether for a particular ITS-S.

Following functional entities:

- In the ITS-S
  - ITS station agent
  - Station authorisation manager
- In the ITS infrastructure
  - ITS network agent
  - ITS authorisation status manager

Update local authorisation status repository Following functional entities:

- In the ITS-S
  - ITS station agent
  - Station authorisation manager
- In the ITS infrastructure
  - A-ticket distributor
  - Enrolment credentials verifier

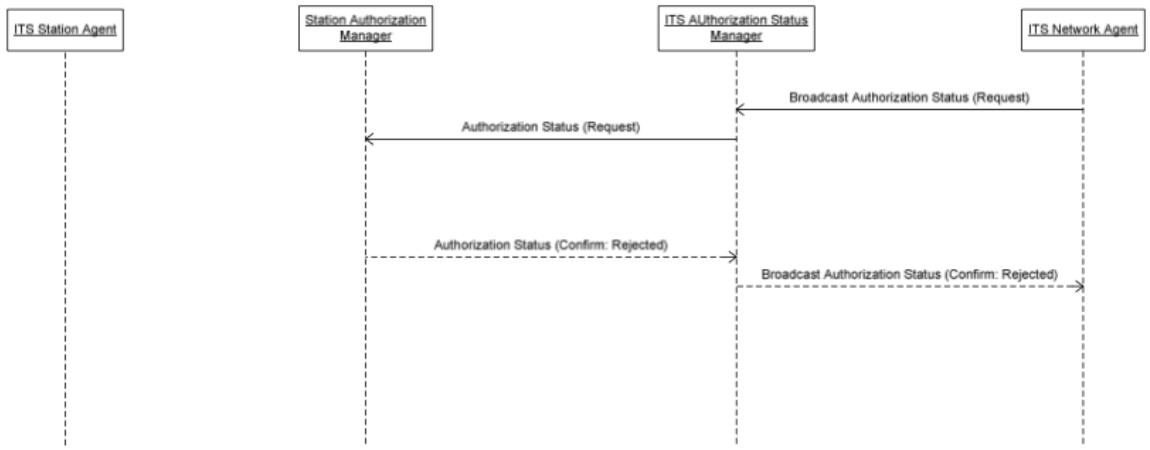

Figure E.6: Successful publication of authorisation status

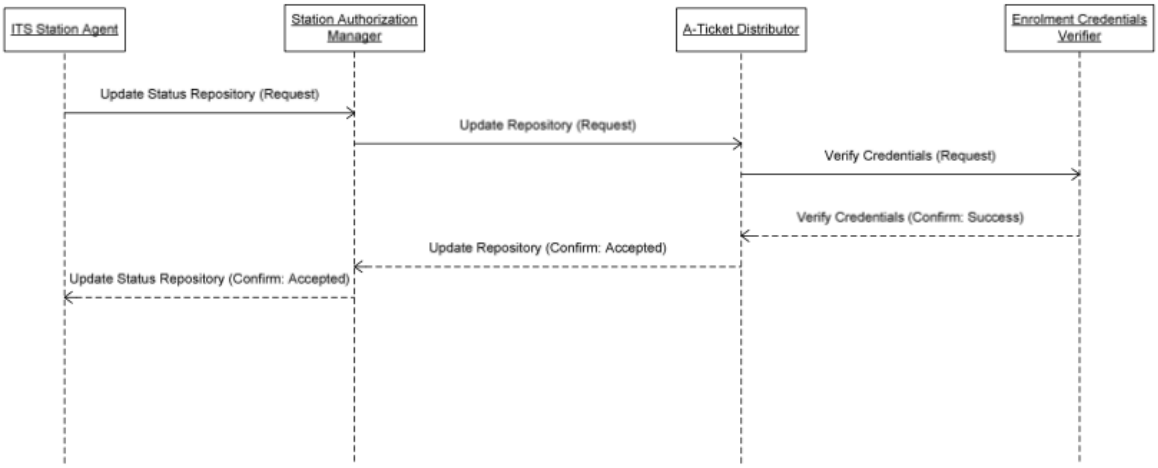

Figure E.7: Successful update of local authorisation status repository

Security Associations

Establish Security association Allows two ITS-Ss to establish a one-way SA so that one ITS-S may send securely to the other. In order to allow two ITS-Ss to establish a bi-directional secure communication this service shall be used twice.

Following functional entities:

- In the initiator
  - Security association initiator agent
  - Initiator security association management
- In the responder
  - Security association responder agent
  - responder's security association management

Update security association Allows two ITS-Ss that already share an SA to update any of the parameters of that SA. Same functional entities as above.

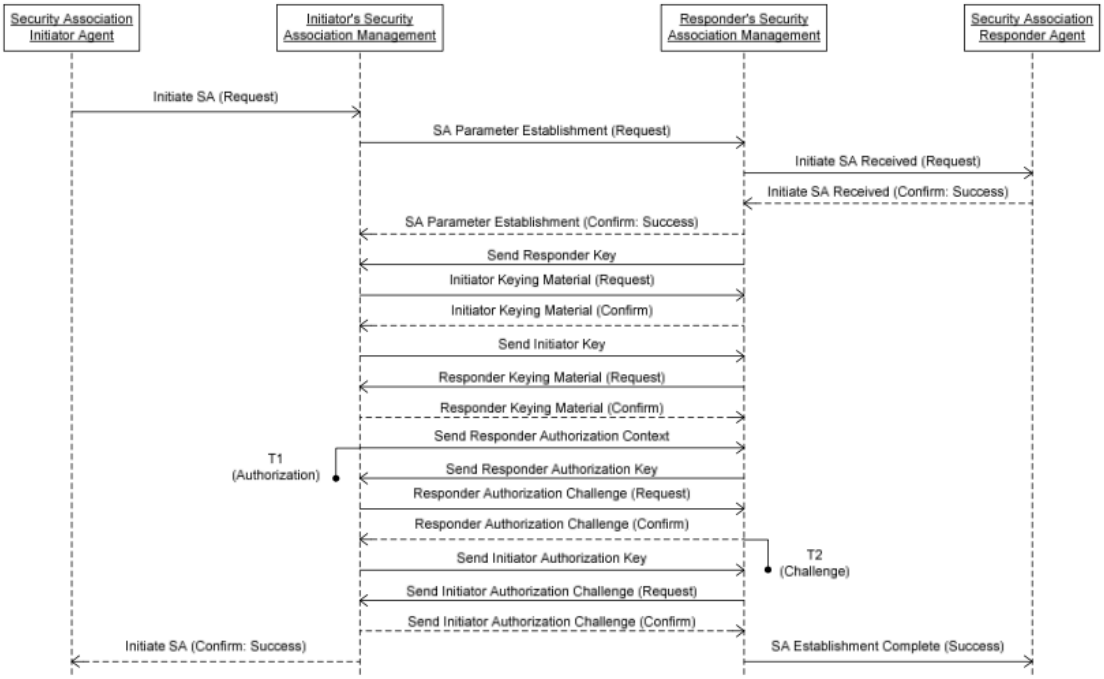

Figure E.8: Successful establishment of a Security association

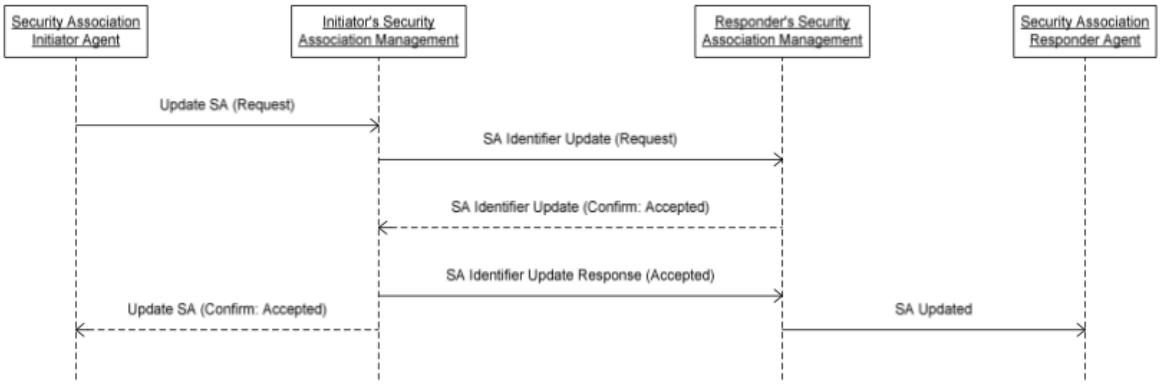

Figure E.9: Successful update of a Security Association identifier

Send secure message over SA Allows two ITS-Ss who have established an SA to send and receive a message securely using that SA.

The Send Secured Message security service encrypts and authenticates an ITS message before it is transmitted to its destination. This security service involves no exchange of information with entities outside the ITS-S.

Remove security association Allows two ITS-Ss to terminate an established SA.

Same functional entities as above.

Figure E.10: Successful removal of a security association

F IMPACT OF RISKS OF V2I

Threats	Safety	Privacy	Operational		Highest value
Threats regarding back-end servers					
Back-end servers used as a means to attack a vehicle or extract data	0	2	0		2
Services from back-end server being disrupted, affecting the operation of a vehicle	1	1	2		2
Data held on back-end servers being lost or compromised (data breach)	0	2	0		2
Threats to vehicles regarding their communication channels					
Spoofing of messages or data received by the vehicle	2	2	3		3
Communication channels used to conduct unauthorised manipulation, deletion or other amendements to vehicle held code/data	2	2	3		3
Communication channels permit untrusted / unreliable messages to be accepted or are vulnerable to session hijacking / replay attacks	1	2	3		3
Information can be readily disclosed (i.e. interception of information / eavesdropping)	1	2	1		2
Denial of service attacks via communication channels to disrupt vehicle functions	1	2	3		3
An unprivileged user is able to gain privileged access to vehicle systems	0	3	3		3
Messages received by the vehicle or transmitted within in, contain malicious content	2	0	3		2

Figure F.1: Rating of severity of potential attacks

G QUANTIFYING RISKS OF V2I PROJECTS

Note that in the third column, a change of the values from ETSI TS 102 893 given to one of the factors is being indicated with a asterisk (*) after that specific value.

UNECE	ETSI (threat group)	Values	Attack potential	Likelihood
Threats regarding back-end servers				
Back-end servers used a means to attack a vehicle or extract data	Modification and deletion of stored information (roadside)	Time: < 1 week (1) Expertise: proficient (2) Knowledge: sensitive (4) Opportunity: moderate (4) Equipment: specialised (4)	15	1
Services from back-end server being disrupted, affecting the operation of a vehicle	- DoS: Denial of access to incoming messages (roadside) - DoS: Denial of access to outgoing messages (selfy created roadside)	Time: < 1 day (0)* Expertise: expert (5) Knowledge: restricted (1)* Opportunity: easy (1) Equipment: specialised (4)	11	2
Data held on back-end servers being lost or compromised (data breach)	Acquisition of behavioral details (roadside)	Time: < 1 week (1) Expertise: proficient (2) Knowledge: sensitive (4)* Opportunity: moderate (4) Equipment: standard (0)	11	2
Threats to vehicles regarding their communication channels				
Spoofing of messages or data received by the vehicle	- Masquerade as an emergency vehicle - Masquerade	Time: < 1 week (1)* Expertise: expert (5) Knowledge: restricted (1) Opportunity: moderate (4) Equipment: standard (0)	11	2
Communication channels used to conduct unauthorised manipulation, deletion or other amendements to vehicle held code/data	Modification and deletion of transmitted information (vehicle)	Time: < 1 month (4)* Expertise: expert (5)* Knowledge: restricted (1) Opportunity: moderate (4) Equipment: specialised (4)	18	1
Communication channels permit untrusted / unreliable messages to be accepted or are vulnerable to session hijacking / replay attacks & Messages received by the vehicle or transmitted within in, contain malicious content	Modification and deletion of transmitted information (vehicle)	Time: < 1 week (1) Expertise: expert (5) Knowledge: restricted (1) Opportunity: moderate (4) Equipment: standard (0)*	11	2
Information can be readily disclosed (i.e. interception of information / eavesdropping)	Acquisition of behavioral details	Time: < 1 week (1)* Expertise: layman (0)* Knowledge: public (0)* Opportunity: easy (1) Equipment: standard (0)	2	3
Denial of service attacks via communication channels to disrupt vehicle functions	- DoS: Denial of access to incoming messages - DoS: Denial of access to outgoing messages	Time: < 1 day (0) Expertise: expert (5) Knowledge: restricted (1) Opportunity: moderate (4) Equipment: specialised (4)	14	2
An unprivileged user is able to gain privileged access to vehicle systems	Acquisition of personal information (vehicle)	Time: < 1 month (4)* Expertise: expert (5) Knowledge: sensitive (4) Opportunity: moderate (4) Equipment: specialised (4)	21	1

Figure G.1: Mapping from UNECE vulnerabilities to ETSI with corresponding values, attack potential and likelihood of attack / vulnerability

H INTERVIEW QUESTIONS GUIDELINE

Introduction

- Do you use methodology / guidelines and if so, for what subjects and what goal?

Assessing existing guidelines if suitable for usage

- How do you determine if you need a guideline / search for it?
  - When is it suitable from your perspective, which aspects do you look at?
- How do you convince a client that this framework is the one he needs, if this is relevant at all?

Assessing guideline if content wise suitable for usage

- What do you need from a consultant perspective regarding information? How much detail for instance?
- Do you combine existing frameworks in practice?

I INTERVIEW TRANSCRIPTIONS

Interview 1

Introduction

Question: Do you use methodology / guidelines and if so, for what subjects and what goal?
Answer: in the case of consultant 1 it is fairly straightforward in the sense that all used standards are for information security. Examples are the ISO and BIO (Baseline Informatiebeveiliging Overheid) which is an extension of the ISO standard for government organisations. For Northwave consultant 1 focused on quality assurance with ISO 9001.

Assessing existing guidelines if suitable for usage

Question: How do you determine if you need a guideline / search for it?
Answer: this depends on the knowledge of the organisation. Consultant 1 gives an example of an organisation which has no idea of how to set up an ISMS (Information Security Management System) or how to write a information security policy. In this case consultant 1 used the so called 'Fast track' methodology of Northwave itself, including several templates. The Fast track methodology focuses on the minimal requirements regarding certification of ISO 27001.

This way a consultant can quickly assess where the necessary focus points have to be laid because you can quickly show results, which consultant 1 indicates is one of the biggest advantages of the Fast track methodology from a consultancy point of view. This is also because information security is according to consultant 1 often being seen as not very important and costing unnecessary resources. In the image below, consultant 1 shows the differences between a standard ISO 27001 certification process and the Fast track of Northwave, starting with a risk analysis.

Question: When is a guideline suitable from your perspective, which aspects do you look at?
Answer: this depends on the maturity of the client. Some clients know more about information security, which can better indicate if they want to comply to a certain standard. Some clients do not have this level of knowledge and just want to do 'something with information security.' In this case Northwave advises them and in case of information security the default is ISO 27001. There are in principle no other choices than ISO 27001. What a client can do is focus on a specific aspect within the norm, e.g. business continuity or privacy, of which you can in turn get other norms or laws to comply with.

Question: How do you convince a client that this framework is the one he needs, if this is relevant at all?
Answer: consultant 1 states that you have to match the guideline to the wishes of the client. If a client wants to certify itself for ISO, the ISO 27001 is used, so this is clear. Even if a client indicates it wants its information to be secure and adequately stored / processed, the ISO 27001

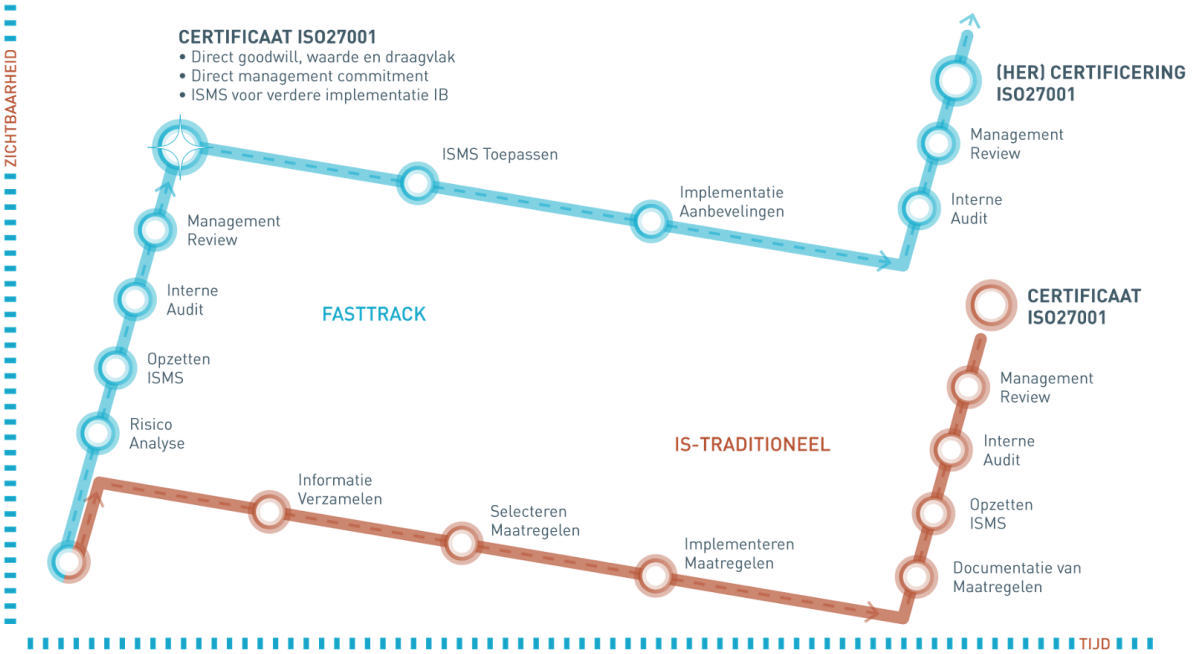

Figure I.1: Northwave Fast track methodology

is used. Consultant 1 indicates that without the usage of ISO 27001 information security will be 'difficult' because you will reinvent the wheel unnecessary and project your own thoughts on a client instead of a proven standard.

Assessing guideline if content wise suitable for usage

Question: What do you need from a consultant perspective regarding information? How much detail for instance?
Answer: when focusing on specific aspects within the ISO 27001 and using other standards within this standard, the preference is to have as much detail as possible. This is also a wish of the client: do they just want a quick look at the specific subject, or do they want to dive deep into the subject? Consultant 1 indicates that this differs per situation and there is no fixed answer to this question as the level of detail is also a wish of the client. Northwave can, however, advise the client which level of detail is needed, but again, this differs per situation.

Consultant 1 explains that Northwave does an intake with a so called '0 measurement' to gather information about the client and what are, consequently, the wishes of the client what to improve upon? Another perspective is risk-based: where can the client improve, what will be the focus area of Northwave? Lastly, the management can also indicate a higher wish which Northwave can use as a starting point.

For implementation of specific aspects of ISO 27001 the 'Fast track' methodology of Northwave itself is used by consultant 1. In this Fast track method, the first step is a risk analysis, as can be seen in Figure I.1.

If a client wants to focus on e.g. business continuity management within the ISO 27001 standard, consultant 1 would use another ISO standard specifically for that. ISO 27002, where advice of how to implement control measures of annex A of ISO 27001 is given, is also preferred by consultant 1. Consultant 1 indicates how she prefers clear definitions of how to implement specific aspects, also for the translation to the client. However, every client is different, and the ISO 27002 does leave space for interpretation of every specific client, without being prescrip-

tive, which is preferred by consultant 1.

Question: Do you combine existing frameworks in practice?
Answer: yes, for instance a standard by the NCSC (National Cyber Security Center of the Netherlands) and another best practices document was combined in order to create a list of security requirements for applications. However, this was not done with the goal of making a new guideline of best practices document for further documentation.

Interview 2

Introduction

Question: Do you use methodology / guidelines and if so, for what subjects and what goal?
Answer: Consultant 2 states that the experience with standards are mainly ISO standards (i.e. ISO 27001 and ISO 27002), with the subjects all mainly related to information security, risk management and how to set up and manage and management system. In addition to that, you have best practices guidelines being supplied by the branch itself (e.g. information security) which in practice are being seen as the best way of working.

Assessing existing guidelines if suitable for usage

Question: How do you determine if you need a guideline / search for it?
Answer: this differs per subject which guideline is used and from which organisations. For instance if you look at guidelines for strong passwords, you have multiple options ranging from 12 characters and 1 capital letter to the most characters to not using passwords at all.

Question: When is a guideline suitable from your perspective, which aspects do you look at?
Answer: which guideline you pick depends on the client. If the client only has 4 employees and a IT budget of 1000 euros, consultant 2 argues that this knowledge influences which guidelines he uses to implement strong passwords and how this can be maintained, i.e. not using passwords at all would need many arrangements in place and is therefore not suitable, while the second option of as much characters as possible is safer and easier to maintain.

Another example is with determining risks of a client. Northwave often uses RAVIB (a Dutch risk analyses framework) to determine threats. However, is a client does not recognise any of the threats for his or her company, another list with threats can be used in this fits the client better.

Question: How do you convince a client that this framework is the one he needs, if this is relevant at all?
Answer: this depends on the associated risk. If there is no risk, no measures are necessary. If you first hold a risk analysis, then determine which measures are necessary to implement. This depends on the clientele in general: if all clients have different risks, a risk analysis is the best staring point. However, if the clientele is exposed to the same risks, a general risk assessment can be suitable. A risk assessment is furthermore very suitable for obtaining a picture for the client what the scope would be when implementing measures and which risks they are exposed to. Consultant 2 adds the metaphor of a fire: the fire brigade assesses when arriving at a scene where the fire is most violently and where it can be reached to stop, before it actually starts extinguishing the fire at that point.

Consultant 2 adds that a client is coming to Northwave with a question or a problem. The client hires Northwave to solve this question / problem and if Northwave indicates which standards or guideline they use in order to do this, then the client is overall already very happy. Most, if not all, used standards are accepted and verified around the world. If you receive the question why you use a certain standard from the client, who is Northwave to change to another, less accepted standard? In all cases the standard /frameworks serves as a starting point. If the client doubts this standard / framework: at least it is better than now because often the client has nothing in place.

Assessing guideline if content wise suitable for usage

Question: What do you need from a consultant perspective regarding information? How much detail for instance?
Answer: Consultant 2 mentions that all the standards / best practice documents he uses are used as a directive. For clients consultant 2 says situations are not always 0 or 1, or black or white, which makes the exact text of a standard or guideline less important. The exception is for when an ISO certification project is being started for which hard requirements have to be met.

Here it is also important to know the client. The baseline for this is how a client earns his money. If you know this and which processes, systems and applications are necessary to earn money. This way a high level standard like ISO 27001 can be applied much easier and what this means for an organisation. An example is when a requirement states 'you should backup everything' but applications in the cloud are used and in the contract of the cloud supplier it is stated how data is being backup-ed, this requirement mainly turns into contract management and making sure the agreements are being fulfilled.

Consultant 2 also gives an example of how a best practice guide about business continuity mentions how a client can structurally work on this subject, when also giving examples of how to do this. Especially the aspect of giving examples of how a company in a specific situation should be doing this and this is being seen useful by consultant 2 because you can see more clearly the thinking behind the documentation by this situation outline. On the other hand, consultant 2 mentions how this giving of examples of how requirements can be fulfilled, can lead to tunnelling / narrowing of the scope: you are being restricted in your possibilities because you are only looking at one specific situation. Consultant 2 sees the aspect of giving examples / outlying situations as one of the most differentiation factors between standards/ frameworks and guidelines / best practice guides: standards / frameworks are certain fixed frames within you can operate and how you fulfil this is up to the client, while guidelines / best practice guides outline a certain amount of steps which have to be followed in order to achieve something but that is positive since you followed these steps in the first place.

Consultant 2 adds that a guideline can also be used to obtain a certain baseline / minimum requirements after you have done the first risk assessment, after which you start tackling the baseline first before implementing all measures of i.e. the ISO standard. The Fast track method of Northwave works this way by focusing first on the most important aspects to obtain certification, before implementing all measures mentioned in ISO 27002. The first target is however, to being able to structurally and efficiently tackle all the issues (i.e. create an ISMS). This does not mean that you are secure though but the client is now able to solve this more easily than before.

Question: Do you combine existing frameworks in practice?
Answer: yes. This is both by taking aspects from existing guidelines and just using them for one client and also creating new documentation. In the first case a certain client in grid manage-

ment for electricity uses very specific equipment where a normal vulnerability scan would cause disruptions. However, if a standard prescribes that a vulnerability scan has to be executed, another (sector specific) framework is being used to implement vulnerability management for this specific environment.

Regarding creating new documentation is the State of Security scan of Northwave. This scan uses multiple aspects from standards and frameworks (i.e. ISO 27001 focusing on management side, the CIS (Critical Security Controls) controls for more technical aspects and certain laws to comply to privacy / GDPR) in order to fully asses the security of an organisation.

Interview 3

Introduction

Question: Do you use methodology / guidelines and if so, for what subjects and what goal?
Answer: yes, on a continuous base. Most activities involve the usage of best practices or standards. Examples are the ISO 27001 standard, along with assessment frameworks which are based on standards like COBIT (Control Objectives for Information and Related Technology), cloud control frameworks, along with other frameworks / standards as long if they have a relationship with information security. Furthermore a deduction of existing standards is being used for the State of Security assessment of Northwave where consultant 3 also has experience with.

Assessing existing guidelines if suitable for usage

Question: How do you determine if you need a guideline / search for it?
Answer: consultant 3 states that the requirements from a client in combination with a specific subject you can quickly find specific frameworks. Then consultant 3 looks at the publisher if this is renowned / broadly accepted and if the framework is usable for this specific client / situation. Regarding information security there are many frameworks / standards but the most accepted ones are scarce and often lead to the same standards regarding management, technical side (i.e. SIS (Security Infrastructure Solutions)) or threats (OWASP Top 10).

Question: When is a guideline suitable from your perspective, which aspects do you look at?
Answer not specifically asked, can be subtracted from answer below.

Question: How do you convince a client that this framework is the one he needs, if this is relevant at all?
Answer: how standards are used depends on how big clients are and what they encompass. Some clients tend to have formal documentation in the backend and display a simple version to clients, while others implement everything very formal and bureaucratic. Northwave tries to convince the client to be as pragmatic as possible by focusing on the minimum baseline to be complied to while extensions are possible later on in the trajectory. The speed of what a client can handle is also important in how fast you can implement measures or set up a management system. A start up for instance is less formal than a bank or insurance companies which are more bureaucratic and therefore require a different approach in using standards. Adapting to a company is here, again, a key aspect.

Consultant 3 adds that before the start of a project the to be used documentation is already agreed upon. However, how the specific documentation is being implemented is something you have to discuss with management.

Assessing guideline if content wise suitable for usage

Question: What do you need from a consultant perspective regarding information? How much detail for instance?
Answer: when using the ISO 27001 for instance, Northwave has a template where it is outlined how a certification / high level structure of a client can be achieved. However, when looking at operational measures (i.e. Annex A of ISO 27001) then consultant 3 indicates Northwave does not use specific templates because this is too specific to apply for every client and having the danger you end up with something not fitting for the organisation.

Consultant 3 adds how management systems are very much prescriptive in what you have to do and which elements a client should have. Because this is on a strategic level often the interpretation follows clearly. However, on an operational level, you have to work with people and let the initiative of implementing measures rest with them. This relates closely to ownership: let the client themselves set up the measures before Northwave steps in and gives specific advice.

Northwave uses their own templates for standards (i.e. ISO, Cobit, GDPR) that are often used in order to be more operational. These templates are a translation from the standard itself to a more operational set of documentation: the template reduces, summarises and structures the content of the standard to a more cyclic way of working while also emphasising the parts of standards which are related to each other. An example is how to handle incident management and strategic reporting, aspects which get more clear in a template than just the text of a standard.

Question: Do you combine existing frameworks in practice?
Answer: yes, especially combining standards / frameworks in order to create new documentation for different clients. The best example of this is the State of Security where, as mentioned, different frameworks / standards are combined in order to analyse a client from 360 degrees perspective. Another example is an internal audit framework with different aspects like security control, procedures for technical implementations to cloud frameworks controls. Here the best aspects per framework were taken and combined.

Interview 4

Introduction

Question: Do you use methodology / guidelines and if so, for what subjects and what goal?
Answer: Consultant 4 says that all the documentation in her past 5 years of experience is about information security. Examples of frameworks are COBIT, ISO, ISF, etc. On the other hand there are standards / guidelines which are published from research organisations, e.g. NIST (National Institute of Standards and Technology) or SANS Institute which are more market focused guidelines / best practices.

Assessing existing guidelines if suitable for usage

Question: How do you determine if you need a guideline / search for it?
Answer not specifically asked, can be subtracted from answer of the question below.

Question: When is a guideline suitable from your perspective, which aspects do you look at?
Answer: often this becomes clear from which community or organisations the documentation is published. There are a few renowned names of which consultant 4 knows that the quality is good enough, e.g. SANS or NIST.

Also relating to the client consultants can look at which suppliers are present in a specific domain, i.e. Microsoft or Amazon, and which documentation they publish regarding best practices. Consultant 4 states that the publisher is very often a good first filter regarding documentation and if this is suitable for their usage.

Question: How do you convince a client that this framework is the one he needs, if this is relevant at all?
Answer: management has to be involved in the choices that are made. If certain guidelines of best practices are used with a certain execution, it is important to explain why you chose for this and this should fit with the vision, mission and strategy of the organisation, which can also be challenged by the management of an organisation.

Assessing guideline if content wise suitable for usage

Question: What do you need from a consultant perspective regarding information? How much detail for instance?

A standard is more high level and directional according to Consultant 4, while the implementation of this standard is always organisational specific. Therefore a standard is more of a directive (instead of prescriptive), while consultants will look later on per subject what an organisation looks like, what questions do they have, how their IT looks like, which people and processes are there, etc. Then consultant 4 looks at more specific guidelines which you can use per situation and subject. When you have an organisation focusing on Microsoft, a standard would require user access. Therefore you would look for specific guidelines targeting Microsoft environments and user access to implement this.

Consultant 4 adds that having the broad outline ('coat rack') is always useful to have and that this can be also useful to have specific documentation for some situations / subjects. However, this specific documentation is according to consultant 4 difficult to use if you cannot place this documentation within the grander scheme (i.e. the used standard / framework).

Consultant 4 adds that the goal of a framework / standard is important to emphasise. Do you want to operate a whole branch / industry or do you want to focus on specific subjects? ISO is for instance for every organisation and can therefore not be specific.

Regarding templates of Northwave consultant 4 mentions that they offer a certain direction. When having a certain end goal and you know the fixed steps in order to achieve that in whichever organisation you are, a template guiding you through this process and achieving a minimum level of security is very useful according to consultant 4.

The balance between the application of the template and the end goal is seen here as the biggest benefit, together with the translation of theory (standard) to practice (template). A template is eventually broad enough that no aspects of the standard are missed but is it not a definitive set of truth and adjusting is sometimes needed. A template is a good starting point to implement a standard but not prescriptive. Afterwards consultant 4 looks at what is still possible and what could be implemented. A template is therefore a win and not really a necessity.

Question: Do you combine existing frameworks in practice?
Answer: Yes, for many clients involved in an ISO certification project there is documentation of specific aspects, like password management, secure development policy, etc. For every client dealing with those aspect, Northwave looks if they document this process so that this obtained knowledge can be applied to other organisations.

J CODING OF INTERVIEWS

Phase of assessing guideline if suitable for usage

Table J.1: Phase of assessing guideline if suitable for usage

Aspect	**Times mentioned**
Knowledge of client	12
Requirements regarding client	3
Maturity of client	2
Size of client	2
Risk based analysis for client	2

Table J.2: Phase of assessing guideline if content wise suitable for usage

Aspect	**Times mentioned**
Detailed information because of wish client	3
Risks as base to determine framework	1
Documentation is directive, not prescriptive	7

K VERIFICATION OF CASE STUDY

If no options below a questions are stated, the question is open.

The following questions were asked to the respondents, in several categories:

1. **Background information**
   - 1.1. What is your current function within Concorda?
   - 1.2. How many years of experience do you have with IT security?
   - 1.3. How many years of experience do you have with V2I projects?
   - 1.4. Could you describe your involvement with the specific project of Concorda?
   - 1.5. Could you describe the current processes regarding security and projects within Concorda? Where do you think strengths are, and where improvements could be made, if any?
2. **Overview of vulnerabilities and risks**
   - 2.1. Have security risks been documented when designing / implementing current projects within Concorda?
     - Yes / No
     - 2.1.1. If yes, could you describe how?
     - 2.1.2. If not, would it, considering the presented overview of vulnerabilities and risks of V2I projects, be valuable?
   - 2.2. The presented vulnerabilities in Table 1 are relevant regarding current and future projects within Concorda:
     - Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree
   - 2.3. The presented attack levels in Table 1 are relevant regarding current and future projects within Concorda:
     - Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree
   - 2.4. The presented impact levels in Table 1 are relevant regarding current and future projects within Concorda:
     - Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree
   - 2.5. The shown priority of the risks are relevant to current and future projects within Concorda:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

2.6. Do you agree with the presented vulnerabilities regarding current and future projects within Concorda? If not, why?

2.7. Do you agree with the vulnerabilities as a starting point of the framework? If not, why?

3. **Overview of attack methods**

3.1. Have attack methods been documented regarding current projects within Concorda?

- Yes / No

3.1.1. If yes, could you describe how?

3.1.2. If not, would it, considering the presented overview of attack methods on V2I projects, be valuable?

3.2. Each attack method is made to clear by the accompanying description:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

3.3. The mapping between vulnerabilities and attack methods are relevant for current and future projects within Concorda:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

3.4. Do you agree with the presented attack methods in this framework? If not, why?

4. **Presented overview of measures**

4.1. Have security measures been documented when designing / implementing current projects within Concorda?

- Yes / No

4.1.1. If yes, could you describe how?

4.1.2. If not, would it, considering the presented overview of security measures, be valuable?

4.2. The presented overview in Table 2 of security measures regarding current and future projects within Concorda are relevant:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

4.3. Each security measure is clearly described:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

4.4. The mapping between vulnerabilities (Table 1), attack methods and corresponding security measures regarding current and future projects within Concorda is clear:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

4.5. Do you agree with the mapping of attack methods to security measures? If not, why?

5. **Overview of security requirements**

5.1. Have security requirements been documented when designing / implementing current projects of Concorda?

- Yes / No

5.1.1. If yes, could you describe how?

5.1.2. If not, would it, considering the the presented overview of security requirements, be valuable?

5.2. The presented overview of security requirements in Table 1 is relevant regarding current and future projects within Concorda:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

5.3. The presented overview of security requirements in Table 2 is relevant regarding current and future projects within Concorda:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

5.4. The mapping between vulnerabilities and security requirements in Table 1 is clear:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

5.5. The mapping between measures and security requirements in Table 2 is clear:

- Strongly disagree / disagree / do not disagree, but also not agree / agree / strongly agree

5.6. Do you agree with the mapping of vulnerabilities to security measures? If not, why?

5.7. Do you agree with the mapping of attack methods to security measures? If not, why?

5.8. Do you agree with the inclusion of security requirements into this framework? If not, why?

6. **Usefulness of framework**

6.1. A comprehensive overview regarding cybersecurity when working with current and future projects in Concorda would be useful in my day to day work:

- Yes, this would help in managing the project more adequately
- No, not at the moment, but this could change in the future when V2I is more mature
- No, not at all, we leave cybersecurity to other vendors
- None of the above, leave comment here:

6.2. Having observed the proposed framework regarding security at V2I projects, would it have had a positive impact on current or future V2I projects?

- Yes, both with current and future projects
- Yes, but only at future projects
- Yes, but only with current projects

- No, at none of the projects
- None of the above, leave comment here:

6.3. Would you consider incorporating a security framework similar as proposed here in V2I projects?

- Yes, both with current and future projects
- Yes, but only at future projects
- Yes, but only with current projects
- No, at none of the projects
- Other, namely...

6.4. In your opinion, how relevant is the proposed framework as a whole regarding security in V2I projects?

L VALUATION OF FRAMEWORK

In the table below the results of the main aspects of the framework are presented. Here only the closed questions where the participants were asked to judge a certain aspect of the framework are included. As explained in section 2.3, this is done by using the following scale:

- Strongly disagree
- Disagree
- Do not disagree, but also not agree
- Agree
- Strongly agree

Every number represents the corresponding participant, i.e. [1] is participant number 2, [2] participant number 2, etc.

Table L.1: Valuation of Main Aspects of Framework in Case Study

Aspect of Framework	**Strongly dis-agree**	**Disagree**	**Do not dis-agree, but also not agree**	**Agree**	**Strongly Agree**
Vulnerabilities and Risks					
Vulnerabilities relevance			[1]	[2] [3]	
Attack levels relevance			[1]	[2] [3]	
Impact level relevance			[1] [2]	[3]	
Priority of Risks relevance			[1] [2]	[3]	
Attack methods					
Attack Method clear			[1]	[2] [3]	
Relevance of mapping between Vulnerabilities and Attack methods			[1]	[2] [3]	
Measures					
Security Measures relevance			[1]	[2]	[3]
Security Measure clear			[1]	[2] [3]	
Mapping between Vulnerabilities, Attack Methods and Measures is clear			[1] [2]	[3]	
Security Requirements					
Security Requirements relevance Table 1			[1]	[2] [3]	
Security Requirements relevance Table 2			[1]	[2] [3]	
Mapping between Vulnerabilities and Requirements in Table 1 is clear			[1] [2] [3]		
Mapping between Vulnerabilities and Requirements in Table 2 is clear			[1] [2] [3]		