

**ACADEMY OF INFORMATION TECHNOLOGY  
HALMSTAD UNIVERSITY**

# **Challenges Within V2X: A cybersecurity risk assessment for V2X use cases**

**Adrian Brorsson**



Bachelor thesis in Information Security

Supervisors: Cristofer Englund & Malin Wagnborg

Examiner: Urban Bilstrup

October 20, 2022

# **Challenges Within V2X: A cybersecurity risk assessment for V2X use cases**

**Adrian Brorsson**

Bachelor thesis in Information Security

# Abstract

Vehicle-to-Everything (V2X) is referred to as the technology enabling communication and data exchange between vehicles and is considered a significant milestone within automotive. By enabling inter-vehicle communication, the vehicles will be more aware of their surroundings—including things outside their current line-of-sight (LOS). The vehicles utilizing this technology are in Europe referred to as Cooperative Intelligent Transport Systems (C-ITS). A single vehicle is referred to as an ITS station (ITS-S). These are the terms presented in the European V2X standard called the ETSI ITS. This thesis considered the ETSI ITS standard since it is one of the most mature within the V2X standardization flora. This thesis investigated some significant V2X use cases and conducted a risk assessment on a selection of these use cases. These significant use cases were discovered by performing semi-structured interviews with five candidates within the field. The conducted risk assessment was performed according to a method called Threat, Vulnerability, and Risk Assessment (TVRA), which ETSI has developed. The results of this thesis work became a set of safety-functional use cases that were considered significant. The cybersecurity risk varied and spanned from critical to minor risk concerning the attacks taken into account. Since security and hardening are critical aspects of automotive connectivity, this thesis provides some future research directions at the end of this thesis. One of these topics is, for example, the privacy perspective on V2X, which was not considered in this thesis.

**Index terms:** automotive cybersecurity, V2X cybersecurity, V2X use cases, ETSI ITS, ETSI TVRA, V2X risk assessment

# Acknowledgements

For this section, I would like to thank everyone who made this thesis possible; To the project commissioner Knowit Secure and the project supervisors & organizers who gave me the opportunity to participate in their educational activities.

To my supervisor at Knowit Secure, Malin Wagnborg, for providing me with valuable information, encouraging me in the thesis work, and guiding me in the right direction.

To my supervisor at Halmstad University, Cristofer Englund, for providing me with valuable resources and his expertise.

To my course instructors for providing me with good feedback on the opposition occasion which made me complete this thesis the best way possible.

To the interview participants for taking their time and providing me with their knowledge and experience, significantly helping me better understand the area of choice.

Lastly, I would like to thank Anna, mamma och pappa!

*Adrian Brorsson*

Halmstad, 2022

*“It will impact safety a lot considering the use cases,  
and on the other hand the connectivity may be very easy to hack,  
so I think cybersecurity is absolutely the most important aspect of V2X”*

Interview participant

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Background V2X . . . . .	1
1.1.1	V2X definition . . . . .	3
1.1.2	Entities utilizing V2X . . . . .	4
1.1.3	V2X communication types . . . . .	5
1.1.4	V2X standards and protocols . . . . .	5
1.1.4.1	Primary standardizations, Standards Developing Organizations (SDOs), and other V2X stakeholders . . . . .	5
1.1.4.2	Radio access technologies . . . . .	6
1.1.4.3	Current debate about standards . . . . .	7
1.1.5	V2X use cases . . . . .	8
1.2	Problem statement . . . . .	9
1.3	V2X and automotive cybersecurity . . . . .	9
1.3.1	Cybersecurity attributes . . . . .	10
1.3.1.1	CIA Triad . . . . .	10
1.3.1.2	Accountability . . . . .	10
1.3.1.3	Authenticity . . . . .	10
1.3.2	Cybersecurity research within V2X and automotive . . . . .	10
1.3.2.1	Cybersecurity challenges in vehicular communications (2019) . . . . .	11
1.3.2.2	Attacks and defences on intelligent connected vehicles: A survey (2020) . . . . .	12
1.3.2.3	Securing Vehicle-to-Everything (V2X) communication platforms (2020) . . . . .	13
1.3.2.4	Security issues and challenges in V2X: A survey (2019) . . . . .	14
1.3.2.5	Security of 5G-V2X: Technologies, standardization and research directions (2020) . . . . .	15
1.3.2.6	5G-based V2V broadcast communications: A security perspective (2021) . . . . .	16
1.3.2.7	Functional safety for enabling present and future V2X use-cases (2021) . . . . .	16
1.3.2.8	V2X Attack Vectors and Risk Analysis for Automated Cooperative Driving (2021) . . . . .	17
1.3.2.9	ETSI security documents (2010, 12, 17, 21) . . . . .	17
1.4	Positioning of this thesis . . . . .	19
1.5	Purpose of this thesis . . . . .	20
1.5.1	Research questions . . . . .	21
1.5.2	Problematization of the research questions . . . . .	21
1.5.3	Delimitations . . . . .	21

<b>2 Methodology</b>	<b>23</b>
2.1 Selection of candidates . . . . .	23
2.1.1 Ethical stance . . . . .	24
2.2 Literature review . . . . .	24
2.3 Semi-structured interviews . . . . .	24
2.3.1 Procedure . . . . .	24
2.4 Data analysis . . . . .	26
2.5 Risk assessment model . . . . .	27
<b>3 Theory</b>	<b>30</b>
3.1 ITS reference model . . . . .	30
3.1.1 Applications and use cases layer . . . . .	31
3.1.2 Facility services layer and ITS messages . . . . .	32
3.1.3 Network and Transport layer . . . . .	33
3.1.4 Radio Access layer . . . . .	33
3.1.5 Management- and Security plane . . . . .	35
3.2 ITS Security Architecture . . . . .	35
<b>4 Result &amp; Analysis</b>	<b>42</b>
4.1 What are some significant use cases of V2X short-range? . . . . .	42
4.1.1 The motive behind the candidates' choices . . . . .	44
4.1.1.1 Day one use cases . . . . .	44
4.1.1.2 Day two use cases . . . . .	48
4.1.1.3 Day three use cases . . . . .	52
4.1.2 What cybersecurity risks can be associated with these use cases? . . . . .	56
4.2.1 Target of Evaluation (ToE) . . . . .	56
4.2.1.1 ToE Definition . . . . .	57
4.2.1.2 ToE Characteristics . . . . .	57
4.2.1.3 Assumptions on the ToE system . . . . .	59
4.2.1.4 Assumptions on the ToE Environment . . . . .	60
4.2.2 Security objectives . . . . .	60
4.2.3 Functional Security Requirements . . . . .	62
4.2.4 Use cases assets and impact rating . . . . .	62
4.2.4.1 ITS applications . . . . .	63
4.2.4.2 Service control . . . . .	64
4.2.4.3 Protocol control . . . . .	64
4.2.4.4 The 5.9 GHz frequency band . . . . .	64
4.2.4.5 Asset impact rating . . . . .	64
4.2.5 Identification of vulnerabilities, attacks, and threat level . . . . .	65
4.2.5.1 Vulnerabilities . . . . .	65
4.2.5.2 Attacks . . . . .	65
4.2.5.3 Threat level . . . . .	67
4.2.6 Quantifying attack potential, vulnerability likelihood and impact . . . . .	68
4.2.6.1 Disturbance of the communications . . . . .	68
4.2.6.2 Message manipulation . . . . .	70
4.2.6.3 Replay attack . . . . .	71
4.2.6.4 Likelihood of attacks . . . . .	72
4.2.6.5 Impact by attacks . . . . .	72
4.2.7 Risk evaluation . . . . .	72

<b>5 Discussion</b>	<b>74</b>
5.1 What are some significant use cases of V2X short-range? . . . . .	74
5.2 What cybersecurity risks can be associated with these use cases? . . . . .	75
5.3 Limitations of the study . . . . .	78
5.3.1 Interviews . . . . .	78
5.3.1.1 An issue with replicating the study . . . . .	79
5.3.2 Data analysis . . . . .	80
5.3.3 Risk assessment model . . . . .	80
5.4 Future work . . . . .	80
<b>6 Conclusion</b>	<b>83</b>
<b>A Interview questionnaire material</b>	<b>89</b>
A.1 Interview slides . . . . .	89
A.2 Consent letter . . . . .	92
<b>B Interview transcripts (Trx)</b>	<b>93</b>
B.1 Interview Candidate 1 (IC1) Interview Transcript . . . . .	93
B.2 Interview Candidate 2 (IC2) Interview Transcript . . . . .	96
B.3 Interview Candidate 3 (IC3) Interview Transcript . . . . .	99
B.4 Interview Candidate 4 (IC4) Interview Transcript . . . . .	105
B.5 Interview Candidate 5 (IC5) Interview Transcript . . . . .	116

# List of Figures

1.1	Relationship between V2X stakeholders (illustration replicated from [1]). . . . .	3
1.2	AutoVSCC framework . . . . .	11
1.3	The scope of this thesis considering the AutoVSCC framework. . . . .	20
2.1	Coding frame for the TA. . . . .	27
3.1	Illustration of the ETSI ITS communication stack. . . . .	30
3.2	Illustrations of the three main V2X deployment phases and the automated driving functions stages mapped together. . . . .	32
3.3	Illustration of the ITS frequency band and its respective sub-bands and channels as defined in ETSI ITS documentation [2]. . . . .	33
3.4	Difference between 802.11 and 802.11p. . . . .	34
3.5	Security Entities . . . . .	36
3.6	Illustration showing where different security services operate within the ITS reference model. . . . .	41
4.1	Chart of use case occurrences according to the interview candidates' selections. The table is color-coded. Red: use cases within day-phase 3; Green: use cases within day-phase 2; Blue: use cases within day-phase 1. . . . .	43
4.2	Illustration on the ToE. . . . .	59
4.3	The simplified version of Figure 3.6 shows a typical data flow through the ITS protocol stack for a particular use case. . . . .	63
4.4	The version of Figure 4.2 and 3.6 combined in one illustration showing potential attack surfaces. . . . .	66
A.1	Slide 1 . . . . .	89
A.2	Slide 3 . . . . .	90
A.3	Slide 4 . . . . .	90
A.4	Slide 5 . . . . .	91

# List of Tables

1.1	The two direct short-range communication modes and their options/enhancements.	6
1.2	The relation between the ETSI TVRA and the three-stage approach. . . . .	18
2.1	Interview candidates information . . . . .	23
3.1	Use case examples in accordance with their application and application class. . . . .	31
3.2	Security Services Categories . . . . .	36
3.3	Security Services entity . . . . .	37
3.4	Security Management entity . . . . .	38
3.5	Security Defense Mechanisms entity . . . . .	40
4.1	A presentation of all the use cases chosen by the interview candidates. The use cases are presented with their respective abbreviation and are referred to as “use case codes.” The full description of each use case is written out in the Description column. Each use case is also tagged with its associated day phase, e.g., Cooperative Merging Assistance (CM) is a day 3 use case. The table is color-coded by Red: use cases within day-phase 3; Green: use cases within day-phase 2; Blue: use cases within day-phase 1. . . . .	43
4.2	ToE service specification. . . . .	58
4.3	ToE characteristics and behavioral communication patterns. . . . .	58
4.4	ToE Security Objectives . . . . .	61
4.5	ToE Security Functional Requirements . . . . .	62
4.6	Asset impact rating . . . . .	64
4.7	Attack plausibility . . . . .	67
4.8	Attack intensity rating . . . . .	67
4.9	Threat level . . . . .	68
4.10	Attack potential of Radio jamming . . . . .	69
4.11	Attack potential of DoS & DDoS . . . . .	69
4.12	Attack potential of Message manipulation . . . . .	70
4.13	Attack potential of Replay attack . . . . .	71
4.14	Attack likelihood determined in relation to threat level and vulnerability rating for DSW-EEBL. . . . .	72
4.15	Attack likelihood determined in relation to threat level and vulnerability rating for HLN-EVA, GLOSA, and SPTI. . . . .	72
4.16	Overall impact rating by attacks . . . . .	72
4.17	Risk evaluation for radio jamming considering the ToE . . . . .	73
4.18	Risk evaluation for DoS & DDoS considering the ToE . . . . .	73
4.19	Risk evaluation for message manipulation considering the ToE . . . . .	73
4.20	Risk evaluation for replay attack considering the ToE . . . . .	73

5.1	Use cases summarization (ordered in deployment phases from 3 to 1). . . . .	74
5.2	Risk evaluation summarization . . . . .	77
5.3	The risk results differences between this thesis and [3] considering use case DSW-EEBL. . . . .	77

# List of abbreviations

ACC	Adaptive Cruise Control
AD	Automated Driving
ADAS	Advanced Driver-assistance System
AV	Automated Vehicle
C-ITS	Cooperative Intelligent Transport Systems
C-V2X	Cellular V2X (no matter short- or long-range)
DSRC	Dedicated Short Range Communication
EEBL	Emergency Electronic Brake Light
ELEC	Electronic
HLN	Hazardous Location Notification
ITS	Intelligent Transport System
ITS-G5	The interface enabling vehicular comm. in the 5.9 GHz
ITS-S	Intelligent Transport System Station
LOS	Line-of-sight
NLOS	Non-line-of-sight
OEM	Original Equipment Manufacturer
OTA	Over The Air
PC5	ProSe Direct Communication Interface 5 (short-range cellular comm.)
RSU	Road Side Unit
SCH	Service Channel
SDO	Standards Developing Organizations
TA	Thematic Analysis
ToE	Target of Evaluation
TRX	Transcript
TVRA	Threat, Vulnerability, and Risk Assessment
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
Uu	Interface between the UTRAN and the UE (long-range cellular comm.)
V2X	Vehicle-to-Everything
VANET	Vehicular ad hoc Network
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environments

# Chapter 1

## Introduction

Vehicle-to-Everything (V2X) communication is one of the technologies that will enable Autonomous Vehicles (AVs) [4]. This technology is already available at some scale and enhances the driving experience (comfort), traffic efficiency, and road safety [5]. Still, the technology needs to be improved in several areas before AVs can rely on it entirely. Nonetheless, the technology will—in its now initial deployment phase—help the driver become better aware of the environment. The traditional way of providing the driver with additional information about the environment, thus improving the driver's awareness of the surroundings, is with the intercepted data from the onboard sensors. But, there's a certain limitation to this approach: the sensors can only intercept what they see from their current perspective, i.e., their current line-of-sight (LOS) [6]. By enabling communication and exchange of traffic status data between vehicles and infrastructure, vehicles will be able to present the driver with information of their non-line-of-sight (NLOS), allowing perception and higher predictability of things behind the corner, thus improving traffic safety [7]. This technology is called Vehicle-to-Everything (V2X), a significant milestone in the automotive industry considering the aspects mentioned earlier: comfort, efficiency, and safety. This thesis will investigate a few significant V2X use cases and evaluate the cybersecurity risk for some of them.

The [List of abbreviations](#) explains the meaning of some of the most relevant and repeated abbreviations and acronyms used in this thesis.

### 1.1 Background V2X

Wireless communications, and especially mobile telecommunication networks, have opened up for unthinkable technology. Looking back only a decade, many of the things possible today would seem unimaginable. This revolutionary technology has affected all possible functions of society in one way or another. Today's majority of enterprises, businesses, and societal functions have at least some technical systems that rely on wireless and mobile communications in their organization [1]. With the development of 5G, more demanding systems can now also rely on cellular communication, which opens up major opportunities within the society and industries. An example might be automotive. The automotive industry is now shifting toward making vehicles more

independent of the driver, creating technology within vehicles that can trigger warnings and take action upon information sent over networks—enabling better and safer transportation. With 5G as an example, these vehicles are now closer to reality. And 5G isn’t the only option; Wifi has also been available as a solution for a long time to enable connectivity between vehicles. Wifi was actually the first solution considered for V2X direct communication since cellular was not mature enough to offer the same capability back in 2010 [8, 9] when the Wifi option was first proposed. But, as mentioned earlier, as cellular has developed into a more mature state, it can now also be utilized for V2X direct communication [10]. But despite 5G being newer than Wifi, it might not necessarily be a better option. Wifi is still a strong candidate, and improvements for this protocol for V2X scenarios are current. More information about V2X communication types and *Wifi versus cellular* is presented in sections 1.1.3 and 1.1.4, respectively.

Many vehicle manufacturers—or “OEMs” (Original Equipment Manufacturers)—are currently investigating how they can make their vehicles more intelligent and independent of the driver. For example, some people reading this are probably aware of Tesla’s investments within this area with their so-called “Full Self-Driving” (FSD) system that they’ve implemented into their latest models. This system is a typical example of vehicle technology that pushes the boundaries in developing autonomous vehicles (AVs) [11]. But the fact is that “Full Self-Driving” systems—i.e., AVs—are not yet commercially available on a large scale [12]. There are only a negligible number of vehicles that so far meet the precise criteria of autonomy according to Society of Automotive Engineers (SAE) J3016 [13]. These vehicles are also only available in specific regions in a few parts of the world where they are allowed [14, 15, 16, 17]. But many OEMs consider themselves to have met the required technology for autonomous driving (AD), and certain vehicles are qualified as AVs from a technical perspective [18]. Still, other challenges exist and are beyond the OEMs control, such as legislation [1]. Therefore most of these AVs cannot yet be released—or at least not the autonomous functions. Vehicles qualified as AVs from a technical perspective will be able to upgrade their so-called Advanced Driver-Assistance Systems (ADAS) functions with Over-the-Air (OTA) updates for achieving a higher autonomous level directly when upgraded. So, when regulation allows AVs on the roads or when the implementation of V2X is complete (considering AVs that will utilize V2X for the latter scenario), OEMs will potentially be able to release their autonomous functions with OTA updates [19]. This feature will also be crucial from a broader perspective since other vehicle systems can also be patched. Then the need for recalling vehicles posing a significant safety risk due to some system instability or vulnerability—such as with the Jeep Hack event where 1.4 million cars were recalled by Fiat [20]—will possibly be drastically reduced.

Considering the above, connectivity (as previously explained) will undoubtedly provide better conditions for deploying vehicles with autonomous and other high-end functionalities. But for this to happen, close collaborations are required between OEMs, government agencies, decision-makers, infrastructure sector actors, telecommunications network operators, standardization organizations, and last but not least, the end-user—i.e., the driver and passengers [1].

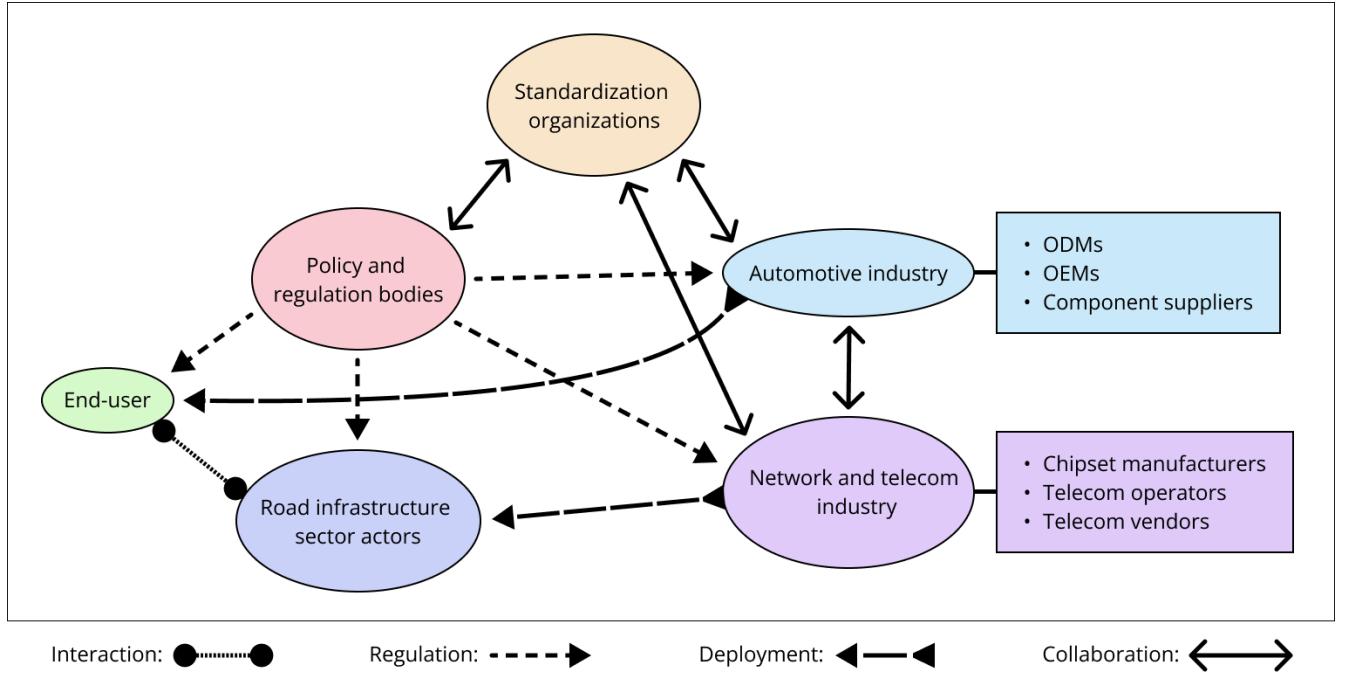


Figure 1.1: Relationship between V2X stakeholders (illustration replicated from [1]).

In short, vehicles with autonomous functionality stand in front of a two-fold challenge: technical and organizational. The technical challenge is developing and implementing the fundamental functionalities, such as communication between vehicles (V2X) with extremely low latency and high-reliability [1]. While the organizational challenge is the adaptability of these systems in real-life situations, requiring infrastructure and universal standards [21].

### 1.1.1 V2X definition

V2X is an acronym for Vehicle-to-Everything and is a broad term that entails mainly technology enabling vehicles to communicate with things in their local surroundings. The “X” refers to the “things in the surroundings” [22], i.e., everything in the vicinity. For example, cars sharing data with—and intercepting information from—other cars in their vicinity in a so-called vehicular ad hoc network (VANET) [6]. The cars advertise their location, planned route, and other useful information (such as alerts if a car becomes stationary on the road due to a breakdown) to the surrounding vehicles so the driver can be aware of the upcoming traffic scenario and plan accordingly. The recent example is typical for the early deployment phase of V2X communication. In later deployment phases, the cars may collect information about their vicinity through their onboard sensors and then this information is—not only processed within the certain vehicle, but also—distributed in the VANET, allowing other vehicles to take advantage of that data to improve their vicinity awareness even further [6]. This information can then also be forwarded to the ADAS for more automation.

There are subcategories available to the term V2X that describes particular scenarios for the technology. For this thesis these are referred to as "*link types*," as how it's called in [1].

- Vehicle-to-Vehicle (V2V)—The communication between two vehicles.
- Vehicle-to-Infrastructure (V2I/I2V)—The communication between vehicles and the infrastructure.

These two options are the leading link types of V2X, considering the definitions and the descriptions in the relevant literature as of this writing 2022 [1, 6]. But there are two other very frequently mentioned link types alongside the two main ones [1]:

- Vehicle-to-Network (V2N)—Making it possible for vehicles to use internet-based cloud services for their automotive features such as GPS map updates or the infotainment system that most vehicles nowadays are embedded with [1]. This option also utilizes the OTA updates, simplifying the software update process for modern vehicle systems [19].
- Vehicle-to-Pedestrians (V2P)—The communication between vehicles and vulnerable road users (RSUs).

The two latter communication options are also considered V2X communication directions, and therefore the V2X concept is not limited to only V2V and V2I/I2V [1, 4].

### 1.1.2 Entities utilizing V2X

V2X is, as previously explained, one of the technologies for allowing vehicles more autonomy in the future. But V2X should not be confused with AVs since V2X isn't an autonomous function; instead, it is the communication between vehicles that either is autonomous or—for the current modern vehicles—only equipped with some automated processes (ADAS). For example, the Volkswagen car ID 5 has some early V2X functionality services implemented that only alert the driver about traffic status and warn about road hazards which are displayed on the dashboard. These services in the V2X-equipped VW cars go under the name of Car-to-Everything (Car2X), which VW has chosen to call it in this early stage of deployment [23, 24]. The car also has the latest ADAS services, which indeed provide some automated functions, but the car is still not autonomous according to the definitions within SAE J3016 [13]. So, V2X is currently used to improve the performance of modern vehicles advancing toward the next generation of automotive functional safety systems and higher levels of autonomy [19, 24].

Vehicles that utilize this communication and participate in a V2X network should be considered cooperative vehicles [13]. The term referring to vehicles equipped with V2X and automated functions are therefore not simply "AVs" but instead referred to as "Cooperative AVs (CAVs)," this term can be considered the universal term for such vehicles. In Europe, V2X-equipped vehicles are though, in general, mostly referred to as "Cooperative Intelligent Transport Systems" (C-ITS) [22]. C-ITS also refers to mainly road-bound vehicles with this functionality [1]. The broader term ITS Station (ITS-S) includes all entities involved in a V2X network, i.e., the vehicles, Road Side Units (RSUs), and vulnerable road users (VRUs) devices equipped with V2X functionality [19, 25]. These entities are equipped with the same fundamental components, and therefore, they

are not distinguished [26]. But it is important to mention that all these terms are mostly bound to a certain standard. Standards are covered in section 1.1.4.

### 1.1.3 V2X communication types

There are two main types, or categories, within the V2X communication:

- Short-range communication—Referring to direct communication between vehicular nodes with the option of both single- and multihop messaging [27, 28]. This communication option uses either an interface with wifi-similar compatibility in a so-called VANET or an interface for cellular sidelink called PC5 (read more about this in section 1.1.4).
- Long-range communication—Mostly referred to as up- and downlink communication with the cellular Uu interface, which requires cellular base stations as RSUs [1]. Long-range communication can be classified into two main channels, namely:
  - Broadcast channel—Refers to messages sent to multiple entities within the network without the transmitter knowing the receiver’s addresses. A broadcast channel within V2X may be the Global Navigation Satellite System (GNSS) [29].
  - Addressable channel—This channel is usually used when transmitting voice/data to a devoted receiver, i.e., a specific destination address [29].

### 1.1.4 V2X standards and protocols

Several standards are available for V2X, some of which are more commonly known and established than others. For example, the ETSI ITS standard (built upon the IEEE 802.11p/WAVE access technology) has been around since 2010 and is thus one of the oldest V2X standards [25]. Below are some primary standards, standards developing organizations, and radio access technologies presented.

#### 1.1.4.1 Primary standardizations, Standards Developing Organizations (SDOs), and other V2X stakeholders

There are multiple SDOs and regulation bodies that either directly or indirectly are active within the domain of V2X development and deployment. The many V2X stakeholders’ technical specifications and technical reports require harmonization to decrease potentially overlapping documents, i.e., close collaborations and agreements (see, e.g., Figure 1.1 in section 1.1).

##### European Telecommunications Standards Institute (ETSI)

ETSI is one of the largest standardization organizations active within the V2X development [30]. Their standard “ETSI ITS” has already been adopted to some extent by Volkswagen [31]. ETSI consists of several technical groups involving several collaborating participants and partners. The

technical committee (TC) for the V2X technology is called ITS. The ITS TC supports the acceleration of ITS deployment in Europe by creating technical specifications, technical reports, and common European standards documents for harmonization between V2X stakeholders and interoperability of all the elements involved. Despite their current focus on Europe, they aim to achieve global standardization.

### **3rd Generation Partnership Project (3GPP)**

3GPP is a project involving several SDOs—ETSI, for instance—to produce technical specifications and reports for cellular telecommunications systems [32]. The project has been active within the V2X field since 2016 focusing purely on C-V2X technology, thus covering both the PC5 and the Uu interface. The 3GPP documents are produced by jointly reviewing results from the standardization organizations' investigations, e.g., ETSI's research on the topic [1].

### **The Institute of Electrical and Electronics Engineers (IEEE)**

IEEE is a large association consisting of several technical professions, and the IEEE Standards Association (IEEE-SA) organization is one of them. IEEE-SA is active in most technological areas, developing standards for many industries, including telecommunications. IEEE-SA produces the 802.11p and 802.11bd access technologies standards.

### **Society of Automotive Engineers (SAE)**

SAE is another association of engineers, specifically within the aerospace and automotive industries. SAE formed a technical committee in 2014 to produce the J2735 DSRC V2X standard. The standard was developed in collaboration with ETSI and the IEEE1609 working group. SAE also formed a C-V2X committee in 2017 to support the development of C-V2X for 802.11p-based standards. The purpose is that cellular technology should support in situations where 802.11p can't be used for fulfilling a particular goal [1].

#### **1.1.4.2 Radio access technologies**

As mentioned earlier, there are two main radio access technologies for V2X direct short-range communications:

Table 1.1: The two direct short-range communication modes and their options/enhancements.

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• 802.11 protocol family – 802.11p</li> </ul> | <ul style="list-style-type: none"> <li>* The task group was formed in 2004 [1] and the specifications were published in 2012, and thus the oldest radio access technology for direct communication proposed for V2X.</li> <li>* This radio access technology is used within the ETSI ITS standard as of 2022.</li> </ul> |
|--|--|

- 802.11bd
  - \* IEEE created the 802.11bd task group 2019 to enhance the above predecessor.
  - \* 802.11p and bd are compatible with each other.
- C-V2X
  - LTE-V2X
  - 5G NR-V2X \* Enhanced version of LTE-V2X.

Solutions (or standards) built on the 802.11p protocol might be referred to as the traditional V2X direct communication solution enabling Wireless Access in Vehicular Environments (WAVE), thus also often referred to as 802.11p/WAVE. In contrast, newer C-V2X solutions involving 5G NR nowadays have accomplished the same (if not better) performance capabilities in comparison to the IEEE 802.11p and 802.11bd (read more about this in the next section [1.1.4.3](#)).

#### **1.1.4.3 Current debate about standards**

In the beginning, C-V2X was mainly referred to as only long-range communication since it had to rely on the Uu interface that requires base stations to function. Thus, it was not suitable for vicinity information exchange due to cloud traversing latency. Now, as of 2022, and with Long Term Evolution (LTE) and fifth generation (5G) cellular communications, the scenario is very different. With this cutting-edge cellular technology, direct communication between entities over cellular is possible with an interface technically referred to as the PC5 interface, enabling *side-link cellular communication* with much lower latency compared to transmissions via the Uu interface [22]. In some literature, C-V2X may also be referred to as LTE-V2X and/or 5G NR-V2X (New Radio V2X) [1]. With this evolution of cellular communication, a considerable debate has occurred between the advocates of the original direct communication solution with the 802.11p protocol and the cellular side-link (PC5) advocates. For example, Qualcomm, one of the world's biggest semiconductor suppliers in telematics, has contributed a lot to the C-V2X solution specifications. They have been a supplier to the automotive industry for over 15 years and deliver chipsets for both direct communication solutions, i.e., PC5 and 802.11p. They argued in a blog post [33] as early as 2018 about different advantages with C-V2X above the 802.11p solution as a company with a significant experience with both solutions. One of their arguments is that 802.11p was an appropriate solution for vehicle communication at the beginning of the V2X development phase. As of 2018, and now also 2022, C-V2X is, according to many telematics companies, the best suitable radio technology for V2X. The reason is that the 5G NR has better guarantees in areas such as range and field performance compared to 802.11p, according to their respective test results [33]. 802.11p is susceptible to certain congestion and doesn't have as specific minimum performance guarantees as 5G NR. It becomes problematic when considering more advanced and safety-dependent applications with strictly defined requirements. Therefore, 5G NR is a competing solution for these applications and use cases with clearer performance guarantees according to [33]. But despite these advantages of 5G NR, certain OEMs such as Volkswagen have already implemented some

basic V2X functionality based on the 802.11p technology. They've done this to push the development of V2X forward, investing in technology that, according to them and several others, is the most suitable technology for vehicular environments. 802.11p, for example, has a 1 km communication range and works at speeds of 500 km/h [34]. But despite the benefits these investments might seem as high risk since the debate is ongoing, but there might as well be a high reward awaiting them. For example, the European Commission (EC) recently stated in their ITS directive for 2022 the importance of interoperability and backward compatibility of new V2X technologies. This directive now protects Volkswagen as a guarantee that the 802.11p solution will now forth function for a vehicle's whole life cycle. Therefore, Volkswagen has set the standardization tone for Europe regardless of the ongoing debate [35]. In association with such investments (such as with Volkswagen) and directives considering ITS-G5, the 802.11p protocol has undergone new ventures by the IEEE Task Group. These ventures are referred to as the IEEE next-generation V2X (NGV) 802.11bd. This enhanced protocol improves the physical and data link layer of 11p while maintaining compatibility with the 11p. This protocol thus competes against 5G NR.

### 1.1.5 V2X use cases

There are many use cases for V2X, and the most well-known are, as mentioned before, driver comfort, traffic efficiency, and road safety. In a lower level of abstraction, more detailed-described use cases exist, which can be categorized within these three *well-known use cases*. Some famous examples of such use cases are:

- Green Light Optimum Speed Advisory (GLOSA) is a use case that will provide information about an intersection's status and when the intersection's red lights turn green (or red), advising the driver (or the vehicle's ADAS) of an appropriate speed for approaching the intersection more efficiently [5].
- Electronic Emergency Brake Light (EEBL) is when a vehicle brakes very hard—either by road hazard prevention or human error—and sends an alert to the drivers behind to avoid a chain reaction of panicking braking vehicles in the last second. This alert appears on the following vehicle's dashboards so the driver or the vehicle's ADAS can take action accordingly and successively slow down in time approaching the hard-braking vehicle [19].
- Emergency Vehicle Approaching (EVA) is similar to EEBL in the messaging. The active emergency vehicle sends a warning message that alerts vehicles' in its vicinity, making them aware of its presence not only through the sirens but also through an alert on the dashboard [5].
- Cooperative Adaptive Cruise Control (C-ACC) is ACC with implemented V2X performance. The current ACC is when the vehicle uses some ADAS functions to control vehicle dynamics in general traffic situations with information only gathered from its onboard sensors. C-ACC also involves information sent within the V2X network, which gets mixed into the sensor fusion functionality of a C-ITS [5].

- Platooning is a use case mainly for trucks (the equivalent use case for cars is “C-ACC ‘string’”) which will let trucks link together on a highway in a so-called “platoon.” The use case will support trucks leaving and joining the platoon with dedicated messages for these maneuvers. A platoon depends much on the automation level that the participating trucks have. It is challenging to maintain a safe platoon if all the trucks don’t have the same automation capability, i.e., autopilot and accurate sensor fusion functionality [5].

These use cases above are relatively universal, no matter standard. Still, it is worth mentioning that other use cases that aren’t as universal might differ in definition depending on what standard. Therefore, it may be important to clarify the standard of a specific use case when discussing overall V2X use cases. Use cases are described further in section 3.1.1.

## 1.2 Problem statement

According to all the above, V2X is undoubtedly one of the current big activities within the automotive industry. Based on this, much research is current, and the field of science has been widely studied for the last decade with standardization documentation released as early as 2009 [36]. Also, almost every OEM in the automotive industry has several ongoing major projects and collaborations regarding this technology. They perform these projects within environments of real-life situations, test sites, and simulations. The main factors why car manufacturers invest in this technology are the earlier mentioned safety, efficiency, and comfort benefits. But it is also due to some other factors. For example, safety organizations such as Euro NCAP have begun to base their safety rating on these technologies since they also see benefits with these functions [35]. Car manufacturers must then fulfill specific technological requirements to earn the highest rating at these safety evaluation organizations, something all car manufacturers strive to accomplish. But even though the accomplishment of technological progress is current, the cybersecurity perspective may not yet have reached the same mature stage as the functionality itself [29]. But much attention is currently being brought towards cybersecurity for automotive, and the first standard that defines automotive cybersecurity was released last year [37]. This strengthens the fact that it is inevitable and vital to observe modern vehicles as electronic communications and information systems and evaluate the cybersecurity of these vehicles similar to how it is performed on any other regular IT system [38].

## 1.3 V2X and automotive cybersecurity

Studies of cybersecurity usually have different methodologies, some might focus only on attacks and attack surfaces with conceptual networking models such as the five layers TCP/IP protocol suite as a reference. Others might focus on the CIA triad or other cybersecurity-related attributes to determine specific security objectives for using these in a risk assessment to evaluate a particular system’s risk factors. In contrast, some might focus more on security requirements and potential

countermeasures against discovered threats. Or that risk assessment and countermeasures are considered in a single report. There are plenty of ways to conduct cybersecurity research within a particular area. In the section below, several studies will be presented which also exemplifies different ways to conduct research.

### 1.3.1 Cybersecurity attributes

#### 1.3.1.1 CIA Triad

The most common attributes used within cybersecurity are the ones that compose the CIA triad, i.e., the confidentiality, integrity, and availability concepts—but these aren't the only ones. Accountability and authenticity are two other concepts worth mentioning for this thesis besides the ones forming the CIA triad. There exist many more, but they are not relevant to this thesis.

#### 1.3.1.2 Accountability

Accountability is, in some scenarios, used interchangeably with non-repudiation though they slightly differ from each other. Accountability ensures that a user can be held accountable for what the particular user does by reviewing log files etc. Non-repudiation is somewhat broader. It means that a user should not be able to deny anything that the user has done. But for this to be true, several other cybersecurity concepts, such as authorization, accountability, and auditing (AAA), must be included [39].

#### 1.3.1.3 Authenticity

Authenticity is closely related to integrity, but instead of checking the data integrity, it checks the integrity of the origin. I.e., authenticity verifies so that the transmitter is the recipient's anticipated transmitter [39].

### 1.3.2 Cybersecurity research within V2X and automotive

The following section presents some recently published and related research and development works within automotive cybersecurity—note that most of them were published before the ISO/SAE 21434 [37] standard was released. Automotive cybersecurity encompasses defense and restoration mechanisms for threats and attacks towards modern vehicles as electronic communications and information systems [40].

The following reports have been carefully selected and aim to provide the reader with an overview of the cybersecurity research being conducted in V2X, as well as a simple presentation of results, such as the definition of specific threats, attacks, and countermeasures. The academic papers have been chosen according to publication date no earlier than 2019 and citations no fewer than 20, with [41] as the only exception with only four citations. The reason there are no research papers earlier than 2019 depends on the topic's recent progress in the development according to

section 1.1.4. 2019 is a suitable year since this was also the year when the deployment of mature V2X use cases was introduced [22, 23, 31].

Standardization documents for V2X have also been considered and especially the documents from the standardization organization ETSI since they've performed a comprehensive risk assessment on their technology which is interesting for this thesis's purpose (section 1.5). These documents were reviewed to understand specific technical information or certain methodological concepts relevant for V2X security.

### 1.3.2.1 *Cybersecurity challenges in vehicular communications (2019) [42]*

In this paper, Zeinab El-Rewini et al. propose a framework including three different layers. These are (1) sensing, (2) communication, and (3) control. This framework is supposed to give a better understanding of automotive security. The framework is called Autonomous Vehicular Sensing Communication Control (AutoVSCC), and the three different layers imply:

3. Control – This layer represents the autonomous functions within a vehicle, e.g., adaptive cruise control (ACC), which controls the speed, braking, and steering to a certain extent.
2. Communication – Covering the area of inter- and intra-vehicle communication.
1. Sensing – Refers to the sensors equipped on the modern vehicles, namely vehicular dynamics- and environment sensors.

An illustration of the layers are given in Figure 1.2.

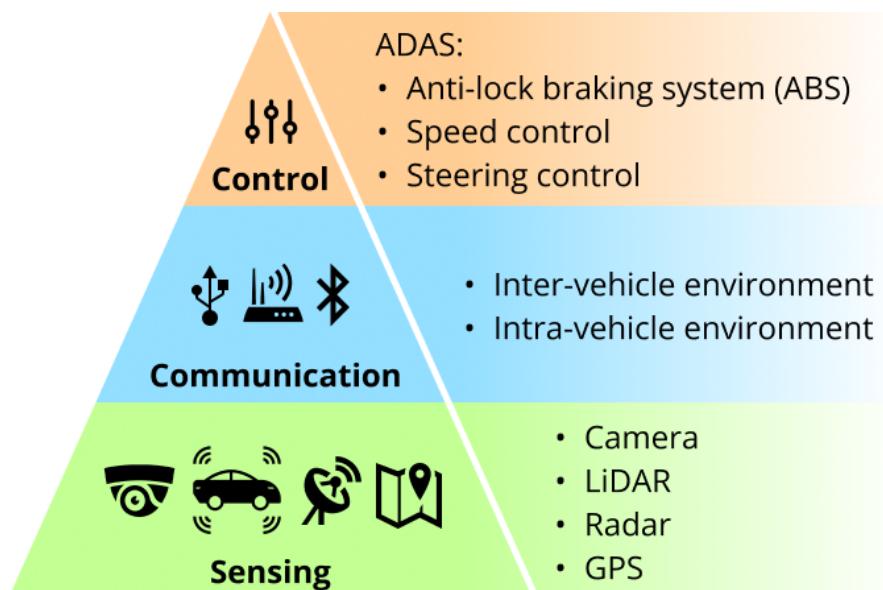


Figure 1.2: AutoVSCC framework

Their framework clarifies automotive security in the following way; the attacks identified on the sensing layer will also affect the upper layers, i.e., communication- and control layers. And

attacks at the communication layer will also affect the control layer etc. The authors use their proposed framework to describe their particular research scope within automotive security—which in this paper is on the communication layer. Further, they provide a sophisticated overview of the communication layer and its subcategories:

- Intra-vehicular environment
  - Automotive bus system (e.g., protocols such as CAN, LIN, FlexRay, MOST)
  - Vehicular ports (OBD2-, USB-, and the electric charge port)
  - Infotainment system
- Inter-vehicular environment
  - V2X communication (i.e., remote communication technologies, e.g., 802.11p, cellular, Zigbee, Bluetooth, etc.)
  - Cloud-based databases (infotainment and other purposes)
  - Clustering (subgroups of vehicles within VANETs)

The authors then analyze these subcategories of the communication layer from a security perspective. They conduct a literature review and provide a compilation of all the threats, attacks, and countermeasures obtained from a comprehensive set of scientific reports. They also provide a table with attack potentials on V2X communications ranging from low → moderate → high. The authors then discuss this information in detail in subdivided sections similar to the above punctuation list. The paper also provides an overview of future and potential security measures currently being researched.

### **1.3.2.2 Attacks and defences on intelligent connected vehicles: A survey (2020) [43]**

This paper investigates defense mechanisms against cyber-attacks within the broad scope of C-ITS<sup>1</sup> and the challenges therein, meaning they have focused both on the V2X aspect (inter-vehicle) and the intra-vehicle environment<sup>2</sup>. Despite the broad scope, they provide an in-depth analysis of the three mentioned characteristics. First, the authors cover state-of-the-art vehicle systems and address the so-called traditional Electrical/Electronic Architecture (EEA) and the drawbacks of applying advanced C-ITS functions to this particular architecture. The C-ITS needs optimized architecture for better internal vehicular network communication, better computation capabilities, and a better structure design for improved data flow and overall EEA improved performance. This

---

<sup>1</sup>In the report, the authors refer to these vehicles as Intelligent Connected Vehicles (ICV). This term is synonymous with C-ITS; therefore, the C-ITS is used in the description of their report to keep relative consistency of the chosen terms in this thesis.

<sup>2</sup>Referring to the components within a modern vehicle such as the Electronic Control Units (ECUs), On-Board Units (OBUs), On-Board Diagnostics (OBD), infotainment system, etc.

new and optimized architecture is called the next-generation EEA. They also provide information about internal vehicular network protocols, such as the Controller Area Network (CAN bus) protocol, which is the most successful within the automotive industry. But they also mention other protocols such as Local Interconnect Network (LIN), FlexRay, and Media Oriented Serial Transport (MOST). They address the benefits of the protocols and why they are in use but point out that they most likely will not be used for the backbone of the next-generation EEA. The Automotive Ethernet (AE) is a more likely candidate for this, with its larger bandwidth and better security. Besides the protocols, the authors also cover automotive software systems, sensors, and other units and components embedded within today's modern vehicles. This information is necessary for the next section of the paper, which involves vulnerabilities and cyber-attacks both on the external network communication (V2X) and the internal network, i.e., the intra-vehicle environment (EEA). It is a section with detailed descriptions of attacks and cybersecurity prerequisites. After that, they provide another detailed section focusing on security measures and defense mechanisms against the attacks they mention. They categorize these measures and mechanisms into four categories: cryptography, network security, software vulnerability detection, and malware detection. The author then provides a table summarizing all the essential info within the paper, thus appropriate as a reference for determining security measures according to security requirements. The authors have performed a literature study to collect the information in this paper.

### **1.3.2.3 Securing vehicle-to-everything (V2X) communication platforms (2020) [29]**

This survey is an extensive overview of the V2X domain, primarily focusing on security and privacy for direct 802.11p-based communication—but where they point out that most of the security and privacy concerns for 802.11p-based communication can also be considered for LTE-V2X (C-V2X), meaning that the paper is also relevant for C-V2X. The authors investigate everything from security/privacy standardization activities, challenges, threats, and attacks on- and proposed security measures for V2X. They write about the attackers' capabilities, intentions, and various attack variants that can be performed on a vehicular network. They classify attacks into different categories: active, passive, online, offline, internal, and external attacks. They refer to active attacks as when the attacker actively interacts with the vehicle, which causes abnormal behavior (e.g., data injection, DoS, spoofing and tampering with data, etc.). Passive attacks are, e.g., eavesdropping on communication to collect sensitive data, i.e., privacy-related attacks. Online attacks are when the attacker wirelessly exploits the vehicle at an operational state, unlike offline attacks, when the attacker needs physical access to the vehicle. The attacker could be authenticated or have system-level access, making the attacks internal. All other attacks are classified as external attacks. The authors focus mainly on DoS, Sybil, and false data injection. This is because these attacks are within the scope of threatening the current state of V2X security mechanisms. They describe these in detail and their various presence within the different networking layers and present existing solutions for detecting these attacks. Besides this, they also dig into some integrity mechanisms for how messages can be validated in a vehicular network.

Furthermore, the authors also outline possible concerns that are still a problem despite the available solutions to the attacks mentioned. They refer to these problems as gaps in and in-between security solutions and outline these as possible open issues, which is their primary contribution to the field of science. Their discoveries derive from reviewing and studying over 150 research papers published by academia, the industry, and government initiatives. They used a 25-year filter (1994-2019) to search for sources, which led to a comprehensive research foundation. They used Google Scholar, IEEE Xplore, and ScienceDirect, among other search engines for scientific publications. With such a comprehensive list of sources, they delimited their research to only malicious activity—i.e., they excluded anything related to abnormal activity due to faulty software or hardware. They also limited their study to purely vehicular communication security and excluded things such as general security as much as they could. But they still provided the necessary information for parts within the paper where they could not ignore the general concepts of connectivity (e.g., resource allocation, access- and interference mechanisms). Lastly, they analyze and discuss both 802.11p-based and C-V2X communication state-of-the-art security. They also point out some security issues within the intranet of a vehicle and how that can pose a security threat to V2X despite the intranet not being included within the V2X domain by definition.

#### **1.3.2.4 Security issues and challenges in V2X: A survey (2019) [27]**

The authors focus mainly on V2X security concerns and associated countermeasures. The paper first introduces the reader to the general concept of V2X. It provides a detailed overview of V2X features, various applications (including traffic management, safety, comfort, and infotainment applications), how it is evolving, and why it will be one of the enabling technologies for better road safety and efficiency in the future. They describe standardization activities with most focus on DSRC with the underlying IEEE 802.11p/WAVE standard at the access layer and IEEE1609 family in the upper layers. They explain these standards and the DSRC communication stack with an architecture model as reference. But they also shortly describe the LTE-V2X (C-V2X) activities and how the 3GPP standard is emerging. After that, they highlight the challenges, requirements, and primary attacks on V2X communication. They say that if considering a broad perspective on V2X, 802.11p-based and LTE-V2X (C-V2X) communication are vulnerable to already known network attacks, as Hasan et al. [29] also points out. The authors for this paper express the importance of designing detection and defense mechanisms within V2X communication standards that respect the user's needs and meet the requirements of V2X security. The following is a generalized outline of requirements that the authors mean, if considered, will build trustworthiness towards V2X systems: confidentiality, integrity, and availability according to the CIA triad, but also privacy and reliability. These are requirements that every communication system should consider, but it is even more important for V2X. The authors underline these requirements' importance but also observe the challenges of meeting them. They identify the following challenges: Dynamic Network Topology, Network Scalability, Heterogeneity, Communication Latency, Data Priority, Adoption to Future Platforms, Attack Prevention, and User Trust and Privacy. After they've covered V2X requirements and challenges, they give a comprehensive study on what attacks the V2X

network is vulnerable to. They classify these attacks according to the “Nature of threat,” which they categorize as below within a table:

- Behavioral pattern
  - Selfish attacks
  - Malicious attacks
- Attacks on H/W and S/W
- Attacks on infrastructure
- Attacks on privacy
- Data trust attacks

The table also consists of the “Role of the adversary during the attack,” e.g., “provide incorrect location information.” They also specify what service—or requirement—the attack compromises, e.g., availability and/or integrity. After that, they write about securing V2X communication and state-of-the-art mitigation solutions for possibly preventing the attacks mentioned. They do this with the following subsections: Symmetric Key Cryptography, Privacy Preservation, and Message Authentication. Lastly, they cover some completed or ongoing projects within V2X.

### **1.3.2.5 Security of 5G-V2X: Technologies, standardization and research directions (2020) [44]**

This article is a detailed overview of C-V2X security involving all communication options—up-, down-, and side-link transmission focusing on the current C-V2X situation. The authors dive into the differences between LTE-V2X and 5G-V2X techniques and their respective security with detailed illustrations as explanatory models. They also shortly compare C-V2X to 802.11p-based communication. They list some C-V2X security use cases to complement existing studies that involve research about the more general C-V2X use cases (practical and application-based). They also write about C-V2X security architectures and trends within that topic. They propose a novel Security Reflex Function (SRF) based architecture and a conceptualized illustrated model for this architecture. The architecture’s purpose is to fulfill features supporting Ultra-dense and Ultra-secure mobility management, which aims to support many connected vehicles while maintaining secure mobility management of entities within 5G-V2X. The authors call the presented functionality within the proposed architecture the “Security Reflex Function (SRF).” Read more about this architecture in their article.

In their article, they also provide an extensive list of attacks against V2X and categorize the attacks into three columns; what type of attack, what network types it involves—i.e., DSRC, LTE-V2X, 5G-V2X—and involved and/or affected entities/functions. Looking at this list, it is clear that the attacks that C-V2X is vulnerable to are also attacks that threaten DSRC.

Lastly, for this article, the authors discuss open issues—such as insider and zero-day attacks—alongside the usability of their proposed architecture.

### 1.3.2.6 5G-based V2V broadcast communications: A security perspective (2021) [41]

This paper focuses on the C-V2V communication with the PC5 interface based on the 3GPP standard. They examine sufficiently efficient security solutions in the context of the safety applications network requirements—such as low latency desires—and required defense properties according to the 3GPP standard. While their focus is primarily on the PC5 interface, hence the 3GPP standard, they still present the security services defined in IEEE 1609.2 and ETSI TS 102 940. But this is due to the 3GPP security solutions using the same security procedures, i.e., the VPKI architecture defined in IEEE and ETSI. So, despite the focus being primarily on the 3GPP, security characterizations in the IEEE 1609.2 and ETSI TS 102 940 are also described. The description of these security characterizations within the standard are security solutions operating in the upper layers of the ITS reference architecture model. The authors point out some shortcomings of this approach considering different traffic conditions—i.e., fast-moving vehicles, dense traffic scenarios—and the requirements of the safety applications. After the authors have given the reader a problematization description, they present a survey of alternative approaches with security solutions at the access layer considering the PC5 interface. Having the security at the access layer can provide better system compatibility for improved satisfaction of the standard's mentioned safety and security requirements while reducing deployment costs. The authors collected these alternative approaches from recently published scientific reports and thus conducted a literature study as their methodology. Their result mentions four security solutions suitable for implementation at the access layer considering PC5: asymmetric-based schemes (PKI), group-based solutions, symmetric-based schemes (e.g., MAC and HMAC), and hash chains. The authors analyze these solutions' advantages and drawbacks. They look into some cybersecurity objectives such as authentication, integrity, and non-repudiation, to name a few. They then present this information in a table appropriate as a reference for determining security solutions for safety applications. The authors summarize that a hybrid security solution is the most suitable. Since the authors have a security perspective on this technology, they also address cyber-threats against vehicular networks to indicate the importance of optimized security solutions in these environments.

### 1.3.2.7 Functional safety for enabling present and future V2X use-cases (2021) [19]

This paper describes the fundamentals of V2X communication and what the technology will do for the traffic environment. The paper also describes the need to examine V2X use cases from a hazardous perspective according to the Automotive Safety Integrity Level (ASIL) process defined in the ISO 26262 standard. The author describes functional safety requirements and what ASIL level (A, B, C, or D) the V2X should achieve to minimize false alarms while at the same time increasing the availability for improved accident prevention. The paper's scope is on the V2X protocol in general, i.e., both C-V2X and DSRC, which means that the author does not differentiate these protocols in such a high level of abstraction. The author concludes that there's no dependency on whether the vehicle uses C-V2X or DSRC to fulfill the paper's purpose, which is to analyze for potential failures in functional safety. So, despite the broad scope of the V2X protocol, the

author has a specific focus on V2X safety use cases which narrows their scope. The author uses the following classifications for evaluating a use case potential hazardous risk:

- Severity—This defines the level of injury from 0-3 (no injuries – fatal injuries).
- Exposure—The likelihood of a certain failure from 0-3 (improbable – high probability).
- Controllability—The driver’s ability to control the vehicle and prevent an accident from 0-3 (controllable – uncontrollable).

These are the attributes used in a so-called Hazard Analysis and Risk Assessment (HARA), a powerful analysis method for evaluating and ranking hazards for a system, and in this case, a vehicle. HARA, among other analysis processes, is mentioned in ISO 26262. The author then divides the use cases into their respective day phase. So, first, the author starts with day one use cases where they evaluate two common talked-about use cases, namely EEBL and “Left Turn Assistance.” These use cases are then assessed according to the above. Then the author does the same for a day two use case and a day three use case, namely, “Side Collision” and “Highway lane merge coordination.” After evaluating the risk for these use cases, the author continues by defining the safety goals of V2X technology and how to mitigate the assessed risks.

#### **1.3.2.8 V2X Attack Vectors and Risk Analysis for Automated Cooperative Driving (2021) [3]**

This paper looks at some well-known use case examples within the V2X domain, which they then analyze from a cybersecurity perspective by investigating possible attacks that may threaten the use cases. The authors use a risk assessment model inspired by the one used in [19], i.e., the risk methodology for functional safety following ISO 26262. They proceed with their risk assessment model using the same aspects of exposure, severity, and controllability found in the functional safety risk methodology but with a different scale ranging from 0 to 1, where 1 is critical and 0 is no impact.

Their primary focus is on ETSI ITS and SAE J2735. Their contribution is the evaluated security risk for the selected use cases being subject to an attack. The discovered risks can then be used to determine if a particular use case poses a more considerable risk than the actual beneficial safety features can contribute with. Finally, they run one of their selected use cases in a simulation and introduce a selection of the attacks. The use case they chose for this experiment were the well-known "Platooning." Running this use case in a simulation to see how it performs if subject to an attack gave a direct response to the potential risks that it involves.

#### **1.3.2.9 ETSI security documents (2010, 12, 17, 21)**

ETSI has six primary documents regarding the security of their V2X standard, i.e., the ETSI ITS. One defines fundamental security requirements (according to regulations, policies, and best practices) for ITS [26], a second document [45] is a risk analysis performed on ITS communication.

And lastly, the rest of the documents [46, 47, 48, 49] specifies detailed security requirements and technical solutions based on the first document [26] and the results of the risk analysis [45].

ETSI has developed a risk analysis methodology referred to as the ETSI Threat, Vulnerability, Risk Analysis (TVRA). This risk analysis method is described in detail in [50]. The method relates to the ITU-T three-stage approach recommendation I.130 described in [51]. The three stages within this approach are described in Table 1.2. The table also shows the seven TVRA steps in relation to the three-stage approach and their common denominators, such as step 2 being linked to stage 1.

Table 1.2: The relation between the ETSI TVRA and the three-stage approach.

ETSI TVRA	<b>I-130 (Three-stage approach [51])</b>
<b>Step 1:</b> Definitions of the scope (ToE)	<b>Stage N/A</b>
<b>Step 2:</b> Security objectives	<b>Stage 1:</b> Shall specify basic and supplementary services and their requirements.
<b>Step 3:</b> Functional security requirements <i>ETSI TS 102 731 [26]</i>	<b>Stage 2:</b> Shall specify the main functional entities of the services and the associated requirements. This stage should also fulfill the requirements in stage 1.
<b>Step 4:</b> Evaluate assets	<b>ETSI TVRA document [45]</b> This document explains the association between the security objectives (step/stage 1), fundamental security requirements (step/stage 2), and detailed security requirements (step 7/stage 3). The document is essentially the argument for the detailed security requirements considering steps/stages 1 and 2.
<b>Step 5:</b> Identify vulnerabilities and threats	
<b>Step 6:</b> Evaluate likelihood and impact	
<b>Step 7:</b> Evaluate risk	

*Continued on next page*

Table 1.2 – *Continued from previous page*

<b>ETSI TVRA</b>	<b>I-130 (Three-stage approach [51])</b>
<b>Step 8:</b> Detailed security requirements	<b>Stage 3:</b> Shall specify all the necessary protocols and equipment for these services at every relevant data transmission point, i.e., at each physical and logical interface, etc.
<i>ETSI TS 102 940 [46]</i>	
<i>ETSI TS 102 941 [47]</i>	
<i>ETSI TS 102 942 [48]</i>	
<i>ETSI TS 103 097 [49]</i>	This stage should also fulfill the requirements in stage 1 and 2.

ETSI has developed this TVRA to make better security standards. Document [26] can be seen as representing the step 3/stage 2 since it involves descriptions of ITS fundamental security services and security architecture which is further developed later in the last step 8/stage 3. Document [45] is a so-called technical report by ETSI that summarizes the results of their TVRA performed on their standardization (ETSI ITS). This document can be seen as occupying steps 4-7 of the TVRA method since it dives into vulnerabilities, threats, and risks concerning the ITS standard. And finally, once again, document [46] is a more detailed version of [26] according to, quote; “Based upon the security services defined in ETSI TS 102 731.” This document is meant more as a guide for the security implementation and deployment of ITS communication following the ETSI standardization. The three other documents support ETSI TS 102 940, i.e., [47, 48, 49]. So, i.e., these four documents together can be seen as fulfilling the final step 8/stage 3—complementing each other.

## 1.4 Positioning of this thesis

By reviewing the previous section 1.3.2 of earlier research studies, it is clear that most of the contributions involve recommended security services and solutions against the attacks threatening both inter- and intra-vehicular environments. Also, most studies have a broad scope covering several automotive topics from the cybersecurity perspective. And those studies with a more specific scope are instead very technically detailed with a low-level abstraction approach. When considering these three aspects, it may be necessary and advantageous to shed more light on the V2X area and its cybersecurity but with a more profound overview of the general V2X topic before digging into the actual technical and cybersecurity-related details. This has been conducted already, with a comprehensive introduction and background of the V2X area. Figure 1.3 highlights the focus area of this thesis considering the AutoVSCC framework presented in [42], basically the inter-vehicular environment, and more specifically on V2X direct communication.

Since most reports already cover the topic of V2X cybersecurity countermeasures well, the remainder of this thesis will be more similar to [19] and [3], where both of these papers look at the risks of some V2X use cases. [19] doesn’t base its research on any particular V2X standard in contrast to [3], which does base its research on the ETSI ITS standard. In accordance with this,

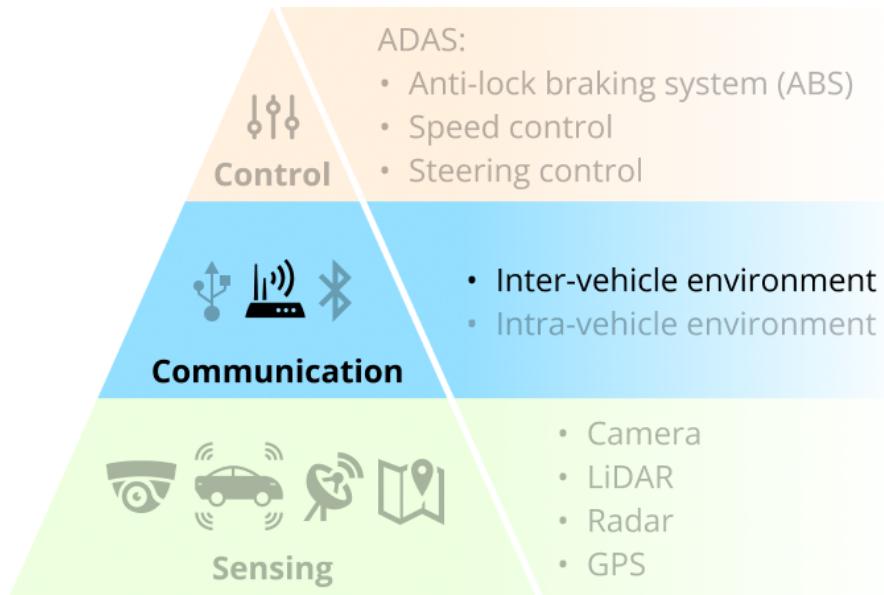


Figure 1.3: The scope of this thesis considering the AutoVSCC framework.

it might seem reasonable to research the standard currently focused on in the U.S., namely the 3GPP C-V2X. But since the ETSI ITS standard has achieved a particular mature stage as it has already been adopted by Volkswagen [31], and was one of the first standards available for V2X (thus having an elaborated security architecture [46]), the standard will be the base for this thesis research as well. This makes the scope of this thesis, and the scope of [3] relatively similar. But there will be a difference. The risk assessment method that [3] uses (the same as in [19]) will not be used in this thesis. This thesis will perform a risk assessment following the ETSI TVRA methodology. This is done to demonstrate the TVRA usage while at the same time validating that the latest security requirements [46, 47, 48, 49]—as the result of the real ETSI TVRA [45]—are appropriate for the use cases discovered in this thesis work.

## 1.5 Purpose of this thesis

This thesis aims to better understand some V2X direct communication use cases and examine a selection of them through a cybersecurity perspective. The report first establishes an overview of some use cases (both present and future) within the V2X direct communication domain. A cybersecurity risk assessment is then performed on a selection of these overviewed use cases with the latest security requirements ([46, 47, 48, 49]) taken into consideration. I.e., from the current state of the V2X technology and security, what cybersecurity concerns follow when a certain use case is introduced to a C-ITS? This thesis will then be able to validate if the latest security requirements are appropriate for the discovered use cases.

The thesis's purpose is to contribute an overview of V2X use cases, give information on V2X current standardized security requirements and solutions, and validate the cybersecurity risk for a

selection of the overviewed use cases. In short; to provide an additional perspective on the area of V2X, namely V2X use case cybersecurity.

A demonstration of how the ETSI TVRA can be applied to a scope of use cases will be given for natural reasons since it will be performed step by step in this thesis. Finally, the thesis also gives some future research directions.

### 1.5.1 Research questions

#### 1. *What are some significant use cases of V2X short-range?*

This research question is supposed to provide the thesis with specific use cases within V2X that have a certain awareness around them according to a few carefully selected interview candidates within the area. The meaning of *significance* in this thesis refers to use cases having a more considerable occurrence between these interview candidates. The idea is that the research question below will use the result of this question as input.

#### 2. *What cybersecurity risks can be associated with these use cases?*

When use cases according to the previous question have been discovered, the idea is to use a selection of these as Target of Evaluation (ToE) for a cybersecurity risk assessment. This question will provide the thesis with the cybersecurity perspective following what has been explained in the problem statement (section 1.5.2); that cybersecurity is now one of the most important aspects to consider for automotive when more connectivity gets involved.

### 1.5.2 Problematization of the research questions

Before the research questions are answered, some problems need to be addressed. There are two main problems. The first problem is that the automotive industry constantly changes, especially within connectivity. Therefore, this thesis result might not sufficiently represent the reality when published. The second problem is the complexity of the V2X area concerning this thesis's time and resources. Since the research questions are relatively broad in their definition, certain essential and technically detailed aspects of cybersecurity within V2X might be overlooked or missed. This is problematic since this would affect the result negatively. This is taken into account.

### 1.5.3 Delimitations

This paper will focus mainly on the ETSI ITS standard (i.e., the European V2X standard) and its associated use cases and security architecture. Although ETSI ITS is the primary focus, much of the concepts and conclusions within this thesis will also—to some extent—apply to other standards, such as the U.S. 802.11p/WAVE-based J2735 DSRC and the 3GPP standards since these have a relatively same security architecture. So, despite the focus, the thesis will provide information for understanding the general theory of V2X technology and security. Thus, the work will

not dive deep into the lowest levels of abstraction (mainly regarding advanced techniques as mentioned earlier). Further, a more narrow scope regarding the risk analysis scope will be achieved later in the thesis according to the first research question's formulation. A selection of the use cases for the risk assessment will be made, making the work of the thesis more proportional to the available time and resources.

# Chapter 2

## Methodology

This section defines the methodology, and the scientific approach used to collect the empirical material to answer the first research questions for this study; *What are some significant use cases of V2X short-range?* In short, the method used was a literature review combined with a qualitative research methodology in the form of semi-structured interviews. A risk assessment according to the TVRA methodology was conducted to answer the second research question; *what cyber security risks can be associated with the selected use cases?*

### 2.1 Selection of candidates

All five interview candidates (ICs) have different backgrounds but with the same current focus on V2X in common. Table 2.1 presents a short description of each interview candidate.

Table 2.1: Interview candidates information

Interview candidate	Description	Position
IC1	Researcher with a current focus on attack injection towards systems such as ITS. Has a background in computer science and currently works on several large projects within the area of ITS.	Institution
IC2	Has majored in communication engineering and has now a leading role at an OEM within the area of V2X connectivity and cybersecurity.	OEM
IC3	Has worked both in the telecom and automotive industry with radiocommunication and connectivity for several years. Currently has a leading role at an OEM within V2X and cybersecurity.	OEM
IC4	Is a software architect and have worked with software development for several years with a focus on vehicle communication, connectivity, and security.	Supplier (tier 1 & 2)
IC5	Has a background in systems science and security. Currently works as an operative manager within the area of connectivity and leads certain projects in the development of V2X technology.	Supplier (tier 1 & 2)

### 2.1.1 Ethical stance

Following ethical guidelines [52], all interview candidates were given a consent letter (letter attached in appendix A) in which they were informed that participation was entirely voluntary and that they may choose to end the interview at any time without any reason. They were also informed that the interview would take place via Microsoft Teams (no obligation to have a camera on) and recorded for analysis purposes. All participants were also informed that they are anonymous, that all information collected will only be used for analysis in the context of this study, and that no information of a sensitive character will be requested. The recording of the interviews will be deleted when they are no longer necessary. Participants were asked to contact the author with any questions or concerns and that the author would delete any section of the interview if the participant wished so.

## 2.2 Literature review

The literature review was used to prepare the theory for this report and provide a conceptual introduction and understanding of the area of choice, basically V2X cybersecurity. According to earlier research, several reports about V2X cybersecurity already exist. Therefore, a literature review was the most reasonable method for building the theory part of this report.

The search engines used for this literature review were IEEE, Halmstad University Ezproxy, and Google Scholar. The searches provided the literature study with scientific reports. The reports were obtained with specific search filtering from 2019 and forward, with the following search terms; V2X, cybersecurity, risk analysis, threats, and use-cases – thus narrowing the search results to interesting reports for this particular work. The year 2016 for the scientific reports was chosen so that the cybersecurity risks presented would be relatively representative of the year when this report was written.

## 2.3 Semi-structured interviews

While the literature review provided the report with the theory chapter, the qualitative analysis carried out by interviews provided more rich and detailed information. The interviews involved people working or conducting research within the field of V2X and who possess technical knowledge about the technology, its use cases, and certain related cybersecurity concerns.

### 2.3.1 Procedure

The interviews were held in week 13, 2022, and every interview was around one hour long.

The interviews were performed over Microsoft Teams both because of the easiness of meeting over a video call when the interview candidates and the author were not located at the same places and due to the software's simple recording capabilities. The interview agenda and questions were

presented in a PowerPoint over screen sharing. The questions were as follows:

First, some general questions about V2X were asked:

- *What do you think of the current situation of V2X?*
- *What do you think is the biggest challenge so far for V2X?*
- *What companies do you think have the biggest influence on this technical development right now?*

These questions gave the author an understanding of the interview candidate's outlook on the area of V2X, their point of view, and their focus.

The task was designed as a question within the interview (see the question further below). Each interview candidate was given a list of use cases to pick from for this question. This list can be found in the C2C-CC white paper called "Guidance for day 2 and beyond roadmap" [5]. This roadmap is focused on Europe's automotive C-ITS deployment and summarizes both already deployed and future planned use cases. Despite C2C-CC being the roadmap's creators, C2C-CC has also received support from stakeholders such as CRoads and standardization organizations when needed. Therefore, this list within this roadmap is well suited as a reference list for this task. Every candidate was given 15 minutes to complete this task and was, according to the definition of the question, to pick four use cases of each day-phase category, i.e., four from day one, four from day two, and four from day three:

*From your perspective of expertise within this area, choose:*

- *4x day-1 use cases*
- *4x day-2 use cases*
- *4x day-3 use cases*

*... that you consider will have/or already has a significant role for traffic situations. By "significant role," I mean use cases that you consider are the most relevant or predominantly crucial thinking from the core of V2X technology.*

The "core of the technology" refers to the three aspects; driver comfort, traffic efficiency, and road safety.

The candidate was told only to pick four use cases within each day phase because it seemed like a reasonable number for being able to complete the task within 15 minutes and that it also leaves room for the candidates to be able to choose relatively different use cases. For example, for day one 36 use cases exist in the list. Here, each candidate could choose unique use cases altogether. For days two and three, 15 and 16 use cases respectively exist, which doesn't give the

same possibility but is still a good quantity to choose amongst while still maintaining room for different answers.

Each candidate was given a copy of a Google Sheet which they could mark their answers. This Sheet was shared over Teams.

This task, or this part of the interview, was unique compared to how semi-structured interviews are traditionally performed. This task was indeed more structured and more like the quantitative methodology. But this task seemed the most appropriate way of letting each candidate choose use cases when they had a moment to themselves and think and resonate about what use cases they wanted to include in their picking. Each candidate could have performed this task before the interview, more like a traditional quantitative study. But this would have required more time from the interview candidate, and the time it would have taken each candidate to perform the task would have been difficult to confirm in this scenario. Each candidate needed to be given the same amount of time to complete the task. Otherwise, the candidates might have begun to read more into each use case and chose use cases according to the use case description rather than their current knowledge. Or that a candidate would perform the task too quickly, not paying equal attention to the task as the others, thus giving a quite imperfect answer compared to how the candidate completed the task during the interview. But the biggest reason why this task was combined with an interview was for both practical data retrieval and for discussing the following questions below with each candidate's choices fresh in mind:

- *Explain a bit of why you chose these four day-x use cases?*
- *Do you see any potential cyber threats toward a vehicle with these use cases?*
- *If so, are there any security measures?*

After these questions, the interview ended, and the author thanked the candidate for the participation.

## 2.4 Data analysis

The data analysis method used on the interview material in this thesis was the so-called Thematic Analysis (TA). The TA is the most flexible analysis method in that it can be used in many different areas of science, thus very applicable for this topic as well [53]. It is also a method that can generate more complex data, and since this report handles a complex area, the TA seemed to be a suitable method of choice. Also, based on the time and resources that this work had to relate to, the TA method is a relatively simple analysis method, which was also a choice-factor. The TA is effective in many different scenarios considering its flexibility.

Regarding the research questions having a specific description, two *latent themes* were defined for the collected data of interest, the so-called "data set." The two themes were (1) use-cases and (2) cybersecurity concerns in accordance with the research questions (section 1.5.1). The TA will also be of the deductive type, which has a more theoretical approach than the other alternative,

inductive TA. The deductive type TA process identifies patterns within the data set with a "top-down" method, meaning that specific themes within the data set are pinpointed. In more scientific terms, the data set is being "coded" according to a pre-existing "coding frame" constructed also according to the research questions (section 1.5.1). See the coding frame in Figure 2.1.

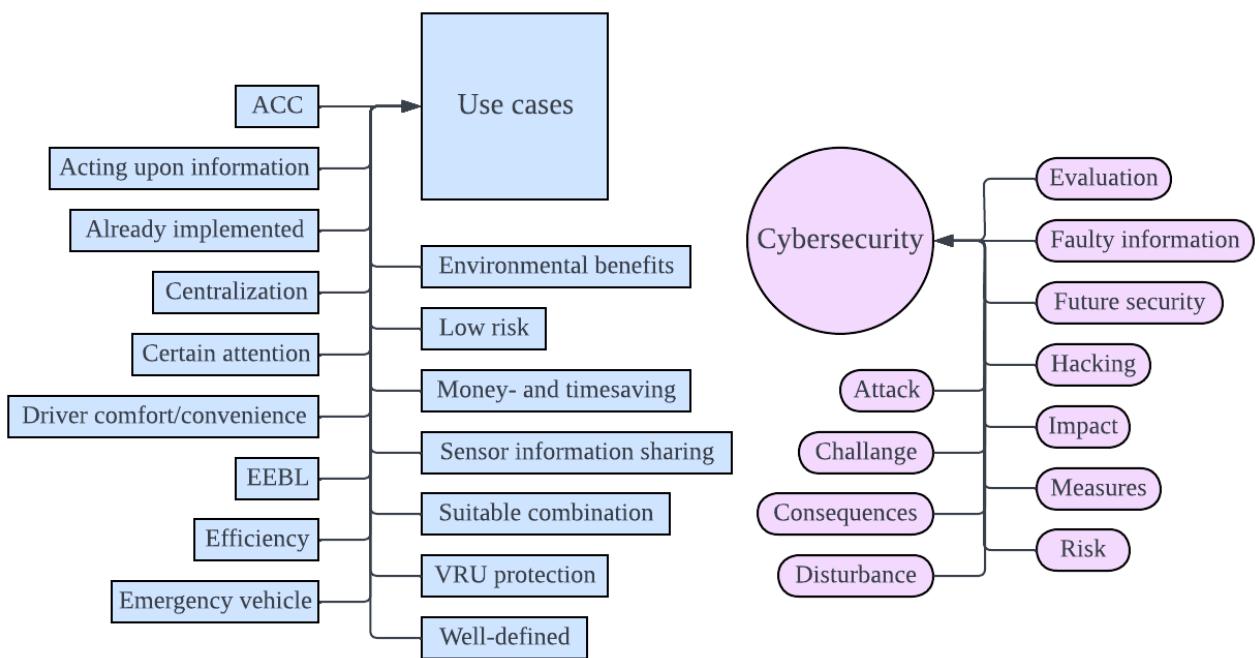


Figure 2.1: Coding frame for the TA.

Information within the interview material that seems relevant to this thesis and correlates to any codes in the coding frame will be extracted into citations. The relevant citations for this thesis will be presented according to Citation 2.1 with the data (information) extracted, the corresponding codes the data has been correlated to, and also references to where the specific info can be found within the transcripts.

#### Citation 2.1

Data extract	Coded for	Ref.
"Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit vestibulum ut placerat."	<ul style="list-style-type: none"> <li>• Code<sub>1</sub></li> <li>• Code<sub>2</sub></li> </ul>	Trx: ICX Row: xxx

## 2.5 Risk assessment model

ETSI's Threat, Vulnerability, Risk Analysis (TVRA) method, as described in [45], is, in short, a systematic ten-step risk assessment performed on an Information Communication Technology (ICT) system and the assets it's composed of. The overall goal of the TVRA is to identify potential

unwanted incidents that could occur to a system or its assets. This is done by identifying weaknesses, threats, and threat agents willing to attack the system. This information is then used for further analysis, namely the likelihood and impact of a threat, resulting in particular risks to which the system and its assets are exposed to in relation to its current security requirements. In accordance with the risks ratings, it becomes apparent of what risks that require highest priority for being mitigated with redefined security requirements followed by actual security countermeasures. The TVRA process is described below:

1. The risk assessment first involves identifying the Target of the Evaluation, the so-called ToE, and its environment. This step defines a specific scope of what kind of issue (a whole system, physical-, human-, or logical assets of a system) should be evaluated. The goal is to create a definition with a high level of abstraction of the ToE. I.e., only inventory the main components of a system (or elements of a component) and their environment—resulting in the main assets. This information is used for further analysis in the next steps. In this step, the TVRA purpose should also be defined, e.g., evaluating a system after an implemented function.
2. This step should also be reviewed with a high level of abstraction. It aims to establish an overview of the security needs for the standard or system in focus. The security objectives will be determined by reviewing the assumptions of the ToE and its environment from the previous step to the CIAAAA attribute framework (this framework is described in section 1.3.1). When determining security objectives, it is essential to ensure that every objective is realistic, achievable, measurable, and relevant [54]. This is necessary for establishing reasonable security requirements in the next step and thus achieving a meaningful risk assessment—in this case, a TVRA.

**NOTE:** The security objectives can be divided into two distinct groups, namely the ToE and its environment. It can be effective when performing a comprehensive TVRA but is necessarily not a requirement for the TVRA to still be successful [54].

3. Identification of the functional security requirements considering the security objectives.
4. Inventory of the ToE's assets but now in a lower level of abstraction compared to step 1. I.e., what are the necessary building blocks for an asset (main components and/or elements of a component)? Additional assets can also be identified by taking the previous steps into account.
5. Identification of the ToE's vulnerabilities<sup>1</sup> and threat level considering adversaries that may exploit these.

---

<sup>1</sup>A vulnerability, as defined in ISO/IEC 27033-1:2015 [55] is a weakness within a system that can be exploited by a threat.

6. Quantifying the likelihood and impact of these vulnerabilities being exploited by an adversary.
  7. Evaluate risk.
  8. Identification of alternative security requirements for reducing the risks.
  9. Cost-benefit analysis of the security requirements.
  10. Specifications of detailed security requirements and services (countermeasures).
- 
- These steps are left out of this thesis.

The three last steps are left out of this thesis since the purpose is only to validate that the security requirements within the ETSI TS 102 940 series documents [46, 47, 48] and [49] are appropriate for the use cases that have been discovered.

# Chapter 3

## Theory

Before the results are presented, some things must first be studied and provided to the reader, presented in this section of the thesis.

### 3.1 ITS reference model

The communication stack of the ETSI ITS standard involves four processing layers which can be illustrated according to the figure below:

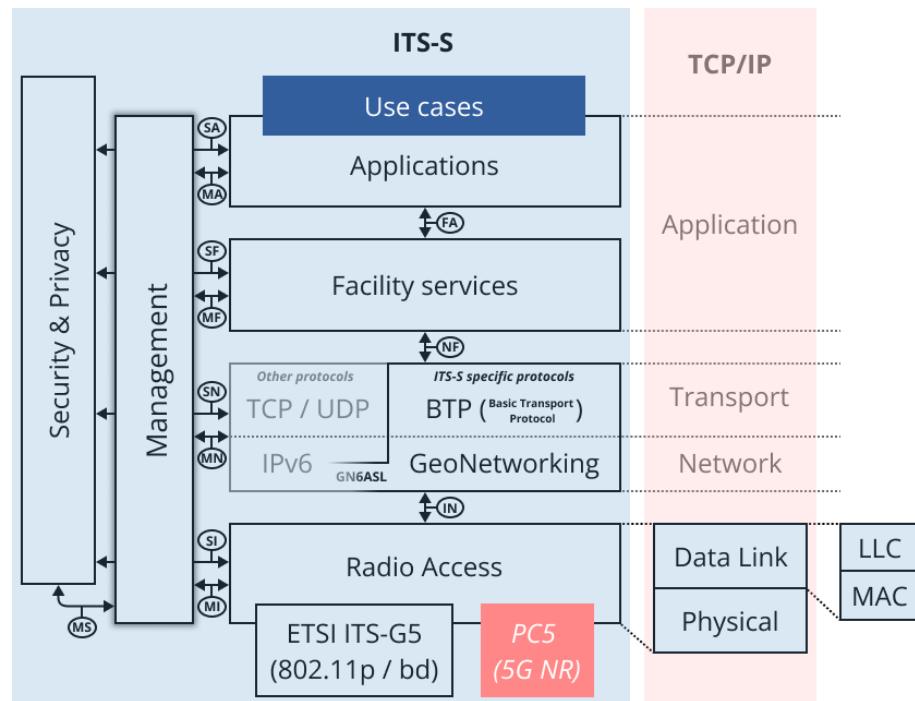


Figure 3.1: Illustration of the ETSI ITS communication stack.

This is not an exhaustive reference model but a simplified illustration only for this thesis purpose. The illustration shows the layers of the ETSI standard protocol stack similar to how it's

presented in ETSI's documentation for the ITS-S Communications Architecture [25].

This illustration also shows the Five layers TCP/IP model as a reference to the ITS-S layers. In addition, the PC5 interface has been added to this illustration at the access layer to demonstrate that the 802.11p and 802.11bd access methods are not the only ones available for V2X direct short-range communication [56]. Keeping in mind, though, that the 802.11p and 802.11bd are the primary access technologies for the ETSI ITS standard as of 2022.

### 3.1.1 Applications and use cases layer

As introduced in section 1.1.5, V2X use cases can be classified into three *main use cases*, namely driver comfort, traffic efficiency, and road safety. From a more technical perspective, these three *main use case categories* are defined as “application classes” within certain ETSI documentation, e.g., [46, 25, 36]. This thesis will henceforth use the same definition. These application classes can be further divided into certain ITS applications, fulfilling the desired use cases. The table 3.1 below shows the mapping of the use cases used as examples in section 1.1.5 in accordance with their application and application class.

Table 3.1: Use case examples in accordance with their application and application class.

Applications Class	Application	Use case	Day Phase
Traffic efficiency	Co-operative Speed Management (CSM)	Green Light Optimum Speed Advisory (GLOSA)	Day one
Road safety	Road Hazardous Warning (RHW)	Electronic Emergency Brake Light (EEBL)	Day one
Road safety	Co-operative Awareness (CA)	Emergency Vehicle Approaching (EVA)	Day one
Road safety	<i>Co-operative Awareness (CA)</i>	Cooperative Adaptive Cruise Control (C-ACC)	Day two
Road safety	<i>Co-operative Awareness (CA)</i>	Platooning	Day three

The two last use cases in the table have their applications in italics, and this is because they are future use cases that do not yet have all their details in place. Therefore their associated application/applications may change over time, and the information given above is only the current categorization as of 2022.

Three main deployment phases exist for all the V2X use cases called *day one*, *two*, and *three+* shown in both table 3.1 and figure 3.2. Each phase represents the advancement of V2X. Every phase can also be linked to the advancements in AVs since V2X will be a crucial component of AVs as described in section 1.1. All the use cases are categorized into these phases following their technical specifications and future plans for next-generation vehicles. For example, EVA is a day one use case, C-ACC is a day two, and Platooning is a day three+ as of 2022. More

information about the classification of V2X use cases into these day phases is provided in the C2C-CC roadmap [5]. Each use case can be further explained through the application's specifications, such as if the application utilizes broadcast, multicast, or unicast addressing—or single or multihop transmission, or other communication behaviors [57]. This is important to consider in order to define the security around these use cases.

### 3.1.2 Facility services layer and ITS messages

The ITS information is carried in specific messages. Which message to use depends on the purpose of the information. The purpose can then be explained with the desired use case as a reference. For example, the purpose of the EVA use case is to alert vehicles of an emergency vehicle in their vicinity. This information is distributed in a so-called single-hop Cooperative Awareness Message (CAM), and the Cooperative Awareness (CA) application generates this information which is then encapsulated in a message created by one of the associated facility services. In contrast, the Road Hazardous Warning (RHW) application generates information encapsulated in a multi-hop Decentralized Environmental Notification Messages. Examples of some primary ITS messages are shown in the figure below, together with the three use case deployment phases:

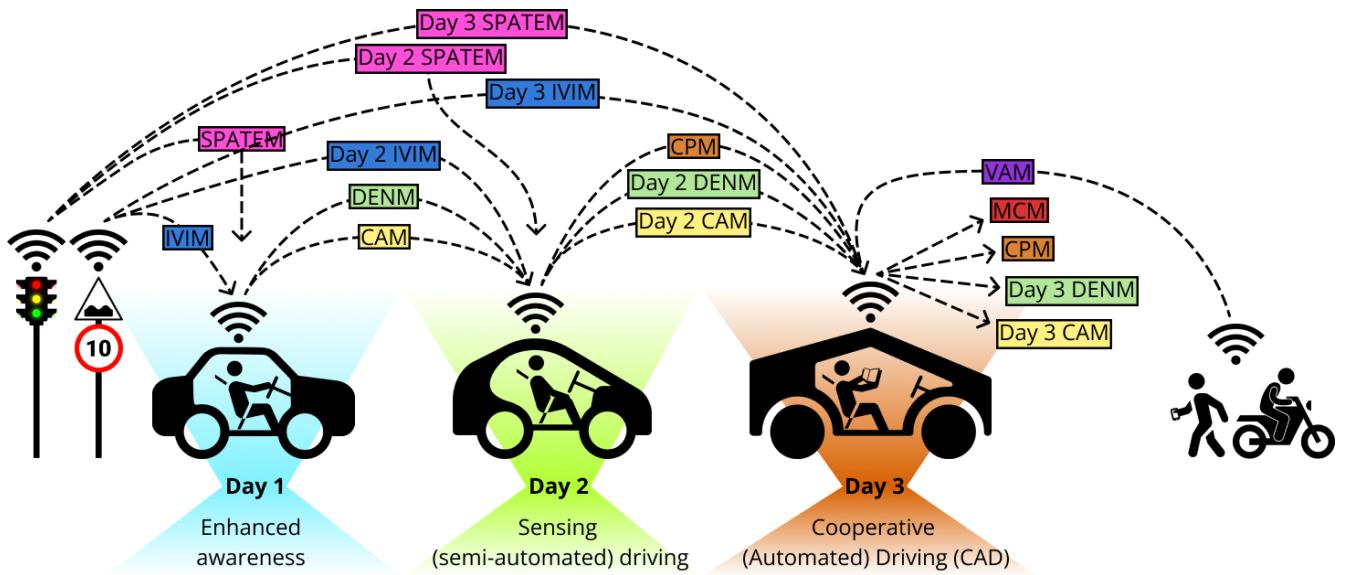


Figure 3.2: Illustrations of the three main V2X deployment phases and the automated driving functions stages mapped together.

All messages are sent within the 5.9 GHz ITS band. The respective sub-bands are dedicated to the different application classes, the ITS G5A sub-band is for road safety applications, and the ITS G5B sub-band is for traffic efficiency applications. See an illustration below for what the different sub-bands within the ITS band are currently allocated for:

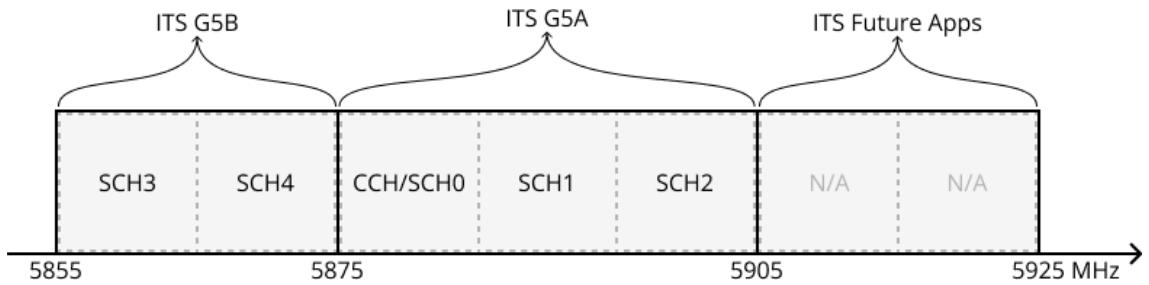


Figure 3.3: Illustration of the ITS frequency band and its respective sub-bands and channels as defined in ETSI ITS documentation [2].

Single-hop messages are always prioritized first, e.g., for the ITS G5A (the safety band), multi-hopping is not allowed in the Control Channel (CCH) and Service Channel 1 (SCH1) if they're currently congested. Then the multi-hopping can only occur in the SCH2. If the SCH2 is also congested during this time, then no multi-hopping operation is allowed for that moment. It is the same principle for the ITS G5B band; no multi-hopping is allowed if the channels are congested. The state of a channel being congested or not is determined by the Decentralized Congestion Control (DCC) [58].

More information about messages and their associated services can be found in [58].

### 3.1.3 Network and Transport layer

The GeoNetwork protocol in the ITS-S protocol stack resides in the Transport and Networking layer. The GeoNetwork protocol enables the transport of packets within the ad hoc network. It provides interoperability for the upper layer, i.e., Basic Transport Protocol (BTP), and GeoNetworking to IPv6 Adaptation Sub-Layer (GN6ASL), by carrying their respective parameters and PDUs. In the context of the GeoNetworking protocol, a PDU of the transport protocols (BTP, TCP/UDP) is referred to as Service Data Units (SDUs). The transport protocols parameters are referred to as Protocol Control Information (PCI), and the GeoNetworking PDU is simply called only GN PDU [59]. When a GN PDU is ready for transmission, it is passed to the radio access layer.

### 3.1.4 Radio Access layer

The lowest layer of the ITS-S protocol stack, the Radio Access layer, bundles the Physical- and Data Link layer of the five layer TCP/IP model, as seen in the illustration 3.1. The technology these two layers use is called ITS-G5, a radio interface that delivers Packet Data Units (PDUs) in a connectionless-type nature. The ITS-G5 technology utilizes already existing communication standards, adding features such as Decentralized Congestion Control (DCC). DCC determines the number of windows for transmission per the current load on the medium, represented as a metric called Channel Busy Ratio (CBR). The data link layer is further divided into two sub-layers; Medium Access Control (MAC) and Logical Link Control (LLC). The LLC layer distinguishes

different network-layer protocols, e.g., GeoNetworking or IPv6, while Protocol Data Unit (PDU) transmissions are scheduled in the MAC layer to once again minimize interference on the medium.

The physical- and MAC sublayer utilizes the so-called ITS-G5 interface (as referenced in the ITS standard) and supports communication at the 5,9 GHz frequency band, which is the allocated spectrum for VANETS in Europe following the IEEE 802.11-2016 standard [28]. For the ITS-G5 technology, one specific parameter is changed in the IEEE 802.11-2016 standard for disabling functionality in the MAC sublayer, allowing communication outside a Basic Service Set (BSS, a.k.a. Access Point (AP)). In more detail, the communication happens without any authentication/association procedures and security mechanisms at the MAC sublayer. These features are no longer supported when modifying the specific parameter for the 802.11. This is, in short, referred to as the 802.11p protocol version of the IEEE 802.11-2016 standard [28]. Implementing 802.11p requires that the node (in this case, the ITS-S) is configured with a predetermined frequency channel in the management plane as the frequency scanning feature for APs and network associations isn't supported by the 802.11p, and communication with other nodes won't be possible otherwise. However, this predetermined frequency channel can be an information source about other available frequency channels for the ITS-S to switch over to, transmit on, and listen to—i.e., where the actual V2X communication should occur/be present [28].

Removing these *time-consuming* security features in the MAC sublayer seems well-suited for environments with fast-shifting vehicle nodes. Otherwise, the vehicles might not have completed a transmission before being out of each other's reach. Removing the security features increases the probability of them completing their communications. But, the change isn't only beneficial; it also comes with its drawbacks of security no longer being current at the access layer [28].

Figure 3.4 shows an illustration demonstrating the difference between a traditional 802.11 network with a BSS and an 802.11p network.

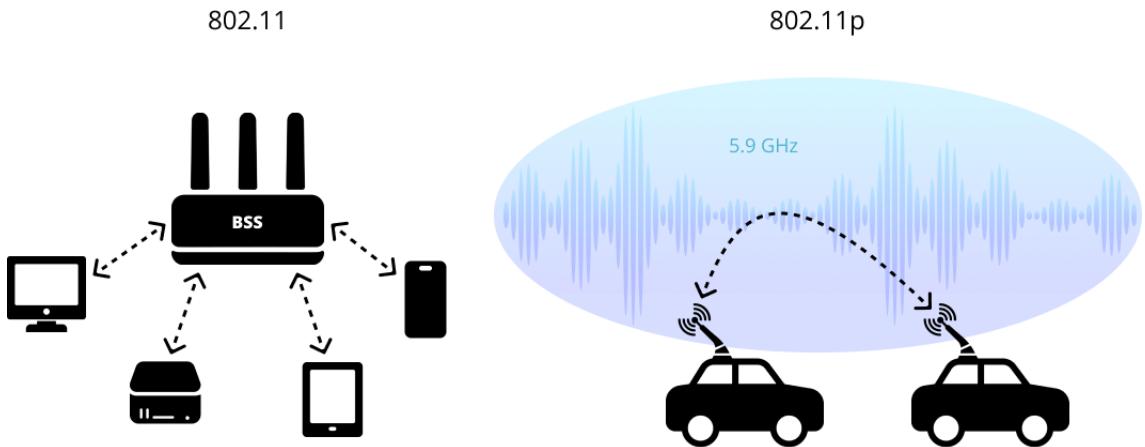


Figure 3.4: Difference between 802.11 and 802.11p.

802.11bd is an improvement on 802.11p, which purpose is to support more advanced use cases. Read more about this particular enhanced protocol in [60].

### 3.1.5 Management- and Security plane

The vertical Management and Security planes are bounded to all the horizontal layers with their respective interfaces. The management plane consists of elements that can be adjusted for certain functionality and involves processes such as mapping applications to specific interfaces (Service Access Points (SAPs)) according to a set of rules. The Security plane involves all the security management, such as intrusion detection-/prevention systems (IDS/IPS), authentication and authorization processes, and the storage of security and identity information such as crypto keys and certificates. Figure 3.1 (the ITS reference model shown at the beginning of this section) shows all the interfaces connecting the respective planes and horizontal layers. Figure 3.6 (shown at the end of this section) shows the communication flow through the respective horizontal layers and where the communication takes a detour through the security plane at each horizontal layer before continuing upwards/downwards the protocol stack. In contrast to the security plane, the management plane doesn't manage the actual communications flow but more the functionality of the horizontal layers.

## 3.2 ITS Security Architecture

For an ITS-S to communicate securely with other stations, the following security services should be supported within the ITS-S as defined in [26] and [46]. The security services can be categorized and also grouped according to—what could be referred to as—the "security entities" within the security plane, as shown in Figure 3.5 and Table 3.2.

Table 3.2: Security Services Categories

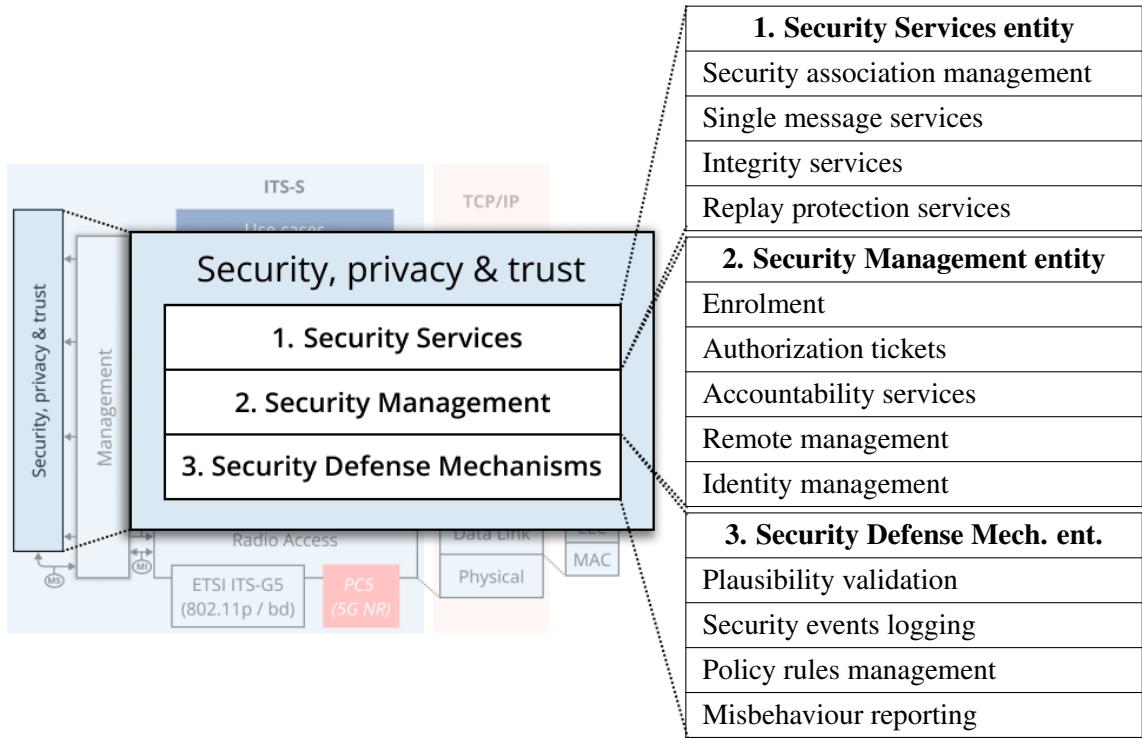


Figure 3.5: Security Entities

The security services category involves several sub-services necessary for authentic ITS-Ss and a secure ITS network. The sub-services are presented below in Tables 3.3, 3.4, and 3.5 under their respective service category.

The services presented in Table 3.3 operate within one or several layers in the ITS protocol stack while the services presented in Table 3.4 operate within the security management entity of the security plane. The services presented in Table 3.5 are additional security services operating to support the other security services or the overall security of the ITS network and infrastructure.

Table 3.3: Security Services entity

1. Security Services entity		
Service category	Service	Description
Security association management	Establish security association	The Security Association (SA) service and sub-services allow two ITS-Ss to establish secure peer-to-peer communication. Both parties shall invoke this service.
	Update security association	
	Send/receive secured messages	
	Terminate security association	
Single message services	Authorize single message	This service and its sub-services authorize single outgoing ITS messages (such as CAMs and DENMs) on the transmitter end (TX) and also validate the authorization of such incoming messages on the receivers end (RX). The authorization process involves the attachment of authorization tickets on outgoing messages and the evaluation of these authorization tickets and associated time-stamps for incoming messages. This service also provides encryption and decryption of single messages.
	Validate single message	
	Encrypt single message	
	Decrypt single message	
Integrity services	Checksum calculation	The calculate check value service operates at the transport and networking layer of the ITS protocol stack and calculates checksums for outgoing messages. The checksums are inserted into the outgoing messages, and the message's integrity is then validated on the RX side. When a certain message checksum doesn't match the RX calculation (during the validation process), the message is rejected by the RX ITS-S.
	Checksum validation	
	Checksum inclusion in outgoing messages	
Replay protection services	Timestamp data	The replay protection security services involve the inclusion of timestamps and sequence numbers into outgoing messages. The RX then validates these timestamps and numbers; if the RX does not expect a message with a certain timestamp or sequence number, it rejects the message.
	Sequence number data	

Table 3.4: Security Management entity

<b>2. Security Management entity</b>		
Service category	Service	Description
Enrolment	Obtain enrolment credentials	This service and its sub-services let an ITS-S request and obtain enrollment credentials from an Enrollment Authority (EA). The enrollment procedure is initiated by a vehicle when it detects the need for new enrollment credentials or enters a new ITS infrastructure area (also called enrollment domain, where credentials from a specific EA only are valid). When an ITS-S requests enrollment credentials from the ITS infrastructure, the EA first verifies the identity of the ITS-S by looking at the associated canonical identity (a unique identifier that can—in straightforward networking terms—be compared to a MAC address). The ITS-S encrypts the request with the EA public key, so the EA decrypts the request and further verifies the ITS-S identity by validating that the request has been correctly signed with a certain cryptographic key (called the ITS-S key stored in the security management entity, see Figure 3.6). The authentication process also involves a certain network challenge the ITS-S has to perform. The OEM provides both the ITS-S's canonical identity and the key. The EA sends an encrypted response containing the enrollment credentials if the authentication process is successful. The response is encrypted with the associated public key to the ITS-S key and signed with the associated private key to the EA key. The ITS-S then uses the enrollment credentials as certificates and temporary identities for pseudonymously requesting and being authorized to receive specific tickets from the ITS infrastructure. These tickets are required for ITS-Ss to communicate securely and pseudonymously with each other within the network (see next service; Authorization Tickets). If the authentication process is unsuccessful, the ITS-S isn't authorized and cannot communicate within the ITS infrastructure. Enrollment credentials can be removed from an ITS-S by the ITS infrastructure, making it no longer authorized to communicate within the network. This requires cooperation between the EA and the Authorization Authority (AA) to keep certain repositories updated (see next service; Authorization Tickets) so all ITS-Ss know the current authorization status information and no longer communicate with removed ITS-Ss.
	Update enrolment credentials	
	Remove enrolment credentials	

*Continued on next page*

Table 3.4 – *Continued from previous page*

<b>2. Security Management entity</b>		
Service category	Service	Description
Authorization tickets	Obtain tickets	The authorization tickets (a-tickets) are necessary for trustworthiness and privacy-protected communication within the ITS network. A-tickets are temporary authorization parameters and are used by ITS-Ss for signing their ITS messages. Certain a-tickets exist for particular ITS services, i.e., one ITS-S can be authorized to only use particular services according to its set of a-tickets. The tickets don't include any permanent ITS-S identifiers, such as canonical identifiers, making the communication pseudonymous between the ITS-Ss. Obtaining a-tickets from the AA is relatively similar to obtaining enrollment certificates from the EA. The request is encrypted with an AA key and cryptographically signed with the ITS-S key. The request procedure begins when an ITS-S is empty or has consumed its previous set of such tickets. The ITS-S then sends a request to the ITS infrastructure and receives a set of a-tickets from the Authorization Authority (AA) if the ITS-S temporary identity and its authorization can be validated. The ITS-S temporary identity and its given authorization rely upon the previously allocated enrollment certificates. If an enrollment certificate is not valid, or if the ITS-S identity cannot be validated, an ITS-S is not given any a-tickets. The publish authorization status and update local authorization status repository services work in relation to each other. The publish authorization status allows the ITS infrastructure to require a certain ITS-S to re-authorize itself by request from another ITS-S or an authoritative entity within the ITS infrastructure. This is done to reassure that all ITS-Ss are authentic and that no ITS-Ss are misbehaving in the network. The update local authorization status repository service lets an ITS-S update a local repository consisting of such authorization information previously mentioned. This is an important feature when ITS-Ss don't have access to the ITS infrastructure but still need the option for verifying an ITS message authenticity.
	Update tickets	
	Publish authorization status	
	Update local authorization status repository	
Accountability services	Record incoming message in audit log	The accountability services' purpose is to record incoming and outgoing messages for log auditing so that certain ITS-Ss can be held accountable for the messages they receive and send. This service may support the repudiation aspect of the security objectives.
	Record outgoing message in audit log	

*Continued on next page*

Table 3.4 – *Continued from previous page*

<b>2. Security Management entity</b>		
Service category	Service	Description
Remote management	Remote activate ITS transmission	The remote management service consists of two sub-services used when a certain ITS-S misbehaves or malfunctions. The two remote services can then be used by authoritative entities within the ITS infrastructure to deactivate or restart the certain ITS-S ability to transmit ITS messages. The services also allow the authoritative entities to re-initiate the transmission service for an ITS-S that already has it deactivated. The service uses the temporary identity to target the concerned ITS-S. The remote management communication between the ITS-S and the authoritative entity is encrypted with the ITS-S key and signed with an ITS infrastructure authoritative key.
	Remote deactivate ITS transmission	
Identity management	Subscribe ID change notif.	These services involve features for the security credentials stored within the ITS-S, and also for the ITS-S identifiers, such as station ID (Facility layer), network ID (Network & Transport layer), and MAC address (Access layer) [61].
	Unsubscribe ID change notif.	
	ID change notification	
	Trigger ID change	
	Lock ID change	
	Unlock ID change	

Table 3.5: Security Defense Mechanisms entity

<b>3. Security Defense Mechanisms entity</b>		
Service category	Service	Description
Plausibility validation	Validate data plausibility	This service validates an ITS message authenticity and if the data it contains can be trusted. An ITS-S utilizes the service when a message is received; the ITS-S compares the data within the message to other recently retrieved traffic status information from other sources to decide if it's trustworthy according to its plausibility. It looks specifically to associated timestamps vs. time-of-day, GPS information vs. geographical position, vehicle speed, and directions.
Security events logging	Log misbehaviour detection information	This service lets an ITS-S log current suspected misbehaving activity within the ITS network. The Misbehaviour Reporting service then reports this information to the ITS infrastructure (see below).
Policy rules management	Configure security policy rules	This service enables the configuration of local security policy rules for misbehavior detection. Regular updates for these rules protect the network from misbehavior activity with a higher probability of the activity being detected.
Misbehaviour reporting	Report misbehaviour	This service is used for ITS-Ss to report suspicious activity within the ITS network to the ITS infrastructure (e.g., a misbehaving ITS-S). The reporting requires an a-ticket for an ITS-S to be able to send information to the ITS infrastructure so that an authoritative entity responsible for the misbehavior administration can process the data.

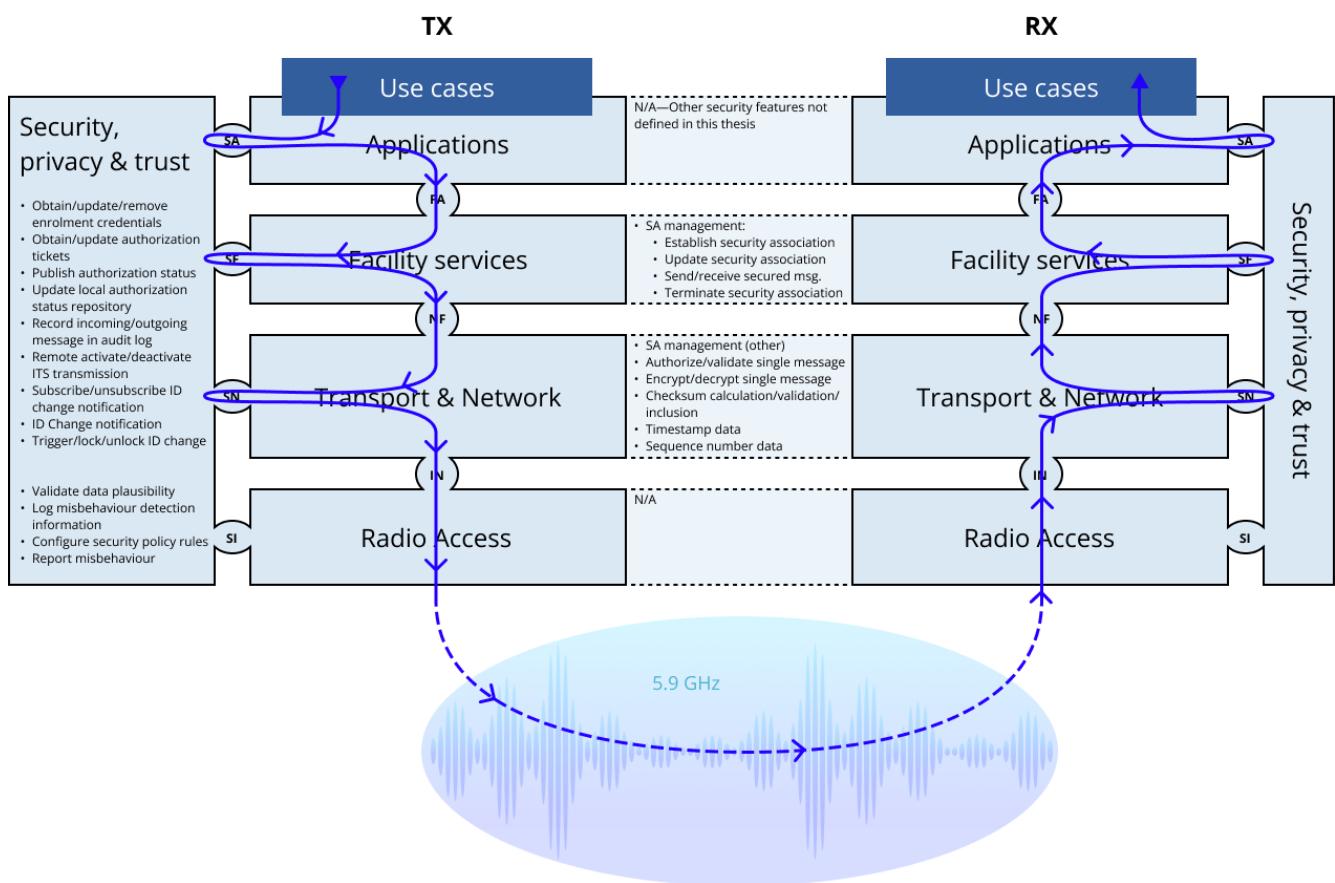


Figure 3.6: Illustration showing where different security services operate within the ITS reference model.

# Chapter 4

## Result & Analysis

Below, the results for the research questions of this thesis will be presented, i.e. (1) *What are some significant use cases of V2X-short range?*, and (2) *What cybersecurity risks can be associated with the use cases?*

To answer question 1; the interview results will be analyzed, leading to the desired set of significant use cases. This will then be presented in both a table and by the interview candidates' motivations in the form of citations.

To answer question 2; a ToE will be defined with four of the use cases in focus, a risk assessment will then be performed on these use cases, both to demonstrate the TVRA method but also to establish what risks that are associated with these use cases.

### 4.1 *What are some significant use cases of V2X short-range?*

As for the task—when each interview candidate was to pick use cases from the list within the C2C-CC roadmap [5] given a particular question (see section 2.3.1)—the distribution of the candidate's selection of use cases became according to Figure 4.1, and the use cases each candidate picked are presented in Table 4.1. The total number of chosen use cases ended in 35. Also, use cases are sorted in descending order according to how they were chosen, and the least chosen use cases are marked in grey. The non-grey use cases are the ones that are considered significant for this thesis and ended up over a certain threshold value. The ones that are marked in blue are the use cases used as input for the second research question—i.e., as the ToE according to section 1.5.1.

**NOTE:** The threshold value(s) were calculated by dividing the total number of the interview candidates' permitted number to pick use cases (i.e., 5 candidates  $\times$  4 picks = 20) with the total number of use cases for each deployment phase in the C2C-CC roadmap. An example is given

below:

$$20 \text{ picks} / 15 \text{ use cases} = 1.333$$

Since a use case can't be picked 1.333 times, the number is rounded up to 2. This means that for deployment phases 2 and 3 (which contains 15 and 16 use cases, respectively, in the C2C-CC roadmap), a use case has to be picked at least three times to be considered significant for this thesis since two times might have occurred because of a larger coincidence. Deployment phase 1 is different since this contains 36 use cases within the C2C-CC roadmap.

$$20 \text{ picks} / 36 \text{ use cases} = 0.555$$

Figure 4.1: Chart of use case occurrences according to the interview candidates' selections. The table is color-coded. Red: use cases within day-phase 3; Green: use cases within day-phase 2; Blue: use cases within day-phase 1.

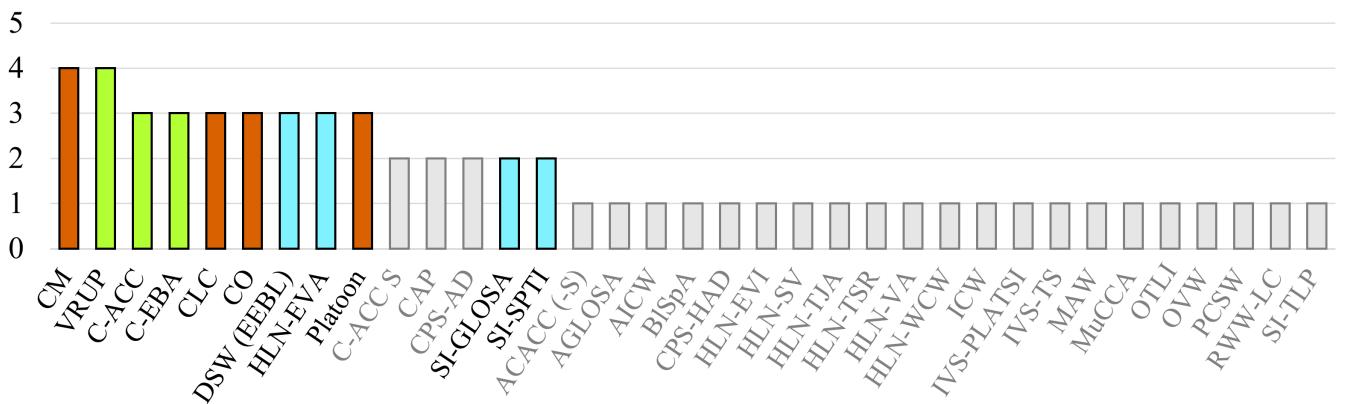


Table 4.1: A presentation of all the use cases chosen by the interview candidates. The use cases are presented with their respective abbreviation and are referred to as "use case codes." The full description of each use case is written out in the Description column. Each use case is also tagged with its associated day phase, e.g., Cooperative Merging Assistance (CM) is a day 3 use case. The table is color-coded by Red: use cases within day-phase 3; Green: use cases within day-phase 2; Blue: use cases within day-phase 1.

Nº	Use case code	Day	Description	IC1	IC2	IC3	IC4	IC5
1	CM	3	Cooperative Merging Assistance	✓		✓	✓	✓
2	VRUP	2	Vulnerable Road User Protection		✓	✓	✓	✓
3	C-ACC	2	Cooperative Adaptive Cruise Control	✓	✓			✓
4	C-EBA	2	Cooperative Emergency Brake Assistance	✓	✓	✓		
5	CLC	3	Cooperative Lane Change	✓		✓	✓	
6	CO	3	Cooperative Overtaking	✓		✓		✓

*Continued on next page*

Table 4.1 – *Continued from previous page*

Nº	Use case code	Day	Description	IC1	IC2	IC3	IC4	IC5
7	DSW (EEBL)	1	Dangerous Situation Warning <small>Emergency ELEC. Brake Light</small>			✓	✓	✓
8	HLN-EVA	1	Hazardous Location Notif. <small>Emergency Vehicle Approaching</small>			✓	✓	✓
9	Platoon	3	Vehicle platooning	✓			✓	✓
10	C-ACC S	2	Cooperative Adaptive Cruise Control String	✓		✓		
11	CAP	3	Cooperative Automated Parking			✓		✓
12	CPS-AD	2	Collective Perception Service for AD			✓	✓	
13	GLOSA	1	Green Light Optimum Speed Advisory	✓	✓			
14	SPTI	1	Signal Phase and Timing Information		✓	✓		
15	ACACC (-S)	3	Advanced Cooperative ACC (String)		✓			
16	AGLOSA	3	Autom. Green Light Optimum Speed Advisory				✓	
17	AICW	2	Advanced Intersection Collision Warning		✓			
18	BlSpA	2	Blind Spot Assistant					✓
19	CPS-HAD	3	Collective Perception Service for Highly AD		✓			
20	HLN-EVI	1	Emergency Vehicle in Intervention		✓			
21	HLN-SV	1	Stationary Vehicle					✓
22	HLN-TJA	1	Traffic Jam Ahead					✓
23	HLN-TSR	1	Temporarily slippery road		✓			
24	HLN-VA	2	Vehicle Assistance					✓
25	HLN-WCW	1	Weather Condition Warning				✓	
26	ICW	1	Intersection Collision Warning			✓		
27	IVS-PLATSI	2	Platoon Support Information	✓				
28	IVS-TS	1	Traffic Signs	✓				
29	MAW	2	Motorcycle Approaching Warning or Protection				✓	
30	MuCCA	3	Multi-Car Collision Avoidance		✓			
31	OTLI	3	Optimized Traffic Light Information with V2I		✓			
32	OVW	2	Overtaking Vehicle Warning					✓
33	PCSW	1	Pre-crash Sensing Warning	✓				
34	RWW-LC	1	Road Works Warning Lane Closure				✓	
35	SI-TLP	1	Traffic Light Prioritisation	✓				

#### 4.1.1 The motive behind the candidates' choices

##### 4.1.1.1 Day one use cases

If starting with safety aspects, the candidates see great opportunities to prevent unnecessary accidents with these day one use cases they've chosen. For example, EEBL (Emergency Electronic Brake Light) will provide drivers with a warning on their dashboard when a vehicle in front of them brakes hard. The warning is directly sent out when the braking is performed by the vehicle

ahead, and the driver behind can act on this warning without not even having sight of the car that's braking, thus not protected by the on-board sensors:

Citation 4.1

Data extract	Coded for	Ref.
<i>"EEBL because it will be a very good function from a safety perspective when our on board sensors can not detect when the car further ahead the car you have right in front of you does a panic brake, your sensors you have today can not detect it, and it is a very high risk that the car in front of you makes a cross brake that you react too late on"</i>	• EEBL	Trx: IC3 Row: 101

But all the use cases essentially have the same purpose, to provide the driver with a warning about something potentially dangerous that the driver can then plan around. Considering this, other motives than only the safety aspect of why the candidates chose as they did are investigation below. In short, it was partly according to these reasons:

1. Usability
2. Centralization
3. Certain attention
4. Already implemented
5. Well-defined in standards
6. Driver comfort/conv.

It turned out that the candidates choose already implemented use cases, such as use cases that Volkswagen has introduced into some of their models. This was confirmed by IC4:

Citation 4.2

Data extract	Coded for	Ref.
<i>"it is difficult not to talk about the things that are actually already implemented by, for example, Volkswagen"</i>	• Already implemented	Trx: IC4 Row: 113

These use cases are now rather known for how they work, and they are currently well-defined in the standards compared to other use cases. If taking EEBL as an example once more, it has already been implemented by Volkswagen and is well-specified in certain standards:

## Citation 4.3

Data extract	Coded for	Ref.
<i>"It is definitely included, because it is such a use case which, partly it is implemented by Volkswagen and it is well specified by Car-2-Car and it is a very common use case example when talking to people about this, such as OEMs and tier one suppliers, EEBL are always in those discussions"</i>	<ul style="list-style-type: none"> <li>• Already implemented</li> <li>• Certain attention</li> <li>• EEBL</li> <li>• Well-defined</li> </ul>	Trx: IC4 Row: 119

Another example is also the use cases involving Hazardous Location Notifications, such as Weather Condition Warning or other similar use cases:

## Citation 4.4

Data extract	Coded for	Ref.
<i>"weather condition, well specified by Car-2-Car, such as triggering conditions are clear, there are many who talk about this use case, it is useful"</i>	<ul style="list-style-type: none"> <li>• Certain attention</li> <li>• Well-defined</li> </ul>	Trx: IC4 Row: 198

Then there is the centralization aspect, which IC2 focused on mainly. It may be more in demand for OEMs to implement V2X into their cars if the infrastructure already has it. And since the infrastructure is centralized, it may be these so-called Road Side Units (RSU) that will be the first ones actually to adopt V2X on a big scale:

## Citation 4.5

Data extract	Coded for	Ref.
<i>"my logic is that day one use cases to V2X technology is not so mature, and there's a low market penetration which means that it is not so many cars equipped with this V2X yet, and then I prefer the I2V, these kinds of use cases since the infrastructure is somehow centralized"</i>	<ul style="list-style-type: none"> <li>• Centralization</li> </ul>	Trx: IC2 Row: 117

But not only RSU are centralized, but Emergency Vehicles are also centralized, and therefore may Emergency Vehicle Approaching be a use case appropriate for being implemented on a big scale in an early phase. It has already even been implemented by Volkswagen as “emergency service vehicles” alert, which is a so-called sub-cause code to their “traffic hazard alert function” [62]. So, this is a use case with a high probability of being implemented into other OEMs vehicles as well:

Citation 4.6

Data extract	Coded for	Ref.
<i>"emergency vehicle approaching ... it is implemented and is rolled out by Volkswagen, it is well specified both by CRoads and by Car-2-Car"</i>	<ul style="list-style-type: none"> <li>• Already implemented</li> <li>• Emergency vehicle</li> <li>• Well-defined</li> </ul>	Trx: IC4 Row: 189

Citation 4.7

Data extract	Coded for	Ref.
<i>"emergency vehicle that we also think could be the first day one, the first type of cars to equip this V2X, because like ambulance, and different emergency vehicles they are centralized"</i>	<ul style="list-style-type: none"> <li>• Centralization</li> <li>• Emergency vehicle</li> </ul>	Trx: IC2 Row: 121

Emergency Vehicle Approaching is a typical use case that shows the power of V2X communication. This use case can be used both for short- and long-range communication and will inform the driver if there's an emergency vehicle in the area. It is essential to receive this information in the cockpit since the driver might listen to music or talk on the phone when on the highway and not pay full attention to any outer notices such as light signals and sirens.

Citation 4.8

Data extract	Coded for	Ref.
<i>"I have a hard time imagining that they would like to put it in the cloud in a database, do you run it locally, like when they turn on the sirens they also turn on an ITS-G5 transmitter or C-V2X transmitter at the same time"</i>	<ul style="list-style-type: none"> <li>• Emergency vehicle</li> </ul>	Trx: IC3 Row: 111

Lastly, for day one use cases, there was also some focus on the driver's comfort or conveniences, such as the Signal Phase and Timing Information (SPTI) use case, which both IC2 and IC3 chose. It should be mentioned, though, that this use case also includes safety aspects, but where the focus from the candidates still partly were on customer functions:

Citation 4.9

Data extract	Coded for	Ref.
<i>"It's more of a good customer function, when you stand at the red light it's nice, I experience that it would have been nice to know if there are 5 seconds left or if there are 30 seconds left before it turns green"</i>	• Driver comfort/conv.	Trx: IC3 Row: 139

#### 4.1.1.2 Day two use cases

For day two use cases, if not considering the safety aspect or the already mentioned reasons as in day one, then the following were new reasons why the candidates chose the day two use cases that they did:

1. Low risk
2. Efficiency
3. VRU protection
4. Action upon information
5. Sensor info sharing

Now automation is becoming more current, which is reflected in the candidate's choices and their reasons for these choices. This is not unexpected either since the day one use cases are only notification functions, something IC5 remarks:

Citation 4.10

Data extract	Coded for	Ref.
<i>"And it is quite clear if you look at the use case, the day one use case is a completely informative use case for the driver in a normal car"</i>	• Low risk	Trx: IC5 Row: 77

In contrast, the later phase use cases involve features that support more and more automation. For example, Advanced Driver Assistance Systems (ADAS) has only been controlled by onboard sensors earlier. But now, when V2X is getting more developed, functions like these can use this V2X as an additional source of information. When entering the day two use case phase, the vehicles will now start to use the V2X to act upon the data sent over the network. This is something IC1 reflects around:

Citation 4.11

Data extract	Coded for	Ref.
<i>"if we send a notification or a signal to a car and inform them of something that is happening in the area, it is important, but it is also more important if we use this information"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> <li>• Sensor info sharing</li> </ul>	Trx: IC1 Row: 77

Cooperative Emergency Brake Assistance is an excellent example of an automation function that can use V2X information; vehicles brake systematically in real-time as soon as a vehicle in front brakes:

Citation 4.12

Data extract	Coded for	Ref.
<i>"cooperative emergency brake assistance that we actually not only send information but also brake on such a message"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> </ul>	Trx: IC1 Row: 163

Another advanced automation function in modern cars today is Adaptive Cruise Control (ACC). IC4 reflects around this technology to be also controlled partly by V2X:

Citation 4.13

Data extract	Coded for	Ref.
<i>"If this technology is actually going to control the car's behavior then it feels like this is a fairly obvious and quite simple case to implement because the base bolts already exist, most cars have some type of ACC but based on radar or other sensors, then adding V2X as an additional information carrier or as an additional sensor into this feels like a fairly simple and fairly low risk"</i>	<ul style="list-style-type: none"> <li>• ACC</li> <li>• Acting upon info</li> <li>• Already implemented</li> <li>• Low risk</li> </ul>	Trx: IC4 Row: 331

What IC4 means with the low risk is that vehicles nowadays, as IC4 mentions, use several onboard sensors with sensor fusion to decide how to act in certain situations upon the information mass they receive from their various sensors. Adding another information source to this sensor fusion system seems like reasonably low risk of affecting something negatively and thus improving redundancy. The ACC will only get more information that strengthens the sensor fusion's decision performance.

## Citation 4.14

Data extract	Coded for	Ref.
<i>"You add another source of information or another sensor to a functionality that already exists and that people are already familiar with"</i>	<ul style="list-style-type: none"> <li>• Certain attention</li> <li>• Driver comfort/conv.</li> <li>• Low risk</li> </ul>	Trx: IC4 Row: 337

In a day two use case scenario, one function of this ACC might be the ACC String. Today the ACC locks the cruise on the vehicle in front. But in an ACC String scenario, the vehicle that is going to cruise may also involve V2X communication to lock the cruise behind a string of vehicles. Then these vehicles can share their future actions, creating a series of flowing and communicating vehicles.

## Citation 4.15

Data extract	Coded for	Ref.
<i>"the ACC today, you lock it on the first car but if you can lock an entire train and get even better flow in traffic"</i>	<ul style="list-style-type: none"> <li>• ACC</li> <li>• Efficiency</li> </ul>	Trx: IC3 Row: 161

Use cases that also involve that the entities in the network shares not only their position, speed, and plans but also their onboard sensor information were prioritized by the candidates:

## Citation 4.16

Data extract	Coded for	Ref.
<i>"That we actually start exchanging information if I see with my radar objects that maybe other cars do not see with their radar, for example children who run behind a bus or something, it is very good that you send out that information and then they get that information"</i>	<ul style="list-style-type: none"> <li>• Sensor info sharing</li> <li>• VRU protection</li> </ul>	Trx: IC3 Row: 165

## Citation 4.17

Data extract	Coded for	Ref.
<i>"If I have a radar sensor that detects something on the road in front of me, a pedestrian going out into the street, or something that is in the way, then I can send that information to cars around"</i>	<ul style="list-style-type: none"> <li>• Sensor info sharing</li> <li>• VRU protection</li> </ul>	Trx: IC3 Row: 370

Citation 4.18

Data extract	Coded for	Ref.
<i>"This is quite important for these self-driving cars which today rely entirely on, for example, camera sensors"</i>	<ul style="list-style-type: none"> <li>• Sensor info sharing</li> </ul>	Trx: IC4 Row: 378

This is very important that this functionality becomes a reality since automated cars today only rely on their onboard sensors. When use cases such as Collective Perception Service for AD are introduced, automated vehicles will increase their action response time. Having a stable communication base before vehicles are presented with more and more automation functionalities is crucial, something that IC5 reflects on:

Citation 4.19

Data extract	Coded for	Ref.
<i>"everyone who works in automotive is pretty much in agreement, I think, that autonomous vehicles will not work with line of sight sensors, over time, but you will have to communicate in some way between vehicles and express intentions between vehicles, and we work very hard on autonomous vehicles today in a silo, and then we work in another silo with V2X communication, and I think you need to build maturity in the communication silo before you reach the same level in the autonomous silo so to speak, you can not like, there are two problems that you should not solve at the same time but you should have a stable as well as, a stable communication platform first and then you can add autonomy"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> <li>• Sensor info sharing</li> </ul>	Trx: IC5 Row: 62

Lastly, for day two use cases, the candidates focused on more vulnerable entities in traffic:

Citation 4.20

Data extract	Coded for	Ref.
<i>"it is also such a use case you talk a lot about, so how do we get other than, in the first place we talk about cars, in the second place motorcycles, but then we have all these others who cycle and those who walks"</i>	<ul style="list-style-type: none"> <li>• Certain attention</li> <li>• VRU protection</li> </ul>	Trx: IC4 Row: 415

These are use cases such as Motorcycle Approaching Warning or Protection and Vulnerable Road User Protection (VRUP). These two use cases will undoubtedly be a groundbreaking functionality if dangerous traffic-related situations could be avoided for more vulnerable entities such as motorcyclists, cyclists, and pedestrians:

Citation 4.21

Data extract	Coded for	Ref.
<i>"it would be very good if it worked that we can warn pedestrians and cyclists"</i>	• VRU protection	Trx: IC3 Row: 186

Citation 4.22

Data extract	Coded for	Ref.
<i>"it is a very important use case for two wheels, it is probably the most important use case for two wheels"</i>	• VRU protection	Trx: IC4 Row: 397

But even though VRUP exists as a day two use case in the C2C-CC roadmap, this use case seems relatively far away. The problem is the positioning; vehicles should only be warned if, for example, a pedestrian walks out on the road, not if the person walks on the sidewalk. This is challenging since this requires a very accurate positioning that does not seem possible today if considering V2X functionality in mobile phones as an example. This would also be a big privacy question to deal with as well. But there are other ways to protect VRUs, such as with Road Side Units (RSUs):

Citation 4.23

Data extract	Coded for	Ref.
<i>"the second possibility is that you have sensors in im- portant places, ie typically road junctions, pedestrian crossings, which register that there are people near a pedestrian crossing and thus send out warnings"</i>	• Certain attention • VRU protection	Trx: IC4 Row: 418

This will warn vehicles about VRUs, but unfortunately, VRUs can't receive any more warnings than the RSUs can provide.

#### 4.1.1.3 Day three use cases

There were three new noticeable reasons why the candidates chose their day three use cases, these were:

1. Suitable combination

2. Environm. benefits
3. Money- and timesaving

But this is also not so unexpected since these day three use cases are planned to involve more automation. This means that they chose use cases that seem to be needed together or that their functionality is most useful when used together. An example is the following four use cases with very important purposes:

- Cooperative lane change
- Co-operative merging assistance
- Platooning
- Cooperative overtaking

Citation 4.24

Data extract	Coded for	Ref.
<i>"Platooning is the same thing and overtaking, emerging, and cooperative lane change, they are important decisions"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> <li>• Efficiency</li> <li>• Sensor info sharing</li> <li>• Suitable combination</li> </ul>	Trx: IC1 Row: 111

They all work individually, but the driving is optimized if used together. By then, the vehicles are probably classified as fully autonomous (according to SAE):

Citation 4.25

Data extract	Coded for	Ref.
<i>"all three use cases work separately, but it gets really good when you have them together"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> <li>• Sensor info sharing</li> <li>• Suitable combination</li> </ul>	Trx: IC4 Row: 473

## Citation 4.26

Data extract	Coded for	Ref.
<i>"Platooning is good for itself, but for it to work really well, then you also need the other two services, i.e., that it should work even when you come to an intersection or entrance, or an exit where other cars should be able to enter the road and automatically merge, either in a platoon, or that you split a platoon and take in another car in between"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> <li>• Efficiency</li> <li>• Sensor info sharing</li> <li>• Suitable combination</li> </ul>	Trx: IC4 Row: 466

## Citation 4.27

Data extract	Coded for	Ref.
<i>"a self-driving car needs to be able to make lane changes, exchange information, handle entrances and exits and have a collaboration there, and then also be able to make overtaking of a truck or another car"</i>	<ul style="list-style-type: none"> <li>• Acting upon info</li> <li>• Efficiency</li> <li>• Sensor info sharing</li> <li>• Suitable combination</li> </ul>	Trx: IC3 Row: 258

For the environmental, money- and timesaving part, these are some of the reflections from the candidates:

## Citation 4.28

Data extract	Coded for	Ref.
<i>"platooning in itself it is a great use case especially for trucks to save fuel and to get a more efficient transport chain, and if you look at the longer term, it is also for the drivers, that you can save quite a lot of personnel costs, and time , that those sitting in the vehicles further back in the platoon probably do not even need to hold the steering wheel but they can use it as rest time, so there is quite a lot of money to save on it"</i>	<ul style="list-style-type: none"> <li>• Driver comfort/conv.</li> <li>• Efficiency</li> <li>• Money- and timesaving</li> </ul>	Trx: IC4 Row: 461

Citation 4.29

Data extract	Coded for	Ref.
<p><i>"There is also huge money to be saved, and Environm. benefits of course, that is also a part, we live in a more sustainability-conscious society and the opportunity to platoon vehicles, I think, is an important part"</i></p>	<ul style="list-style-type: none"> <li>• Environm. benefits</li> <li>• Money- and timesaving</li> </ul>	Trx: IC5 Row: 197

Citation 4.30

Data extract	Coded for	Ref.
<p><i>"From a societal perspective so, parking damages costs a lot of money, it is expensive with parking damages, so if you are going to start saving money as well on this, and get that part involved, it is probably not such a dumb idea to have that, because in a parking lot you would probably be able to automate the parking procedure"</i></p>	<ul style="list-style-type: none"> <li>• Efficiency</li> <li>• Money- and timesaving</li> </ul>	Trx: IC5 Row: 188

Citation 4.31

Data extract	Coded for	Ref.
<p><i>"Cooperative automated parking I think will be a fantastic customer function, because you arrive at, go into town, there will be fewer and fewer parking spaces and then you can just jump out of the car and it drives and parks itself"</i></p>	<ul style="list-style-type: none"> <li>• Driver comfort/conv.</li> <li>• Efficiency</li> </ul>	Trx: IC3 Row: 233

Citation 4.32

Data extract	Coded for	Ref.
<p><i>"GLOSA is actually a fairly important use case for day one as well, but maybe it gets even more interesting when you actually start automatically control vehicles at a good speed to lead them through an intersection or through a series of intersections, then you can save a lot of fuel, and get a better traffic environment in general"</i></p>	<ul style="list-style-type: none"> <li>• Efficiency</li> <li>• Environm. benefits</li> <li>• Money- and timesaving</li> </ul>	Trx: IC4 Row: 446

## 4.2 What cybersecurity risks can be associated with these use cases?

This section performs the risk assessment according to the TVRA method as described in section 2.5. Below, Target and Evaluation (ToE) will be defined upon the four day one use cases selected by the interview candidates.

### 4.2.1 Target of Evaluation (ToE)

1. Dangerous Situation Warning—Emergency Electronic Brake Light (DSW-EEBL)
  - This use case has already been described in section 1.1.5. Still, in short, it enables any vehicle to disseminate an alert to its local followers when performing a hard brake [5].
2. Hazardous Location Notification—Emergency Vehicle Approaching (HLN-EVA)
  - This use case has also already been described in section 1.1.5. In short, this use case lets an active emergency vehicle disseminate a warning about its presence to local vehicles so they can create a corridor for the emergency vehicle in time if necessary [5].
3. Green Light Optimum Speed Advisory (GLOSA)
  - This use case has also already been described in section 1.1.5. In short, this use case lets an RSU—or more specifically, an intelligent traffic light—disseminate information about the most effective speed for efficiently approaching a traffic light that's about to turn green (or red) [5].
4. Signal Phase and Timing Information (SPTI)
  - This use case hasn't been described before, but it is very similar to GLOSA. The use cases differ on some minor points, but in general, and for this thesis, SPTI and GLOSA can be described as working in harmony with each other [58].

**NOTE:** The rest of the use cases are left out from this thesis risk assessment. Instead, other researchers within the automotive cybersecurity community are encouraged to use these as future research directions. Read more about this decision and why this is relevant in section 1.5.3.

Further definitions are required to analyze these day-one use cases, or the ToE scope, for related risks. For this, two things need to be done. First, a diagram with the use case characteristics must be set up. Then, assumptions must be made about these use case characteristics following their current and supposed functionality.

#### 4.2.1.1 ToE Definition

Precise definitions of the scope are required for a TVRA to be successful. Therefore, the so-called ToE needs to be defined in a realtive straightforward way to be able to identify its assets in step 4 of the TVRA process effectively. ToE can be defined as where exposed interfaces exist for a system. Therefore this also includes the environment in which the system is applied, referred to as the *ToE environment*. The ToE should also be considered as a “system under standardization.” The goal is to describe the ToE and ToE environment in a higher level of abstraction (an overview) as support to further analysis of its characteristics in the following steps 2 and 3 to later on, in step 4, decompose the associated assets related to the ToE. Some practical steps that can be performed for defining the ToE are diagrams that summarize the ToE characteristics. An UML model of the ToE can also be created with the support of these diagrams. Then, with the backing of these diagrams and model, the ToE’s basic architecture, interfaces, and information flows can be determined. Further, following this information, attack surfaces<sup>1</sup> can also be discovered. The recent guidelines are now considered, and diagrams (Table 4.2 and 4.3) for the use cases has been created below. It summarizes the use cases applications, services and their message formats, and lastly behavioral communication patterns.

#### 4.2.1.2 ToE Characteristics

DSW-EEBL and HLN-EVA are enabled by different applications, namely Road Hazardous Warning (RHW) and Cooperative Awareness (CA). They also take advantage of different message formats. The service providing the DENM message, which the RHW application utilizes, is only called—in reference to the message name itself—Decentralized Environmental Notification (DEN) service [58]. The service providing the CAM message is called the same as the application that utilizes the messages, i.e., the Cooperative Awareness (CA) service [58].

GLOSA and SPTI utilize the same application (thus also the same services and messaging formats), namely Cooperative Speed Management (CSM) [46].

Se mapping between use case, application, service, and message below:

---

<sup>1</sup>Attack surfaces are a potential point within the system or its environment for an attack to be carried out towards the system.

Table 4.2: ToE service specification.

ToE Use case)	Application	Service	Message
DSW-EEBL	Road Hazardous Warning (RHW)	Decentralized Environmental Notification (DEN)	DENM
HLN-EVA	Cooperative Awareness (CA)	Cooperative Awareness (CA)	CAM
GLOSA	Cooperative Speed Management (CSM)	Traffic Light Maneuver (TLM) Road and Lane Topology (RLT)	SPATEM MAPEM
SPTI	Cooperative Navigation (CN)	Traffic Light Maneuver (TLM) Road and Lane Topology (RLT)	SPATEM MAPEM

All the use cases use broadcast addressing. DSW-EEBL and HLN-EVA are V2V dissemination, while GLOSA and SPTI are I2V dissemination. All the use cases use the 5.9 GHz ITS band, and the 5875-5905 MHz (ITS G5A) sub-band since all four use cases are for safety purposes. GLOSA's and SPTI's purposes can also be considered for efficiency and, thus, might occupy the 5855-5875 MHz (ITS G5B) sub-band if the ITS G5A is congested. I.e., DSW-EEBL, HLN-EVA, GLOSA, and SPTI can all be classified as road safety use cases, while GLOSA and SPTI also are used for efficiency.

HLN-EVA and SPTI are single-hop and are therefore more prioritized than DSW (EEBL) in congested situations (read more about this in section 3.1.2). The same is true for GLOSA, but since this use case is not safety classified, it is neither critical if it can't operate due to congested channels. None of the use cases establishes a session with another node. See summarization of this information below:

Table 4.3: ToE characteristics and behavioral communication patterns.

ToE (Use case)	Behavioral communication patterns					
	Addressing	Direction	Frequency		Hops	Session
			GHz	MHz		
DSW-EEBL	Broadcast	V2V	5.9	5875-5905	Multi	No
HLN-EVA	Broadcast	V2V	5.9	5875-5905	Single	No
GLOSA	Broadcast	I2V	5.9	5855-5875	Multi	No
SPTI	Broadcast	I2V	5.9	5875-5905	Single	No

The following UML model can be created by examining the diagrams above.

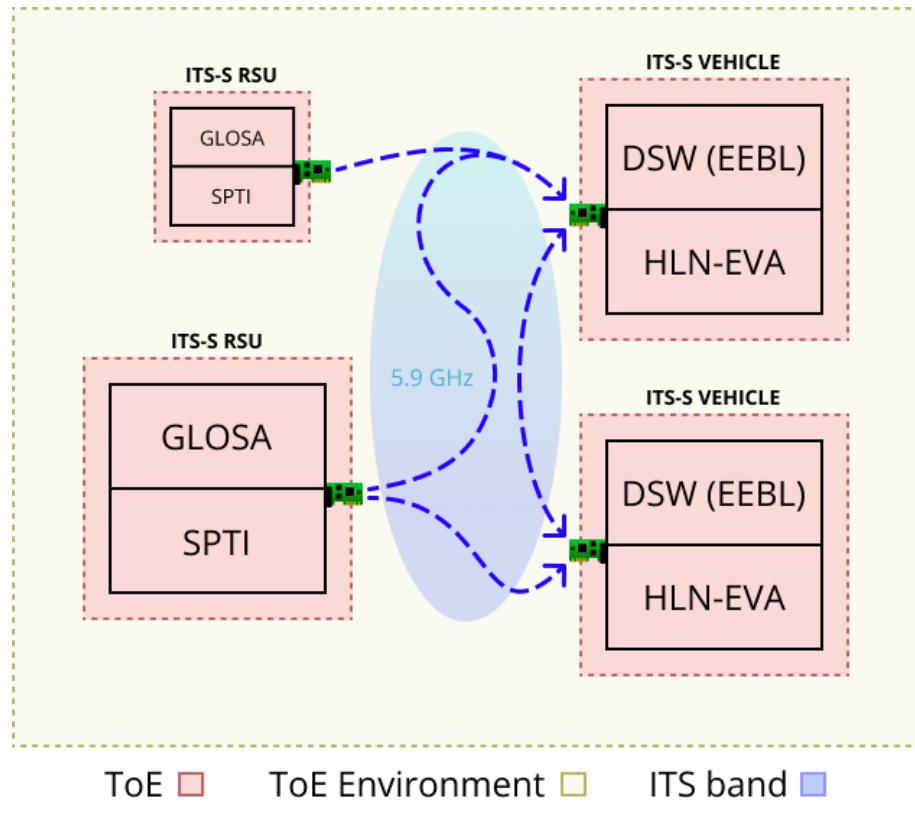


Figure 4.2: Illustration on the ToE.

This model will now be used as support to determine the ToE architecture, relevant interfaces, and information flows. With the help of the latter information, attack surfaces can also be revealed.

#### 4.2.1.3 Assumptions on the ToE system

The four entities above in figure 4.2 are theoretically different units, but in practice, they may be of the same functionality as they all are referred to ITS-Ss, and hence may be produced in the same way. But for this particular model, two distinct entity objects can still be defined, namely: the ITS-S vehicles (utilizing the CAM and DENM services) and the ITS-S RSUs (providing infrastructural information via the SPATEM and MAPEM messages to the vehicles).

Let's, for this thesis, assume that these entities only utilize and provide the use cases given to them in the figure above—following the defined scope of the ToE.

The entities have access to the 5.9 GHz band via their ITS-G5 interface for both sending and receiving. The entities know what channel to use to send specific messages. The entities always have the ability to validate any received information's integrity and authenticity thanks to the VPKI that is available (see section 3.2). The information they disseminate is gathered through onboard sensors of the ITS-S and does not carry any sensitive or classified data worth of confidentiality protection—the information is disseminated for a reason.

The only way for an attacker to compromise a vehicle with the use cases above as the cause is through the exposed interfaces that these entities (which provides these use cases) utilize. The

interfaces are shown by looking at the ToE model in figure 4.2. These are the interfaces where the use cases' respective information flows through, across the ToE environment.

#### 4.2.1.4 Assumptions on the ToE Environment

Two RSUs won't talk to each other since there's no I2I communication option, only V2I/I2V. The RSU will update itself with information from either its sensors, vehicle information (at a later deployment phase), or a backend server via up-/downlink, which is outside the scope of the current ToE. For this thesis, in correlation to the use cases, the assumption is that the RSUs only send and do not receive any information (despite the "produced similarly" hypothesis and that the RSUs and vehicles might both send and receive data and function alike).

#### 4.2.2 Security objectives

This section will focus on the framework of the CIAAA attributes (described in section 1.3.1). It will give a broad overview of the security objectives for the chosen ToE. The following security objectives can be identified upon the ToE information in the previous section:

Table 4.4: ToE Security Objectives

ToE (Use case)	Security Objectives:
	1. Confidentiality
1. DSW-EEBL 2. HLN-EVA 3. GLOSA 4. SPTI	Since all the use cases utilize broadcast addressing to all available receivers, there are <b>no confidentiality needs</b> required.
	2. Integrity Int1: Since all the use cases provide critical safety information, this information must be protected from unauthorized modification and manipulation.
	3. Availability Ava1: Access to all these use cases (thus, ITS services) associated operations should not be made unavailable by malicious activity.
	4. Accountability Acc1: It should be possible to audit critical information (either sent or received by an ITS-S) associated with the use cases (thus, the ITS services) for accountability purposes within the ITS network.
	5. Authenticity Aut1: An ITS-S that is unauthorized to utilize any of these use cases (i.e., the associated services), or to utilize it in an unauthorized way, should not be able to send any related messages. Aut2: It should not be possible for an ITS-S to send messages related to the use cases with another temporary identity than its own within the ITS network.

### 4.2.3 Functional Security Requirements

Table 4.5: ToE Security Functional Requirements

Security Objective:	Security Functional Requirement (SFR):
Int1:	Sfr1: One or more security mechanisms should be available within an ITS-S to prevent the possibility of an ITS-S modifying and manipulating data that will be transmitted. Sfr2: One or more security mechanisms should be available within an ITS-S to validate the data received over the ITS network and detect if it has been modified and manipulated.
Aval1:	Sfr3: One or more security mechanisms should be available within an ITS-S to detect and prevent malicious activity patterns.
Acc1:	Sfr4: One or more recording, logging, and auditing mechanisms should be available within an ITS-S to ensure ITS-S responsibility for exchanged information within the ITS network.
Aut1:	Sfr5: There should exist strict authentication mechanisms within the ITS-S network so unauthorized ITS-S can't, under any circumstances, utilize any of the use cases in a way it isn't authorized to (e.g., pose as an emergency vehicle without being one).
Aut2:	Sfr6: The authentication should also support and prevent an unauthorized ITS-S from being able to use an authorized ITS-S's temporary identity and thus pose as another ITS-S (not just an emergency vehicle).

### 4.2.4 Use cases assets and impact rating

An ITS-S has a tremendous set of components, elements, and other building blocks to function correctly. Since this TVRA is limited to the specific scope of the ToE defined in step 1 (i.e., the use cases at focus), it is essential to set boundaries of what ITS-S assets are to be included further in this TVRA. This step will, therefore, only look into the most crucial assets for the base capabilities required for an ITS-S to be able to utilize the use cases' functionality in terms of processing, sending, and receiving the use case related data.

**CLARIFICATION:** The assets that generate, store, and of any other means manage the data used in the messages related to the use cases, will not be evaluated—only the processing, sending, and the receiving portion.

Reviewing a simplified version of Figure 3.6 from section 3.2, assets can be identified by studying the typical scenario of the data flow when a use case is being utilized. The following assets associated with the use cases can be established:

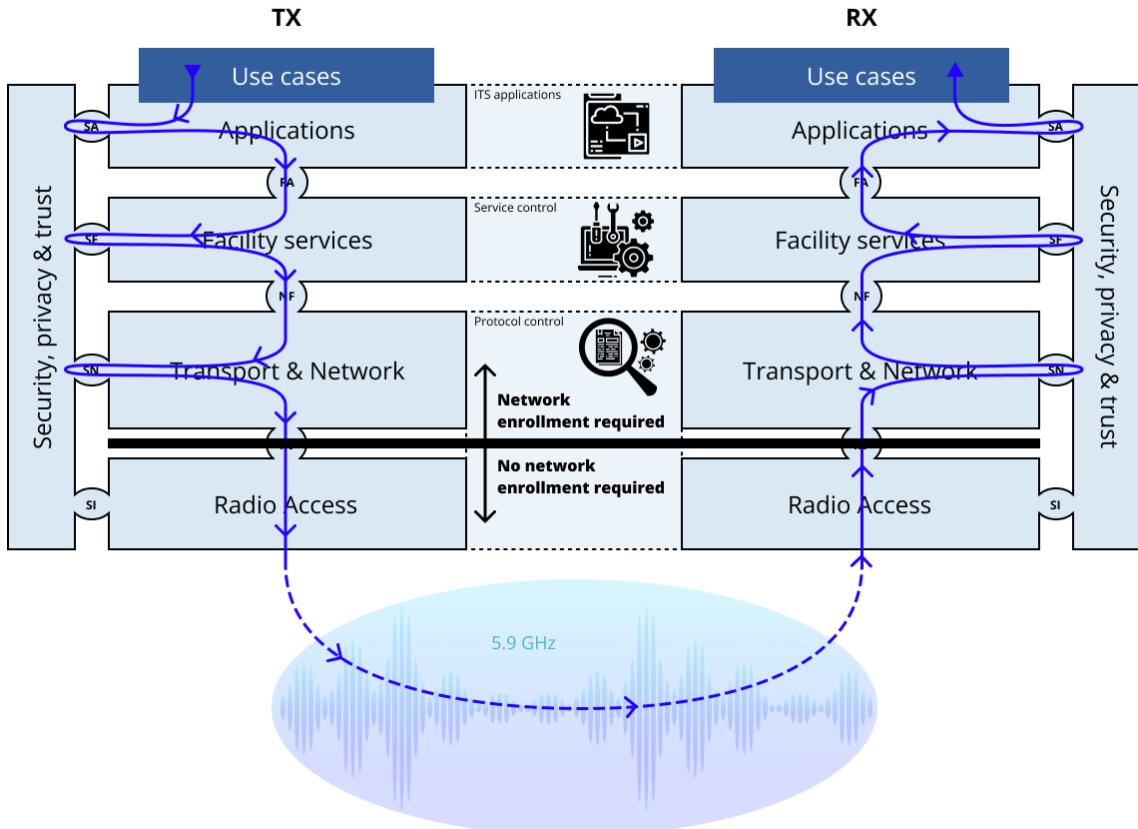


Figure 4.3: The simplified version of Figure 3.6 shows a typical data flow through the ITS protocol stack for a particular use case.

1. ITS applications
2. Service control
3. Protocol control
4. The 5.9 GHz frequency band

#### 4.2.4.1 ITS applications

The application asset processes the associated use case information received by external ITS-Ss. It then forwards this information to the relevant internal element, e.g., the element related to the dashboard, so that the driver can access that information. The application asset can also process data received by internal elements, e.g., from sensors, for transmission to other ITS-Ss in the network. The application asset takes use of the service control asset for the delivery and receiving of data.

**NOTE:** Assets associated with the dashboard and sensors are left out of this evaluation, considering the scope of the ToE.

#### 4.2.4.2 Service control

The service control asset enables and manages the internal communication between the application and protocol control assets without altering the data exchanged. Service control manages the configuration information of the ITS applications stored in a service profile repository. Configuration information may include active and non-active applications. The service control calls upon a certain application when needed, e.g., when ITS information has been received from external sources and needs to be processed. The application and service control asset works in harmonization.

#### 4.2.4.3 Protocol control

The protocol control asset is used for encapsulation and decapsulation, i.e., so a message sent or received can be processed through all the layers and correctly forwarded to its destination and intended function within the ITS-S.

#### 4.2.4.4 The 5.9 GHz frequency band

An ITS-S uses the 5.9 GHz frequency band to transmit and receive ITS messages. It is the dedicated band for C-ITS and is simply called the ITS band. The ITS band is explained more in section 3.1.2.

#### 4.2.4.5 Asset impact rating

Since these assets are the elements enabling the use cases decomposed as the ToE, the use cases are all affected if any of these four assets are compromised. For evaluating the asset impact, each use case will be looked at individually if an asset is compromised. Following the rating system in [50], the ratings in Table 4.6 can be established.

Table 4.6: Asset impact rating

ToE (Use case)	Impact rating
1. DSW-EEBL	1 (Minorly harmed)
2. HLN-EVA	1 (Minorly harmed)
3. GLOSA	1 (Minorly harmed)
4. SPTI	1 (Minorly harmed)

Impact rating 1 corresponds to the following: *The concerned entities are minorly harmed, and the damage is low.* This rating is determined according to the consideration of an ITS-S in a bigger perspective; if an ITS-S is not able to utilize any of these use cases—due to compromised

assets—the effect will not be severe since these use cases only provide additional information to the driver (as of being part of the day one deployment phase). Also, an ITS-S with these use cases will undoubtedly have onboard sensors and ADAS, bringing redundancy to the vehicle’s warning and control system. And despite all these vehicle functionalities, the driver still has the responsibility for the vehicle’s actions according to [13]. It isn’t until later deployment phases that more autonomy will be current, and the responsibility may not lay on the driver anymore. But considering the current scenario, i.e., the early use case deployment phase, onboard sensors and ADAS as redundancy, and that the driver has attention on the driving concerning his/hers responsibility, the impact will most likely be low. **A crash will most likely not occur.**

#### 4.2.5 Identification of vulnerabilities, attacks, and threat level

Despite an ITS security architecture, the network isn’t entirely resistant to attacks. Inside attacks can occur within an ITS network even though there are countermeasures that the adversary must conquer<sup>2</sup>.

##### 4.2.5.1 Vulnerabilities

If combining Figure 4.2 (Illustration on the ToE.) and 3.6 (Illustration showing where different security services operate within the ITS reference model.) into an same illustration (Figure 4.4 shown further below) two attack entries can be established, namely reference points S<sub>1</sub> and S<sub>2</sub>. It can then be summarized that attacks on the ToE originate from either a malicious ITS-S (insider attack) or from the ToE environment.

**NOTE:** Figure 4.4 does not distinguish between an ITS-S RSU and an ITS-S vehicle since the communication process is the same for both stations, regardless of the use case being utilized. The only difference is the use cases payload and the urgency of it being transmitted—which doesn’t have such a decisive role on the actual data flow process.

##### 4.2.5.2 Attacks

The following are some of the most prominent attacks that exist toward V2X communication discovered within the empirical material:

1. Disturbance of the communications
  - (a) White noise/Radio jamming
  - (b) DoS & DDoS
2. Message manipulation

---

<sup>2</sup>In this case, an insider attack means that the adversary is enrolled in the ITS network with a vehicle or some sort of malicious node.

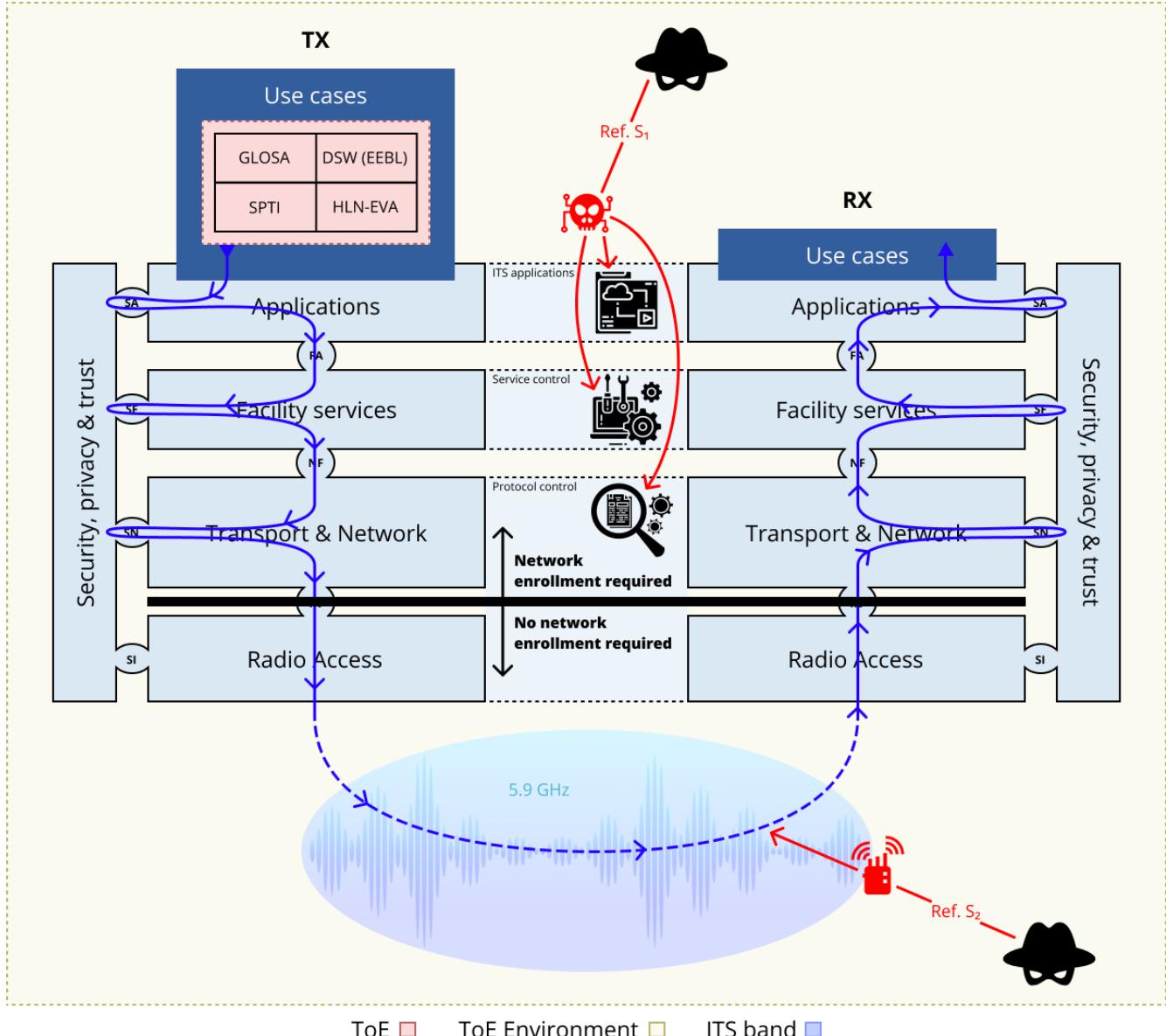


Figure 4.4: The version of Figure 4.2 and 3.6 combined in one illustration showing potential attack surfaces.

### 3. Replay attack

These four attacks are certainly not new and exist for any system or service that utilizes communication [27, 29]. But these attacks might pose a higher risk toward V2X than general IT systems since V2X involves functional safety systems, as mentioned in earlier sections of this thesis.

Table 4.7: Attack plausibility

Attack:	Security Objective:				
	Int1:	Ava1:	Acc1:	Aut1:	Aut2:
Radio jamming		✗			
DoS & DDoS		✗		✗	
Message manipulation	✗		✗	✗	
Replay attack			✗		✗

Table 4.8: Attack intensity rating

Attack	Intensity rating
1. Radio jamming	1 (few attack instances)
2. DoS & DDoS	1 (few attack instances)
3. Message manipulation	0 (single attack instance)
4. Replay attack	0 (single attack instance)

#### 4.2.5.3 Threat level

The threat level differ between the use cases, e.g., an adversary might not be very interested in falsifying EEBL messages (as IC4 mentions in Citation 4.33 below), but falsify emergency vehicle approaching messages—to pose as an emergency vehicle—might be of more interest. If an adversary also wants to create chaos in traffic, the GLOSA and SPTI use cases might be attractive to the adversary since it manages intersections. But in general, there might be an overall low interest among adversaries in attacking V2X direct communication, especially for these use cases' functionality. This is taken into consideration, and following the rating system in [50], the rating in Table 4.9 can be established.

Citation 4.33

Data extract	Coded for	Ref.
"I actually see quite a small reason for an adversary to send out for example an EEBL... might not be much to gain from it"	• Attack	Trx: IC4 Row: 253

Table 4.9: Threat level

ToE (Use case)	Motivation level	Capability level	Threat level
1. DSW-EEBL	Very low	Limited <sup>1</sup>	Low
2. HLN-EVA	Low	Very little <sup>2</sup>	Negligible
3. GLOSA	Low	Little <sup>3</sup>	Negligible
4. SPTI	Low	Little <sup>3</sup>	Negligible

<sup>1</sup>The capability level of DSW-EEBL is considered limited since an adversary might have access to an enrolled ITS-S with certain DWS-EEBL authorization.

<sup>2</sup>The capability level of HLN-EVA is considered very little since an adversary must have access to an emergency vehicle (or at least emergency vehicle authorization).

<sup>3</sup>Since RSUs are publicly accessible by being stationed beside the road, there might be a capability level of little as an adversary might hack it.

The *motivation level* and *capability level* ratings are described in more detail in [50].

#### 4.2.6 Quantifying attack potential, vulnerability likelihood and impact

**NOTE:** Vulnerability rating (used in the table above) has, for each attack, been calculated below as *attack potential*.

##### 4.2.6.1 Disturbance of the communications

All the candidates point out that the communication link, i.e., the information carrier, could easily be disturbed:

Citation 4.34

Data extract	Coded for	Ref.
"it is a very easy attack to do, I really do not see any possibilities at all to prevent it, if you want to disturb the air link you do it very very easily"	• Disturbance	Trx: IC4 Row: 266

Citation 4.35

Data extract	Coded for	Ref.
"to spam the network with messages or with white noise, it is not harder than that to disturb"	• Disturbance	Trx: IC5 Row: 164

Causing a bad communication link can easily be conducted by an adversary, especially with white noise. It may be trickier to perform a DoS or DDoS attack though, since then the adversary needs a legitimate certificate (authorized) to even be able to send *a single* message. White noise,

a.k.a. jamming, is an attack that is very difficult to prevent. Since the attack is performed on the lowest layer of the C-ITS stack (i.e., the physical layer), the adversary doesn't necessarily need to be part of the network, i.e., no network enrollment is required. The attacker doesn't require specific knowledge about the message exchange technology used within the V2X communication. The attacker simply disrupts the communication channel by sending lots and lots of irrelevant signals, interfering with the electromagnetic spectrum (5.9 GHz for 802.11p) and occupying the medium, causing legitimate signals to become limited, thus making incoming V2X messages incorrect.

A jamming attack on V2X communication may increase the latency significantly and thus reduce the network reliability drastically.

Below is the scoring for a jamming attack occurring toward V2X communication:

Table 4.10: Attack potential of Radio jamming

Attack potential rating						
Input:		Radio jamming				
Factor range →		1 day	1 week	2 weeks	1 month	2 months
Factors ↓		Layman	Proficient	Expert	Multiple ex.	N/A
Time (elapsed time)	0	1	2	4	7	1
Expertise	0	3	6	8	N/A	3
	Public	Restricted	Sensitive	Critical	N/A	
Knowledge	0	3	7	11	N/A	0
	Unlimited	Easy	Moderate	Difficult	None	
Opportunity	0	1	4	10	999	1
	Standard	Specialized	Customized	Multiple cu.	N/A	
Equipment	0	4	7	9	N/A	4
						9

Table 4.11: Attack potential of DoS & DDoS

Attack potential rating						
Input:		DoS & DDoS				
Factor range →		1 day	1 week	2 weeks	1 month	2 months
Factors ↓		Layman	Proficient	Expert	Multiple ex.	N/A
Time (elapsed time)	0	1	2	4	7	1
Expertise	0	3	6	8	N/A	6
	Public	Restricted	Sensitive	Critical	N/A	
Knowledge	0	3	7	11	N/A	3
	Unlimited	Easy	Moderate	Difficult	None	

*Continued on next page*

Table 4.11 – *Continued from previous page*

Opportunity	0	1	4	10	999	4
	Standard	Specialized	Customized	Multiple cu.	N/A	
Equipment	0	4	7	9	N/A	4
						<b>18</b>

#### 4.2.6.2 Message manipulation

An example of this was given earlier, demonstrating how this may affect vehicles. And there are lots of different ways this could affect a vehicle, but keeping it short, faulty information is not good.

Citation 4.36

Data extract	Coded for	Ref.
"injecting false warnings would have serious consequences on the system, both in the form of no longer being trusting, and that the system can be triggered to do stupid things"	<ul style="list-style-type: none"> <li>Attack</li> <li>Consequences</li> </ul>	Trx: IC5 Row: 149

For this attack, the use cases might be interesting to look at individually when a specific message with faulty information gets interpreted by the vehicle and how it showcases or acts upon it:

Citation 4.37

Data extract	Coded for	Ref.
"So you have a certificate that is valid, which means that the recipient will receive it, but you provide it with content that is not correct, and that is when these different use cases can actually be interesting, what kind of damage can you possibly do"	<ul style="list-style-type: none"> <li>Faulty information</li> <li>Impact</li> </ul>	Trx: IC4 Row: 305

Table 4.12: Attack potential of Message manipulation

Attack potential rating						
Input: Message manipulation						
Factor range →	1 day	1 week	2 weeks	1 month	2 months	Factor value
Factors ↓						
Time (elapsed time)	0	1	2	4	7	1
	Layman	Proficient	Expert	Multiple ex.	N/A	

*Continued on next page*

Table 4.12 – *Continued from previous page*

Expertise	0	3	6	8	N/A	6
	Public	Restricted	Sensitive	Critical	N/A	
Knowledge	0	3	7	11	N/A	7
	Unlimited	Easy	Moderate	Difficult	None	
Opportunity	0	1	4	10	999	4
	Standard	Specialized	Customized	Multiple cu.	N/A	
Equipment	0	4	7	9	N/A	4
						22

#### 4.2.6.3 Replay attack

A replay attack is when an adversary gathers a message, which the adversary copies and sends again (thus replaying the message). This could be may be conducted at another location or time than the original. This is very problematic, and a critical situation may be where emergency vehicle signals are being abused [1].

Citation 4.38

Data extract	Coded for	Ref.
"replay attack, save all those signals and then send them later on"	• Attack	Trx: IC1 Row: 18

Table 4.13: Attack potential of Replay attack

Attack potential rating						
Replay attack						
Input:	Factor range →	1 day	1 week	2 weeks	1 month	Factor value
Factor range →	↓ Factors					
Time (elapsed time)	0	1	2	4	7	1
	Layman	Proficient	Expert	Multiple ex.	N/A	
Expertise	0	3	6	8	N/A	6
	Public	Restricted	Sensitive	Critical	N/A	
Knowledge	0	3	7	11	N/A	3
	Unlimited	Easy	Moderate	Difficult	None	
Opportunity	0	1	4	10	999	4
	Standard	Specialized	Customized	Multiple cu.	N/A	
Equipment	0	4	7	9	N/A	4
						18

#### 4.2.6.4 Likelihood of attacks

Table 4.14: Attack likelihood determined in relation to threat level and vulnerability rating for DSW-EEBL.

Attack	Threat level	Vulnerability rating	Likelihood of attack
1. Radio jamming	Low	0-9 (Basic)	3 (Likely)
2. DoS & DDoS	Low	14-19 (Moderate)	1 (Unlikely)
3. Message manipulation	Low	20-24 (High)	1 (Very Unlikely)
4. Replay attack	Low	14-19 (Moderate)	1 (Unlikely)
<b>NOTE:</b> The <i>Very Unlikely</i> and <i>Unlikely</i> has the same likelihood value.			

Table 4.15: Attack likelihood determined in relation to threat level and vulnerability rating for HLN-EVA, GLOSA, and SPTI.

Attack	Threat level	Vulnerability rating	Likelihood of attack
1. Radio jamming	Negligible	0-9 (Basic)	2 (Possible) <sup>1</sup>
2. DoS & DDoS	Negligible	14-19 (Moderate)	1 (Very Unlikely) <sup>1</sup>
3. Message manipulation	Negligible	20-24 (High)	1 (Very Unlikely)
4. Replay attack	Negligible	14-19 (Moderate)	1 (Very Unlikely)
<sup>1</sup> Since communication disturbance cannot have a specific target, e.g., only HLN-EVA, without affecting any other use cases, the same likelihood of radio jamming and DoS & DDoS will be considered for all the use cases. Since the two attacks are most likely to occur for disturbing EEBL messages, these are the likelihood values for all the remaining use cases.			

#### 4.2.6.5 Impact by attacks

**NOTE:** The impact value has been calculated by the impact rating of the use cases from Table 4.6 in section 4.2.4.5 (which all became 1 (Minorly harmed)) plus (+) the attack intensity from Table 4.8 in section 4.2.5.2, and when calculated resulted in an overall impact shown below applicable for all the use cases.

Table 4.16: Overall impact rating by attacks

Attack	Use case impact	+	Attack intensity	=	Impact
1. Radio jamming	1 (Minorly harmed)	+	1 (few attack instances)	=	2
2. DoS & DDoS	1 (Minorly harmed)	+	1 (few attack instances)	=	2
3. Message manipulation	1 (Minorly harmed)	+	0 (single attack instance)	=	1
4. Replay attack	1 (Minorly harmed)	+	0 (single attack instance)	=	1

#### 4.2.7 Risk evaluation

This subsection calculates the risk for the use cases considering the four attacks. The procedure is that the likelihood of a specific attack is multiplied ( $\times$ ) with the impact if a use case being subject

to the specific attack. The product becomes the risk, whereas 1-2 equals minor, 3-4 major, and 6-9 critical.

Table 4.17: Risk evaluation for radio jamming considering the ToE

ToE (Use case)	Attack: Radio jamming				
	Likelihood of attack	×	Impact	=	Risk
1. DSW-EEBL	3 (Likely)	×	2	=	6 (Critical)
2. HLN-EVA	3 (Likely)	×	2	=	6 (Critical)
3. GLOSA	3 (Likely)	×	2	=	6 (Critical)
4. SPTI	3 (Likely)	×	2	=	6 (Critical)

Table 4.18: Risk evaluation for DoS &amp; DDoS considering the ToE

ToE (Use case)	Attack: DoS & DDoS				
	Likelihood of attack	×	Impact	=	Risk
1. DSW-EEBL	1 (Unlikely)	×	2	=	2 (Minor)
2. HLN-EVA	1 (Unlikely)	×	2	=	2 (Minor)
3. GLOSA	1 (Unlikely)	×	2	=	2 (Minor)
4. SPTI	1 (Unlikely)	×	2	=	2 (Minor)

Table 4.19: Risk evaluation for message manipulation considering the ToE

ToE (Use case)	Attack: Message manipulation				
	Likelihood of attack	×	Impact	=	Risk
1. DSW-EEBL	1 (Very Unlikely)	×	1	=	1 (Minor)
2. HLN-EVA	1 (Very Unlikely)	×	1	=	1 (Minor)
3. GLOSA	1 (Very Unlikely)	×	1	=	1 (Minor)
4. SPTI	1 (Very Unlikely)	×	1	=	1 (Minor)

Table 4.20: Risk evaluation for replay attack considering the ToE

ToE (Use case)	Attack: Replay attack				
	Likelihood of attack	×	Impact	=	Risk
1. DSW-EEBL	1 (Very Unlikely)	×	1	=	1 (Minor)
2. HLN-EVA	1 (Very Unlikely)	×	1	=	1 (Minor)
3. GLOSA	1 (Very Unlikely)	×	1	=	1 (Minor)
4. SPTI	1 (Very Unlikely)	×	1	=	1 (Minor)

# Chapter 5

## Discussion

### 5.1 *What are some significant use cases of V2X short-range?*

All of the use cases discovered are presented in Table 4.1 in section 4.1. The *significant* use cases from all the discovered ones are presented below in Table 5.1:

Table 5.1: Use cases summarization (ordered in deployment phases from 3 to 1).

Use cases		
Use case code	Description	Day
CLC	Cooperative Lane Change	3
CM	Cooperative Merging Assistance	3
CO	Cooperative Overtaking	3
Platoon	Vehicle platooning	3
C-ACC	Cooperative Adaptive Cruise Control	2
C-EBA	Cooperative Emergency Brake Assistance	2
VRUP	Vulnerable Road User Protection	2
DSW (EEBL)	Dangerous Situation Warning Emergency ELEC. Brake Light	1
GLOSA	Green Light Optimum Speed Advisory	1
HLN-EVA	Hazardous Location Notif. Emergency Vehicle Approaching	1
SPTI	Signal Phase and Timing Information	1

By the examination of various reports for this thesis work, the use cases presented in the table above are familiar with use case examples presented in the available litterature, especially the day one use cases. Some examples of documents where some of the use cases above can be found are: [1, 62, 19, 3, 29]. Platooning is a well-known use case when talking about V2X, and this becomes very clear when all of the reports covered in the earlier research section (1.3.2) of this thesis mention it. The only reports that don't mention it are [44, 27].

If comparing the results of this study with [3], which was the report that was relatively similar to this thesis, it can be found that the EEBL use case has been evaluated in that report too. The

result of their risk for that particular use case will be compared with the risk rating calculated in this thesis in the next section.

## 5.2 What cybersecurity risks can be associated with these use cases?

The biggest cybersecurity-related concern that all candidates express is the risk of involving connectivity in a safety-dependent function, i.e., in this case, vehicles and transportation. In general cybersecurity, two dimensions can be considered or analyzed, which are (1) the impact (or the consequences) of an attack and (2) the likelihood of it occurring. Considering these two principles, V2X-equipped vehicles can pose a great risk since the connectivity might easily be hacked, directly affecting the safety aspect:

Citation 5.1

Data extract	Coded for	Ref.
<i>"it will impact safety a lot considering the use cases, and on the other hand the connectivity may be very easy to hack, so I think cybersecurity is absolutely the most important aspect of V2X"</i>	<ul style="list-style-type: none"> <li>• Consequences</li> <li>• Hacking</li> </ul>	Trx: IC2 Row: 143

Considering the above, the impact dimension is very complicated to calculate for a V2X scenario since there's always an end user involved whose safety cannot be compromised under any circumstances. If a V2X system fails during a cyberattack, it may be life-threatening for the people involved. [19] evaluates and classifies hazards according to severity, exposure, and controllability for several V2X use cases. The attributes are used in a so-called HARA, a risk assessment process for analyzing hazards. They consistently assess the highest level of severity for all the safety use cases they examine. This seems more than reasonable to do, and according to the citations below, it isn't possible to put a price tag on potentially devastating events:

Citation 5.2

Data extract	Coded for	Ref.
<i>"now you don't see me (camera was off) but if I put 'save lives' inside apostrophe signs, this is very difficult to put a price tag on"</i>	<ul style="list-style-type: none"> <li>• Consequences</li> </ul>	Trx: IC3 Row: 71

Despite this complexity, risk factors must be considered and classified systematically, providing a workflow for managing the discovered risks in a prioritized manner. So even though two existing threats might be life-threatening—i.e., posing a severe risk—a systematic approach to managing these two threats reduces the overall risk. It's essential to constantly adapt the risk assessment to the current situation to effectively distinguish between risks in a complex threat

scenario for the best possible prevention. Risk analysis requires good data to reduce uncertainty, and to improve proper risk management [63]. Considering the scenario of a C-ITS, resources for complete safety and reduction of uncertainty for such a system are limited. Hence, a feature providing semi-automated functionality (such as for C-ACC) might be a better alternative than letting end users have complete responsibility for the vehicle maneuvering. I.e., human error might pose a higher risk than ADAS—thus, the risks associated with ADAS are therefore acceptable in comparison.

All the above were considered during the risk assessment process in this thesis. Therefore, the impact level of the use cases in this thesis risk assessment was not given the highest impact rating in contrast to how [19] evaluated their impact levels for their use cases. This was because the use cases that were assessed in this thesis were all day one use cases. The use cases assessed in [19] were both day one use cases and above, and the use cases in the later deployment phases involve more autonomy and should therefore be considered more safety-critical, thus a higher impact rating. But the day one use case that [19] assessed was EEBL, which was also one of the ToE's in this thesis. [19] considered an impact level of life-threatening for this use case, while it was considered minorly harmed in this thesis. The difference in this attribute is probably because this thesis considered an ITS-S in a bigger perspective (that the vehicle has redundancy of onboard sensors and that the driver pays attention to the driving) while [19] considered the vehicle being heavily dependent on the use case function.

If comparing this thesis results with [3] findings, the radio jamming attack, if specifically considering the EEBL use case (since this was the only evaluated use case in common, as mentioned in section 5.1), can be assumed to occur with a high likelihood since both this thesis and [3] rates it high (3/3 and 0.9/1). But the risk isn't the same because the impact rating is higher within this thesis than what [3] considers it to be. Why the impact rating of the radio jamming attack became higher in this thesis in comparison to [3] probably depends on the fact that we in this thesis considered several instances of the radio jamming attack, which resulted in a higher impact rating. [3], on the other hand, considered this as a relatively harmless behavior and argues that, quote; "*loss of connectivity is common in ad hoc networks and functions are designed to expect this.*" This sounds reasonable, and the impact rating that was calculated in this thesis for a radio jamming attack might have become higher than it actually is in real life. But this isn't easy to assume, and the risk assessment process in this thesis was carefully and detailed conducted, and the results should therefore be considered adequately valid. Worth mentioning is that it is absolutely critical not to speculate in a risk assessment process. Certain likelihood and impact factors should only be considered and included in the risk assessment if they have strong evidence. We kept this in consideration for this thesis work, but certain aspects might still have been overlooked, and vital factors might have been missed that caused the impact ratings to be considered either high and/or low. But it should also be pointed out that comparing different risk assessment methods results is also problematic and could be misleading. Table 5.2 is a summary of this thesis's risk assessment results, followed by a comparison to the results in [3] (Table 5.3).

Table 5.2: Risk evaluation summarization

Attack:	Use case:			
	DSW-EEBL	HLN-EVA	GLOSA	SPTI
Radio jamming	6 (Critical)	6 (Critical)	6 (Critical)	6 (Critical)
DoS & DDoS	2 (Minor)	2 (Minor)	2 (Minor)	2 (Minor)
Message manipulation	1 (Minor)	1 (Minor)	1 (Minor)	1 (Minor)
Replay attack	1 (Minor)	1 (Minor)	1 (Minor)	1 (Minor)

Table 5.3: The risk results differences between this thesis and [3] considering use case DSW-EEBL.

Report	
This thesis	[3]
Attack:	Use case: DSW-EEBL
Radio jamming	6/9
DoS & DDoS	2/9
Message manipulation	1/9
Replay attack	1/9

Why the risks happened to become different is probably because the impact rating was calculated differently as different risk assessment methods were used. Another reason might be that either this thesis or [3] has overlooked important aspects and missed vital factors in the risk assessment process. A third reason might be that the threat scenario has changed since last year, and different risks are now current as of 2022.

Some parallels between this thesis results and the ETSI TVRA [45] from 2017 can be established. The risk for radio jamming is relatively the same, thus despite re-defined security requirements in their later documents [46, 47, 48, 49]. In [45], they have several entries in their risk table for communication disturbance attacks, where one entry named “denial of transmission” can be considered radio jamming. The risk rating of this attack is the same (value: 6) in [45] as for this thesis result. But there’s a slight difference in the naming of this risk value in this thesis compared to [45]. Instead of it being critical (as considered in this thesis following the ETSI TVRA model [50]), is it referred to as major in [45]. This is a bit confusing, and the risk for radio jamming might not be completely comparable though the same risk assessment model has been used in this thesis as for in [45]. If comparing the values, the risk remains the same for radio jamming. In contrast, an increased risk has been discovered in this thesis when comparing the risk namings—i.e., critical vs. major.

For the other attacks, the risk factor is certainly lower in this thesis result in contrast to the risks in [45]. DoS & DDoS are for example considered critical in [45], while in this thesis discovered as minor. There are no exact entries for the message manipulation and replay attack in [45] risk table. Still, there is an attacking concept that both of these attacks can be categorized into, namely

“masquerade.” If comparing the masquerade risk rating in [45] to the risk rating for message manipulation and replay attack in this thesis, the risk is higher in [45] compared to this thesis result.

There are two possible reasons why the risks are lower in this thesis result compared to [45], these are:

1. The requirements in the following documents [46, 47, 48, 49] lower the risk for specific attacks (DoS & DDoS, message manipulation, and replay attack) and are appropriate for the evaluated use cases in this thesis. This aligns with this thesis purpose, namely validating the current security requirements are thoroughly sound for the evaluated use cases.
2. A more comprehensive scope was used in the [45] with more assets taken into account compared to this thesis scope which might have led to the differences in the resulting risks.

## 5.3 Limitations of the study

Although a more experimental approach with simulations might have contributed to more precise and accurate risks, similar to the report [3], it was not an option since that would have required more time and resources than what this work possessed. Simulation test suites are available, but only commercially, which was not an option for this thesis.

### 5.3.1 Interviews

When reviewing this thesis’s results, some problematic aspects of the interview methodology must be kept in mind.

When considering question one, “What are some significant use cases of V2X short-range?,” and how these use cases were selected, it is necessary to keep in mind that only five candidates participated. Although all interview candidates are well established in the field and possess great knowledge of the subject, there is a risk that the answers of these five people are not representative of all other actors in the field, especially considering that they have been recruited through convenience sampling and snowball sampling.

To some extent, the problem could have been avoided if more participants had taken part in the analysis. But due to time limitations, this was not possible since every interview took about one hour. Another solution would have been to use a survey. However, as mentioned earlier in the thesis, it would have been challenging to ensure that other factors would not influence their choice, such as taking a longer/shorter time to select use cases. The pros and cons were weighed when choosing between a survey or interviews and landed on the interview, particularly because it opens opportunities for more in-depth discussions, generating more rich and detailed data.

A further aspect that should be highlighted related to question one is the conceptual validity of “significant use cases,” i.e., there is a risk of candidates interpreting the concept differently—something that the candidates themselves noted during the interview. The reliability of the method

when choosing a use case can thus be questioned to some extent. However, the meaning of significance was defined as “use cases that you consider are the most relevant or predominantly crucial thinking from the core of V2X technology” (the “core of technology” refers to the three aspects: driver comfort, traffic efficiency, and road safety), but there is still a risk that the candidates interpreted the definition differently. Some of the candidates also remarked on this issue:

Citation 5.3

Data extract	Coded for	Ref.
<i>“It is not so clear, core of technology, because here you focus, it seems that it is more on functionality”</i>	<ul style="list-style-type: none"> <li>• Uncertainty</li> <li>• Unclear</li> </ul>	Trx: IC1 Row: 56

Previous experience and area of knowledge can have had a major influence on the candidates choices:

Citation 5.4

Data extract	Coded for	Ref.
<i>“If there is someone who has not worked with safety, it may be that the others are quite interested in the use cases that suggest something new, but for me, I would like to know if this use case is safe or not”</i>	<ul style="list-style-type: none"> <li>• Uncertainty</li> </ul>	Trx: IC1 Row: 58

Lastly, the use cases might seem well-defined in papers such as the C2C-CC use case roadmap [5]—which was the paper used for decomposing the use case list used in the interviews—but the fact is that the use cases described in this early phase of the V2X technology not yet are so accurate. How some use cases are defined today may certainly not be defined the same in the future. For example, Weather Condition Warning has three sub-use cases (or so-called sub-cause codes); fog, precipitation, and traction loss. In contrast, Road Closure, Lane Closure, Mobile Road Works, and Winter Maintenance all have the same characteristics but are still divided into individual use cases within the C2C-CC roadmap. These two scenarios could be different in the future. The Weather Condition Warning’s sub-cause codes could be defined as individual use cases. Road Closure could be defined as one primary use case with the other associated use cases Lane Closure, Mobile Road Works, and Winter Maintenance as sub-cause codes. Unfortunately, this made it a bit inadequate when certain use cases seemed to belong to each other, and others did not. This needs to be considered since this may have affected the result.

### 5.3.1.1 An issue with replicating the study

There’s a big issue in that the candidates are anonymous, and the interview material (the recorded material) was deleted after the analysis. This is problematic because the study cannot be replicated in the same way as desired. Everything associated with a study like this must be saved and kept

intact for replication purposes. This was not the case in this scenario and was primarily because of the fact that all candidates were to feel as comfortable as possible participating in the interview—this was our ambition.

### 5.3.2 Data analysis

The inductive type TA did not seem relevant for this thesis since the analysis process involves identifying patterns within the empirical data in a "bottom-up" way. This means that the data isn't coded according to an existing coding frame with a connection to the research question. Instead is it the other way around; coding the data set with the possibility of the research questions evolving during the process. The inductive TA was not suitable since the research questions were already defined before the interviews and the coding process—thus resulting in the deductive type TA.

The disadvantage though of the deductive TA is that it can usually be challenging with the width it provides. The focus can shift to something that isn't interesting or requested by the study because of the broad data collection during the interviews. This was considered as much as possible during the interviews but was a challenging factor that caused some information within the empirical data not to be relevant for this thesis. This is, though, a common outcome of a qualitative study: some of the information isn't entirely relevant for the study's purpose.

### 5.3.3 Risk assessment model

For question two, "What cybersecurity risks can be associated with these use cases?," it is important to remember that BIAS can unintentionally affect the risk evaluation of the use cases even though the author has strived to be as objective as possible through the performed risk assessment processes.

The thesis's risk assessment scope should be considered a micro perspective on a broad subject. The risk assessment result within this thesis should not be considered entirely accurate but instead, be seen as approximate risks threatening the use cases at focus. This is important to consider since the risk analysis otherwise would have had to be more thorough. The risk assessment didn't become completely thorough because of, mainly, the restraint of time and resources.

## 5.4 Future work

There are certainly more challenges with the V2X technology at this moment in time than only cybersecurity. It can be summarized that the whole technology is still in its very early phase, meaning that not even many of the day one use cases are yet current on a big scale. These use cases are still in a planning phase, slowly making their way into the market.

Despite this very early phase of the technology, this thesis, among a tremendous amount of related research papers, has proven that the cybersecurity needs for V2X communication are fundamental. Considering the more narrow scope of the cybersecurity perspective of V2X, the automotive industry needs just as much IT security as the actual IT industry, as also mentioned in the following citation:

Citation 5.5

Data extract	Coded for	Ref.
<i>"so we still need to involve a lot of the IT security technologies into the automotive industry"</i>	• Measures	Trx: IC2 Row: 161

This thesis did, for example, not even evaluate any privacy-related concerns with V2X, though some of the privacy measures within the ITS security architecture were described in the theory chapter of this thesis. This is a very interesting topic for the V2X use cases provided in this thesis, and for V2X in general. For example, the emergency vehicle approaching use case, several communications options may be available in the future for redundancy, e.g., direct and up-/down-link communication. But adding up-/down-link communication for this use case means that information about the presence of where, in this case, the Police are, must be processed in some sort of central node configuration. This could be a severe risk with sensitive information being processed and stored in a database, compared to direct communication where the Police (in this case) only disseminate their presence—very similar to activating their sirens, but instead activating an ITS-G5 transceiver. This is a privacy concern in the perspective of the Police's confidentiality.

Also, new security technologies need to be observed and evaluated if they can be used in the V2X context. One such example is the blockchain technology which IC2 mentions:

Citation 5.6

Data extract	Coded for	Ref.
<i>"we found blockchain, in fact, is quite important for the future of cybersecurity, and also can save a lot of work today and change a lot of today's world, and we think that the blockchain could be a very interesting future based infrastructure"</i>	• Future security • Measures	Trx: IC2 Row: 7

A blockchain mechanism within the ITS network would potentially enable decentralized ITS communication where the authentication and authorization of ITS-S messages are validated according to the blockchain ledger.

And also new security evaluations methods also need to be considered, something IC4 mentions:

## Citation 5.7

Data extract	Coded for	Ref.
<i>"how do you make sure you have a good implementation and what are the tools and methods, how do you measure or evaluate it"</i>	<ul style="list-style-type: none"><li>• Evaluation</li><li>• Future security</li></ul>	Trx: IC2 Row: 482

These are some future research directions discovered during the course of this thesis work. And the critical risk of the radio jamming attack discovered in this thesis might be very difficult to mitigate. Still, further research is encouraged on how this risk might be reduced for a V2X scenario. Lastly, the remaining use cases that were discovered within the interview material as significant use cases but weren't evaluated for risks (i.e., the day two and three use cases) are also subject to future work.

# Chapter 6

## Conclusion

This thesis investigated two main research questions: (1) *What are some significant use cases of V2X short-range?* and (2) *What cybersecurity risks can be associated with these use cases?* We conclude that the use cases in Table 5.1 are somewhat significant, and a certain amount of attention is shed on them within the V2X field. For the second question, a summarization of the cybersecurity risks discovered in this thesis is presented in Table 5.2. The risks range from minor to critical, and it is mostly the radio jamming attack that pose the biggest concern for the use cases used as the ToE. Some of the risks discovered in this thesis are relatively the same in other studies, especially when considering the likelihood rating for communication disturbance attacks (radio jamming, DoS & DDoS). The differences discovered in the risks are mostly related to the difference in the impact rating. Other studies seem to have a lower or higher impact rating than what was considered in this thesis. Therefore, the risks don't become entirely similar. This could depend on three things, namely; (1) because of different risk assessment methods, (2) that this thesis or other reports overlooked important aspects and missed vital factors in the risk assessment process, or lastly (3) that the threat scenario is different now compared to when the other studies were conducted.

Worth mentioning is that it is challenging to perform a risk assessment with the scope of use cases. Still, it is practical since the discovered risk can be directly compared to the actual feature, e.g., a functional safety feature. If a certain functional safety feature contributes bigger benefits than the cybersecurity risk, there's a rational reason to implement it.

In short, this thesis's purpose was to provide an overview of V2X use cases, give information on current security requirements and solutions, and validate if these are appropriate for a selection of the overviewed use cases through a risk analysis. This has been accomplished, and the only critical risk discovered in this thesis was the radio jamming attack. This attack might be challenging to mitigate, but further research is encouraged in the area of whether there exist any accurate solutions that can reduce this risk for a V2X scenario.

# Bibliography

- [1] M. Fallgren, M. Dillinger, T. Mahmood, and T. Svensson, *Cellular V2X For Connected And Automated Driving*. John Wiley & Sons Ltd, 2021, pages: 1-8, 260-261.
- [2] ETSI, “Etsi ts 102 724,” Okt 2012, [https://www.etsi.org/deliver/etsi\\_ts/102700\\_102799/102724/01.01.01\\_60/ts\\_102724v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/102700_102799/102724/01.01.01_60/ts_102724v010101p.pdf), [Accessed 21 Aug 2022].
- [3] O. Sawade, I. Radusch, and M. Hauswirth, “V2x attack vectors and risk analysis for automated cooperative driving,” *IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, June 2021, <https://ieeexplore.ieee.org/document/9448795>, [Accessed 02 Oct 2022].
- [4] H. Bagheri, M. Noor-A-Rahim, Z. Liu, H. Lee, D. Pesch, K. Moessner, and P. Xiao, “5g nr-v2x: Towards connected and cooperative autonomous driving,” Mar 2021, <https://ieeexplore.ieee.org/abstract/document/9392787;https://arxiv.org/ftp/arxiv/papers/2009/2009.03638.pdf>.
- [5] T. W. G. F. of the C2C-CC, “Guidance for day 2 and beyond roadmap,” N/A, Tech. Rep., 07 2021, [https://www.car-2-car.org/fileadmin/documents/General\\_Documents/C2CCC\\_WP\\_2072\\_RoadmapDay2AndBeyond\\_V1.2.pdf](https://www.car-2-car.org/fileadmin/documents/General_Documents/C2CCC_WP_2072_RoadmapDay2AndBeyond_V1.2.pdf).
- [6] L. Chen and C. Englund, “Cooperative intersection management: A survey,” *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, pp. 579, 570, 2016.
- [7] Qualcomm, “5g nr based c-v2x,” <https://www.qualcomm.com/media/documents/files/5g-nr-based-c-v2x-presentation.pdf>, [Accessed 24 Mar 2022].
- [8] Wikipedia, “Ieee 802.11,” Aug 2022, [https://en.wikipedia.org/wiki/IEEE\\_802.11](https://en.wikipedia.org/wiki/IEEE_802.11), [Accessed 24 Aug 2022].
- [9] 3gpp, “Release 14,” Jun 2018, <https://www.3gpp.org/release-14>, [Accessed 24 Aug 2022].
- [10] ——, “Release 16,” Jun 2022, <https://www.3gpp.org/release-16>, [Accessed 24 Aug 2022].
- [11] Tesla, “Computer installations for total self-driving capacity (fsd),” [https://www.tesla.com/sv\\_SE/support/full-self-driving-computer](https://www.tesla.com/sv_SE/support/full-self-driving-computer), [Accessed 12 Feb 2022].

- [12] N. T. S. Board, “Tesla crash investigation yields 9 ntsb safety recommendations,” Feb 2020, <https://www.ntsb.gov/news/press-releases/Pages/NR20200225.aspx>, [Accessed 18 Feb 2022].
- [13] S. of Automotive Engineers, “Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles,” [https://www.sae.org/standards/content/j3016\\_202104/](https://www.sae.org/standards/content/j3016_202104/), [Accessed 18 Jul 2022].
- [14] Slashgear.com, “Honda very carefully sets loose its level 3 autonomous car,” Mar 2021, <https://www.slashgear.com/honda-very-carefully-sets-loose-its-level-3-autonomous-car-04662291>, [Accessed 15 Feb 2022].
- [15] Wikipedia, “Waymo,” Dec 2021, <https://sv.wikipedia.org/wiki/Waymo>, [Accessed 23 Mar 2022].
- [16] ——, “Zoox (company),” Feb 2022, [https://en.wikipedia.org/wiki/Zoox\\_\(company\)](https://en.wikipedia.org/wiki/Zoox_(company)), [Accessed 23 Mar 2022].
- [17] ——, “Cruise (autonomous vehicle),” Mar 2022, [https://en.wikipedia.org/wiki/Cruise\\_\(autonomous\\_vehicle\)](https://en.wikipedia.org/wiki/Cruise_(autonomous_vehicle)), [Accessed 12 Feb 2022].
- [18] Jurist.org, “Do tesla fsd beta releases violate public road testing regulations?” Sep 2021, <https://www.jurist.org/commentary/2021/09/william-widen-philip-koopman-autonomous-vehicles/>, [Accessed 17 Feb 2022].
- [19] Autotalks, “Functional safety for enabling present and future v2x use-cases,” Jul 2021, <https://auto-talks.com/wp-content/uploads/2021/07/Functional-Safety-for-V2X-use-cases.pdf>.
- [20] BBC, “Fiat chrysler recalls 1.4 million cars after jeep hack,” July 2015, <https://www.bbc.com/news/technology-33650491>, [Accessed 16 Aug 2022].
- [21] C. Englund, L. Chen, J. Ploeg, E. Semsar-Kazerooni, A. Voronov, H. H. Bengtsson, and J. Didoff, “The grand cooperative driving challenge 2016: Boosting the introduction of cooperative automated vehicles,” *IEEE Wireless Communications*, p. 148, 2016.
- [22] M. Botte, L. Pariota, L. D’Acierno, and G. N. Bifulco, “An overview of cooperative driving in the european union: Policies and practices,” *Electronics*, Volume: 8, no. 6, p. 306–314, May 2019, dOI: 10.3390/electronics8060616, Available: <http://dx.doi.org/10.3390/electronics8060616> [Online].
- [23] V. A. D. H.-J. Günther), “Car2x communications in the golf 8 towards cooperative safety,” Jun 2020, [https://its-standards.eu/documents/WebinarIsrael/P05\\_2020-06-18\\_Car2X\\_in\\_Israel.pdf](https://its-standards.eu/documents/WebinarIsrael/P05_2020-06-18_Car2X_in_Israel.pdf), [Accessed 09 Sep 2022].

- [24] FutureCar.com, “Volkswagen unveils the new id.5 electric suv-coupe,” <https://www.futurecar.com/4976/Volkswagen-Unveils-the-New-ID-5-Electric-SUV-Coupe>, [Accessed 18 Jul 2022].
- [25] ETSI, “Etsi en 302 665 v1.1.1,” Sep 2010, [https://www.etsi.org/deliver/etsi\\_en/302600\\_302699/302665/01.01.01\\_60/en\\_302665v010101p.pdf](https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf), [Accessed 26 Jul 2022].
- [26] ——, “Etsi ts 102 731,” Sep 2010, [https://www.etsi.org/deliver/etsi\\_ts/102700\\_102799/102731/01.01.01\\_60/ts\\_102731v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf), [Accessed 01 Aug 2022].
- [27] A. Ghosal and M. Conti, “Security issues and challenges in v2x: A survey,” *Computer Networks, Volume 169, 107093*, March 2019, <https://doi.org/10.1016/j.comnet.2019.107093>.
- [28] ETSI, “Etsi en 302 663 v1.3.1,” Jan 2020, [https://www.etsi.org/deliver/etsi\\_en/302600\\_302699/302663/01.03.01\\_60/en\\_302663v010301p.pdf](https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf), [Accessed 26 Jul 2022].
- [29] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, “Securing vehicle-to-everything (v2x) communication platforms,” *IEEE Transactions on Intelligent Vehicles (Volume: 5, Issue: 4)*, pp. 693–713, April 2020.
- [30] ETSI, “Technical committee (tc) intelligent transport systems (its),” 2022, <https://www.etsi.org/committee/1402-its>, [Accessed 10 Sep 2022].
- [31] Topgear.com, “Officially launched: The all-new 2020 volkswagen golf is here,” Oct 2019, <https://www.topgear.com.ph/news/car-news/mk8-volkswagen-golf-launch-tguk-a2613-20191025>, [Accessed 15 Aug 2022].
- [32] 3gpp, “About 3gpp,” 2022, <https://www.3gpp.org/about-3gpp>, [Accessed 10 Sep 2022].
- [33] Qualcomm, “Let’s set the record straight on c-v2x,” Apr 2018, [https://www.sae.org/standards/content/j3016\\_202104/](https://www.sae.org/standards/content/j3016_202104/), [Accessed 18 Jul 2022].
- [34] G. Wireless, “Dsrc vs c-v2x: Comparing the connected vehicles technologies,” Nov 2021, <https://gttwireless.com/dsrc-vs-c-v2x-comparing-the-connected-vehicles-technologies/>, [Accessed 18 Aug 2022].
- [35] c-its-deployment group.eu, “C-its deployment group welcomes the update of the its directive 2022,” Apr 2018, <https://c-its-deployment-group.eu/mission/statements/2021-12-20-its-directive-2022/>, [Accessed 17 Aug 2022].
- [36] ETSI, “Etsi tr 102 638,” Jun 2009, [https://www.etsi.org/deliver/etsi\\_tr/102600\\_102699/102638/01.01.01\\_60/tr\\_102638v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf), [Accessed 13 Aug 2022].
- [37] iso.org, “Road vehicles — cybersecurity engineering iso/sae 21434:2021,” <https://www.iso.org/standard/70918.html>, [Accessed 26 Jul 2022].

- [38] A. O. Affia, R. Matulevičius, and R. Tõnnisson, Eds., *Security Risk Estimation and Management in Autonomous Driving Vehicles*, vol. 424. International Conference on Advanced Information Systems Engineering, 2018, [https://link.springer.com/chapter/10.1007/978-3-030-79108-7\\_2](https://link.springer.com/chapter/10.1007/978-3-030-79108-7_2).
- [39] M. Chapple, J. M. Stewart, and D. Gibson, *(ISC)<sup>2</sup> Certified Information Systems Security Professional Official Study Guide*, 9th ed. John Wiley & Sons, Inc., Hoboken, New Jersey, 2021.
- [40] N. I. of Standards and Technology, “Computer security resource center - cybersecurity definition,” <https://csrc.nist.gov/glossary/term/cybersecurity>, [Accessed 4 Jul 2022].
- [41] M. Muhammad and G. A. Safdar, “5g-based v2v broadcast communications: A security perspective,” *Array, Volume 11* (2021), 100084, September 2021.
- [42] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” *Vehicular Communications 23* (2020) 100214, December 2019.
- [43] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, “Attacks and defences on intelligent connected vehicles: a survey,” *Digital Communications and Networks 6* (2020) 399–421, May 2020.
- [44] V. Sharma, I. You, and N. Guizani, “Security of 5g-v2x: Technologies, standardization and research directions,” *IEEE Network, Volume: 34, Issue: 5*, p. 306–314, September/October 2020, dOI: 10.1109/MNET.001.1900662.
- [45] ETSI, “Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra),” Tech. Rep., 2017, eTSI TR 102 893 V1.2.1: [https://www.etsi.org/deliver/etsi\\_tr/102800\\_102899/102893/01.02.01\\_60/tr\\_102893v010201p.pdf](https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf).
- [46] ——, “Etsi ts 102 940,” Jul 2021, [https://www.etsi.org/deliver/etsi\\_ts/102900\\_102999/102940/02.01.01\\_60/ts\\_102940v020101p.pdf](https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf), [Accessed 07 Aug 2022].
- [47] ——, “Etsi ts 102 941,” Jan 2021, [https://www.etsi.org/deliver/etsi\\_ts/102900\\_102999/102941/01.04.01\\_60/ts\\_102941v010401p.pdf](https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.04.01_60/ts_102941v010401p.pdf), [Accessed 17 Aug 2022].
- [48] ——, “Etsi ts 102 942,” Jun 2012, [https://www.etsi.org/deliver/etsi\\_ts/102900\\_102999/102942/01.01.01\\_60/ts\\_102942v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/ts_102942v010101p.pdf), [Accessed 17 Aug 2022].
- [49] ——, “Etsi ts 103 097,” Okt 2021, [https://www.etsi.org/deliver/etsi\\_ts/103000\\_103099/103097/02.01.01\\_60/ts\\_103097v020101p.pdf](https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf), [Accessed 18 Aug 2022].
- [50] ——, “Etsi ts 102 165-1,” Okt 2017, [https://www.etsi.org/deliver/etsi\\_ts/102100\\_102199/10216501/05.02.03\\_60/ts\\_10216501v050203p.pdf](https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf), [Accessed 07 Aug 2022].

- [51] ——, “Ets 300 387,” May 1994, [https://www.etsi.org/deliver/etsi\\_i\\_ets/300300\\_300399/300387/01\\_60/ets\\_300387e01p.pdf](https://www.etsi.org/deliver/etsi_i_ets/300300_300399/300387/01_60/ets_300387e01p.pdf), [Accessed 07 Aug 2022].
- [52] P. Blomkvist and A. Hallin, *Method for engineering students: Degree projects using the 4-phase Model.* Studentlitteratur AB, 2015.
- [53] B. Virginia and C. Victoria, “Using thematic analysis in psychology,” *Qualitative Research in Psychology.* 3, pp. 77–101, Jul 2008, <https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa>, [Accessed 26 May 2022].
- [54] ETSI, “Etsi tr 187 011,” Jul 2008, [https://www.etsi.org/deliver/etsi\\_tr/187000\\_187099/187011/02.01.01\\_60/tr\\_187011v020101p.pdf](https://www.etsi.org/deliver/etsi_tr/187000_187099/187011/02.01.01_60/tr_187011v020101p.pdf), [Accessed 11 Sep 2022].
- [55] ISO/IEC, “Iso/iec 27033-1:2015,” Aug 2015, <https://www.iso.org/standard/63461.html>, [Accessed 23 Aug 2022].
- [56] ETSI, “Etsi en 303 613,” Okt 2019, [https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303613/01.01.01\\_30/en\\_303613v010101v.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303613/01.01.01_30/en_303613v010101v.pdf), [Accessed 23 Aug 2022].
- [57] ——, “Etsi tr 102 863,” Jun 2011, [https://www.etsi.org/deliver/etsi\\_tr/102800\\_102899/102863/01.01.01\\_60/tr\\_102863v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/102800_102899/102863/01.01.01_60/tr_102863v010101p.pdf), [Accessed 14 Aug 2022].
- [58] ——, “Etsi ts 103 301,” Aug 2018, [https://www.etsi.org/deliver/etsi\\_ts/103300\\_103399/103301/01.02.01\\_60/ts\\_103301v010201p.pdf](https://www.etsi.org/deliver/etsi_ts/103300_103399/103301/01.02.01_60/ts_103301v010201p.pdf), [Accessed 21 Aug 2022].
- [59] ——, “Etsi en 302 636-4-1 v1.4.1,” Jan 2020, [https://www.etsi.org/deliver/etsi\\_en/302600\\_302699/3026360401/01.04.01\\_60/en\\_3026360401v010401p.pdf](https://www.etsi.org/deliver/etsi_en/302600_302699/3026360401/01.04.01_60/en_3026360401v010401p.pdf), [Accessed 27 Jul 2022].
- [60] ——, “Etsi tr 103 766 v1.1.1,” Sep 2021, [https://www.etsi.org/deliver/etsi\\_tr/103700\\_103799/103766/01.01.01\\_60/tr\\_103766v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/103700_103799/103766/01.01.01_60/tr_103766v010101p.pdf), [Accessed 27 Jul 2022].
- [61] ——, “Etsi tr 103 415,” Apr 2018, [https://www.etsi.org/deliver/etsi\\_tr/103400\\_103499/103415/01.01.01\\_60/tr\\_103415v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf), [Accessed 31 Aug 2022].
- [62] V. Newsroom, “New assist and light systems,” Nov 2019, <https://www.volkswagen-newsroom.com/en/the-new-golf-international-vehicle-presentation-5609/new-assist-and-light-systems-5623>.
- [63] ETSI, “Swedish msb method support framework for security management,” Aug 2022.

# Appendix A

## Interview questionnaire material

### A.1 Interview slides

The PowerPoint consisted of 7 slides, but only the slides containing the questions have been attached to this appendix section.



V2X use cases and their cybersecurity

**Agenda**

- 1. Introduce ourselves
- 2. Some general questions about V2X
- 3. Questions about V2X use-cases (perform a little task)
- 4. Questions about cybersecurity regarding the use cases at focus

Figure A.1: Slide 1

**General questions about V2X**

- *What do you think of the current situation of V2X?*
- *What do you think is the biggest challenge so far for V2X?*
- *What companies do you think have the biggest influence on this technical development right now?*



Figure A.2: Slide 3

**Questions about V2X use cases**

From your perspective of expertise within this area, choose:

- **4x day-1 use cases**
- **4x day-2 use cases**
- **4x day-3 use cases**

... that you consider will have/or already has a **significant role** for traffic situations.

By “significant role,” I mean use cases that you consider **are the most relevant or predominantly crucial** thinking from the core of V2X technology.

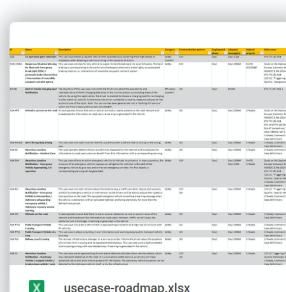


Figure A.3: Slide 4



**Cybersecurity questions**

- *Explain a bit of why you chose these four day-x use cases?*
- *Do you see any potential cyber threats toward a vehicle with these use cases?*
- *If so, are there any security measures?*

Figure A.4: Slide 5

## A.2 Consent letter



# Consent letter

Information about the interview session:

1. According to the scheduled time slot, the interview will be held in about an hour.
2. The interview will be recorded so that the interviewer can look back on the material afterward. The recording will be deleted when the data has been analyzed.
3. If you're not comfortable having your camera enabled while recording, you can have it disabled.
4. As an interview candidate, you will be anonymous in the report and mentioned as Interview Candidate X (ICX).
5. As an interview candidate, you can, whenever you like, interrupt the interviewer or leave the interview session.

Hereby I consent that the interview that I will participate in will be recorded and that the information I share will be used as data in the context of Adrian Brorsson's bachelor's thesis.

Location, Date

Digital meeting over Teams

2022-04-01

Signature

You give your consent orally at the start of the recording.



## Appendix B

# Interview transcripts (Trx)

In this appendix are the transcripts attached. The transcript includes three remark notions which are the following:

[unclear] = Is used where a certain thing that the interview candidate said wasn't clear enough.

(... lorem ipsum ...) = Brackets with some text inside mean that the interview candidate said wasn't clear, but it was probably the text inside the brackets.

... = The three dots *x* two rows means that certain un-relevant interview material hasn't been included. This could be things unrelated to the topic.

### B.1 Interview Candidate 1 (IC1) Interview Transcript

Då ska vi se om det går igång här, sådär, och då IC1, får jag ditt medgivande för att du är med på intervjun och att jag spelar in den

2 Ja

4 Japp, suveränt, då ska jag dela min skärm här.

...

6 ...

När vi gör en attackinjicering, vi har ett system, eller vi har modell av ett system, eller ett system som finns i en simulationsmiljö och vi introducerar attacker, olika typer av attacker för att påverka systemet på ett negativt sätt, och sen ser om systemet kan hantera dem, och på nått sätt gör vi samma sak när vi kör pen testing faktiskt

10 ...

...

12 Så det, om vi pratar om use case, ett use case kan vara adaptive cruise control och adaptiviteten i adaptive cruise control det är med hjälp av att skicka signaler från en bil till en annan bil så det är V2V kommunikation

14 Ah justeja, okej

15 [unclear] (dem informerar andra) bilar i området vad du har som hastighet och sådant och ett specifikt use case kan vara

16 Platooning, då kommer (det här sättets) bilarna att köra ungefär med samma hastighet, så vad vi gör är att vi tittar på den signalen som en bil skickar till en annan bil och försöker att introducera en attack [unclear] blockera till exempel

18 signalen eller köra en typ av attack som kallas replay attack, spara alla dem signalerna och sen skickar vi dem vidare lite senare

20 ...  
...  
22 What do you think of the current situation of V2X?  
Jag tror att det finns massor som forskare gör men det kan vara att det finns inte så många system som använder V2X just nu, precis med det här exemplet som jag gav, adaptive cruise control, det finns modeller, det finns simulationsmiljö som använder cruise control och den adaptiviteten med hjälp av att skicka en signal från en bil till en annan bil med hjälp av trådlös kommunikation, men så långt jag vet så finns det inte så många OEMer i fordonsindustrin som använder den här delen, nu litar dem mest på on-board-sensorer och andra komponenter i bilar, men det är intressant det finns massor som man kan göra där och testning är ganska viktigt eftersom man behöver att vara säker att dem signalerna som bilarna skickar till varandra, att dem kan lita på de signalerna och att det finns ingen attacker som kan påverka dem och blockera dem, så intressant område absolut  
Jättebra, intressanta svar, och då över till nästa då du gick in lite på det, men what do you think is the biggest challenge so far for V2X, och det är väl kanske då att ingen liksom riktigt har liksom implementerat det än då eller vad man ska säga kanske  
34 Nä och jag tror också [unclear] i V2X, och jag är inte expert där, det enda fokus som vi har är att introducera fel och attack i simulations-miljö, med V2X, men vad jag ser som en utmaning generellt sätt är att på samma sätt som vi har märkt tidigare, huvudfokus just nu kan vara att utveckla ett system som kan ge en OEM en lite bättre produkt som de kan sälja bättre och dem skulle vilja vara först inom området, så jag tycker att det kanske är lite för lite fokus på utvärdering av systemen när det handlar om cybersäkerhet till exempel  
Men när du menar lite bättre produkt är det då utifrån liksom [unclear] funktionaliteten eller enkelheten av implementeringen eller  
Nä jag tror det är funktionalitet, det finns en, om dem har en komponent eller om dem har en förbättring som dem kan göra på en bil skulle dem vilja göra det så snart som möjligt så att dem är först i området så att dem sen kan tjäna mycket pengar på detta, så det kanske, fokus på utvärdering av system, det är, jag skulle vilja säga att det kunde ha varit mycket bättre, mycket högre, men det är en utmaning som dem kommer att se i framtiden  
...  
46 ...  
Men dem här två olika grejerna, ett use case som är ganska viktigt för safety, det kanske inte är efficient, eller tvärtom Det är faktiskt, det är väldigt sant, men om du tänker liksom ett use case som om du skulle, för nu vill jag ju då att du ska välja fyra, om du tänker att vilka use case måste verkligen vara med i en sån här lista om du är tvungen och välja, jag förstår att det är en väldigt svår uppgift för jag menar det är som du säger alla use cases har ju sin liksom del i teknologin alltså den är ju väldigt, dem är ju alla viktiga på sitt unika sätt, men hur som helst, så vill jag att du ska välja då, och då får du i första kolumnen här ta ett ID då och sen välja en färg, så du markerar den, och så har du ju day one här då och så kommer day two lite längre ner, och så gör du så, så får du femton minuter på dig, och om du är klar tidigare än det så är det bara att säga till då ju, men under tiden så mutear jag mig och så får du lite tid för dig själv, och så har jag uppe den här sliden då för dig att komma tillbaka till om du vill liksom se på min definition igen då  
56 Ja de är, det är inte så, det är inte så tydligt, core of technology, eftersom här fokuserar du, det verkar som att det är mer på funktionalitet, men jag tror att dem viktiga frågorna dem ligger under safety, men jag gör mitt bästa, så får du kanske koppla mitt svar på nått sätt till min bakgrund eftersom det, om det är nån som inte har jobbat med safety, det kan vara att dem andra är ganska intresserade de use cases som föreslår något nytt, men för mig, jag skulle vilja veta om det här use caset är safe eller inte  
Väldigt intressant att du säger det, det är ju en sak för mig att ta upp i min problematisering, det du säger är ju väldigt relevant  
...  
64 ...  
Jag är klar  
66 Super, nice  
Det var inte så lätt att gå igenom allt på femton minuter, man behöver mycket mer tid faktiskt att läsa alla dem externa

68 Ja, jo självklart det blir ju lite, ja jag tänker, jo men precis alltså det är ju sjukt många, det är det, sen och det blir ju  
också en grej i min slags problematisering, jag tänker också jag vet inte riktigt, man skulle ju kunna göra det på något  
70 slags mer kvantitativ metod och skicka ut liksom som en enkät vid sidan om, men nu har jag ju redan påbörjat den här  
metoden så jag får ju bara ta det med en liten

72 Det är lite svårt tycker jag att kunna lita på alla dem svar på ett bra sätt eftersom folk har olika sätt att läsa och sen  
ibland om man är snabbläsare man kan missa viktiga grejer, men jag försökte mitt bästa, jag tror att jag är nöjd

74 ...  
...  
76 Vi kollar på day two istället, så dem här fyra då, varför har du valt just dem  
Så jag tror att om, om vi skickar en notifikation eller en signal till en bil och informerar dem om någonting som händer  
78 i området, det är viktigt, men det är även viktigare om vi utnyttjar den här informationen och dem use cases som jag  
valde tycker jag att, cooperative acc, vi får en information och vi behöver att göra någonting med den här informationen  
80 som kommer att ha faktiskt en safety påverkan, så om vi får en signal från bilen framför oss att min hastighet är 70  
km/h och sen om en attacker påverkar den signalen och säger att min hastighet är 100 km/h, [unclear] bilen som står  
82 bakom kommer att accelerera och sen så blir det en olycka  
Justeja, att den tar på, av eget beslut där då baserat på informationen

84 Precis  
Trots att bilen framför åker i 70 så liksom ökar ändå bilen bakom för att den ser det som att bilen framför accelererar,  
86 justeja  
Så det finns sensorfusion säkert bilarna, dem behöver att utnyttja information från olika resurser, från sensorer och  
88 radar, lidar och kamera och sen samtidigt den informationen som kommer genom trådlös kommunikation  
Är det dem alla mest liksom vanliga sensorerna en bil är utrustad med  
90 Det finns massor men man kan säga lidar, radar, och sen kamera, och trådlös signalerna, dem är kanske dem viktiga  
informationerna som varje bil behöver att ha och sen gå igenom sensor fusion och sen bestämmer vad det är som vill  
92 göra, vi behöver ha redundans på nått sätt där, och sen det kan vara att informationen som kommer från en sensor dem  
är olika än informationen som kommer från den bilen genom trådlös kommunikation, så bilen behöver bestämma sig  
94 för vilken information kommer jag att lita på, och vad är det beslutet som jag kommer ta, kommer jag att öka min  
hastighet eller kommer jag att minska det, så dem use casen som jag valde, jag tycker att på grund av den situationen  
96 att bilen behöver att välja var att göra näst då är det jätteviktigt från safety och cybersäkerhetssidan, och det är inte bara  
cybersäkerhet som är problem, det är också fel i systemet som är problem om en bil bara  
98 Alltså buggar liksom  
Ah, det är inte bara buggar, eftersom bug är något som vi pratar om när vi pratar om mjukvara, men det är ett hårdvarufel  
100 Hårdvarufel, jaha ok du menar så ok  
Och det är jättevanligt, det händer, så vi hela tiden behöver ha redundans i systemet så att om det finns ett hårdvarufel  
102 på en sensor då vi har fått informationen också genom andra kanaler så kan vi lita på dem informationerna och jämföra  
dem och se hur mycket är den bästa beslutet som vi kan ta, eller bilen  
104 Justeja och då kan man även säga att den här sensorn att den är faulty nu liksom, det är någonting som inte stämmer  
med den i jämförelse med data från flera andra fordon då  
106 Ja, och miljö är ganska viktigt också men när vi pratar om olika väderkondition, så att kanske lidar är bättre i sådan  
[unclear] några av dem, kamera är bättre så det är massor av information som kommer och sen bilen behöver bestämma  
108 vad det är som är det bästa beslutet att ta, så det är generellt sätt huvud grejer som jag försökte att fokusera på, jag tycker  
att cooperative acc, cooperative acc string, och sen emergency braking dem är direkt kopplade till något sånt beslut som  
110 kan ha katastrof-påverkan på systemet, om det finns ett fel i systemet eller om det finns ett problem i systemet, och  
samtidigt för dem andra, platooning är samma sak och overtaking, emerging, och cooperative lane change, dem är  
112 viktiga beslut, att en bil tar ett beslut att byta till en annan (lane) och sen det finns en bil som kommer, och sen det  
finns en (olycka) så det är viktig tycker jag, dem grejerna som jag inte valt mest var dem notifikation och det är något  
114 som är extra information som förare har, dem kan kontrollera systemet, men acc det är en direkt, eller platooning bilen  
bestämmer och det är inte föraren faktiskt

116 Nä justeja, men då kan man säga att du har valt use casen utifrån alltså, utifrån nu då blir det ju ett, primärt då safety  
perspektiv, men där då dem här funktionerna har en liksom direkt påverkan att motverka en katastrof då helt enkelt eller  
118 vad man säger

Ja precis, och [unclear] början av detta kan vara cybersäkerhetsattack, eller det kan vara fel i systemet, men oavsett  
120 om det är en cybersäkerhetsattack eller om det är hårdvara- eller mjukvarufel i systemet, påverkan som jag försökte att  
fokusera på var på safety

122 ...

## B.2 Interview Candidate 2 (IC2) Interview Transcript

I think it's, just want to really make sure that it's, is recording, ok, there we go, so yes IC2 do I have your consent with  
2 you participating in the interview and being recorded

Yes, I agree

4 Yes, nice, ok cool

...

6 ...

... and then we found blockchain, in fact, is quite important for the future (of) cybersecurity, and also can save a lot  
8 of work today and change a lot of today's (world), and we think that the block trend could be a very interesting future  
based infrastructure, [unclear] for the future, so then after that, I think that ok I can [unclear] into the cybersecurity,  
10 and [unclear] together to see how we can use blockchain as a future technology to protect our cybersecurity, and we  
have tried to initialize some projects from both Europe and China with effort in the quite early phase of the technology  
12 to adopt it, so it's very hard to found some projects, so in Sweden we try to collaborate with our autonomous driving  
team to apply a project from, named, I don't remember the name, but it's a European project, it's about the blockchain  
14 as the [unclear] infrastructure, and for that one is that is [unclear] collect the data from different users and because  
you know for the autonomous driving the most important thing is how to generate the this [unclear] the map, to have a  
16 very accurate precisions, but then (this also very) sensitive to the cybersecurity, and in today's way is that we use like  
google, these companies they send some cars to collecting the data by mapping the city, and in the other hands if we  
18 want to increase the efficiency we can have more distributed way, because everyone who have the sensor in the future  
they can (sense) the city and to collect the data (by) everyone, but then the problem is that how we can trust the data,  
20 from different users, the blockchain is a good technology to somehow use the [unclear] to secure the [unclear] then we  
can more efficiently to compose the map, for the autonomous cars

22 ...

...

24 But yes, let's go over to the, now it has gone 15 min already, so we will see how long, or how much we'll cover  
basically, but first I thought of some general questions about V2X, now you did also talk a bit about like the, like the  
26 overall technology as well with like autonomous driving, but yes, I'll still ask some general questions about it, and then  
we going to questions about V2X use cases, and there is where you'll perform your little task, and then lastly questions  
28 about cybersecurity regarding the use cases at focus, and I'll come to what I mean with that, but yes, some general  
questions then, and what do you think of the current situation of V2X, and if you want to add anything additional to  
30 what you've already said

The current situation of V2X is that it's still very early phase to adopt the technology, you can see some OEMs then  
32 already said they had implement V2X, but the problem is that this is very much like the early phase of the telephone  
industry, you need enough users so that you can communicate to each other, so I think the current situation of V2X is  
34 still in the very early phase of it, and but we see some, potential demands from different markets that V2X may become  
mandatory, to adopt it into future cars, due to some safety demands, but it's still for example in the United States, the  
36 V2X is that they try to demand this in some but they have not approved yet so, the thing in China I think, we cannot

see very clear, the about V2x, on the other hand we also heard from for example in China the safety testing, you know  
38 the Euro NCAP, Euro NCAP is for the testing how many stars your car can achieve of this safety rating, Euro NCAP,  
and now both in Europe, China its name is CCAP, they want to add the V2X as one testing (aspect) into their future  
40 safety tests, it means that if the car equipped with V2X, it will have, from the active safety it will have some more,  
more functions to protect the (users), then your rating will be, safety rating will be higher, so from that point of view  
42 I think that OEMs also want to implement have more, interest to implement V2X because then we can increase our  
safety rating in Europe and China in this safety testing

44 Yes definitely, very interesting answer there, thank you a lot, and yes you have basically gone through, like the biggest  
challenges, it's basically their early stage then, and then I have what companies do you think have the biggest influence  
46 like OEMs then, like basically their names, just by curiosity if you have any like, what would you say

...

48 ...

To be [unclear] I think like German OEMs like who is most aggressive (on the) V2X adoptions maybe like Audi and  
50 Volkswagen, they may have big influence on this technical development now, yes and I think in China is that also a  
lot of you know in China you have, there are a lot of new startups and new technology companies that invest into this  
52 automotive industry like the Tesla, [unclear], I think they also are eager to have V2X as well, and due to the different  
technology adopts into different (markets), you know in Europe, now is hard to say, but it seems that Europe will utilize  
54 this 802.11p standard for V2X, and in China already confirmed to use cellular based V2X

Ah ok

56 Yes, that is already confirmed by China, and United States at the beginning they had the, they have this IEEE and the  
[unclear] 11p standard but for [unclear], from history, maybe already 10 years, but since now they, I think from last  
58 year they have some new policies that they want to investigate their cellular based V2X as well

Yes, so they'll like combine the two communications options, both short and long range then?

60 Yes, exactly, but we don't know, which one they'll, they'll only see some policies they want also to invest from their  
transportation department, of the federal department, they want to invest some money, a lot of money into this cellular  
62 V2X, which is also due to their OEMs that's very interested into cellular based V2X, most from Ford and GM, so from  
United States absolute is the Ford and GM, they'll have the biggest influence on the technology in the united states

64 Ah ok, yes, interesting, I thought it was, I'm a little bit biased, so I thought it was Tesla then, with all their, as with their  
full-self-driving and all what it is, but yes, so GM and Ford then

66 Yes, I think it depends on, I think this question its depends on different markets

68 Yes, definitely, it's a bit general actually, but yes just by curiosity I wanted to like hear what brands that are like pushing  
the limits like this technical development or how to say, but yes, I think I definitely got a lot of info there, so now we'll  
go over to the little task, and yes I think I'll give you around, so little bit of short time maybe, but I think I'll give you  
70 around 10 minutes to perform it, but if you, if you definitely feel like you'll need more time you'll get an extra 5 min or  
something

72 Thank you

74 Yes, but I want you to do the following according to this question then, so from your perspective of expertise within  
this area choose four day one use cases, and four day two use cases, and four day three use cases that you consider will  
have or already has a significant role for the traffic situations, and for that I'll share a google sheets document with you,  
76 with all the use case examples that the car too car communication consortium has in their latest use case roadmap

Ok

78 So, in there you'll like pick four day one, four day two, and four day three use cases, and by significant role I mean  
use cases that you consider are the most relevant or predominantly crucial thinking from the core of V2X technology,  
80 basically traffic safety and efficiency then

Sorry Adrian, in here [unclear] are the most relevant or predominantly crucial thinking from the core, is that you think  
82 that which one is the most significant (use case) to improve the safety, or you think which one is the, like our problems,  
which one is most possible to implement

84 No I want you to choose like the ones that you actually think are the most like I say, crucial for like traffic situations,  
not like the ease of implementing, but instead like, the most useful use cases

86 ...  
...  
88 Eh, so let's try this out now, so I'll share you this link then, and change so you have, I'll send it in the chat, and I'll have my slide open here so you can go back to it and just to see once again or what I mean with significant role, but yes not  
90 with the perspective of ease implementation but instead like the what you think are the most useful use cases within this  
Ok  
92 And yes, now I see you're in here, then I want you to in the first column here just target the ID with a background color  
and then be persistent with that color and then I'll, we'll filter them out later when you're done  
94 So, I select the [unclear] and the changes the color of the ID  
Yes exactly, so as I'm doing here with the let's take an easy to pronounce, but EVCSN, electric vehicle charging spot  
96 notification, just change the background color and then have the same color for every selection and then we'll filter  
them out, but yes, so basically I'll have my PowerPoint slide open here so you can go back to it, and yes I'll give you  
98 about like ten minutes then and then yes I'll mute myself during the time, but as soon as you're done you can just tell  
me  
100 Yes sure  
I'll give you some time for yourself  
102 Ok  
Ok yes nice  
104 Yes, hear you later, I'll mute as well  
Hello Adrian  
106 Yes  
I just finished  
108 Ok, how did it go, ok let's see which use cases, ok nice, ok so this was actually, the sort of most important thing in  
the interview, because it's, my studies both qualitative and literature study, so these are actually the use cases in like  
110 relation to how the other participants also answers on this task, that I will perform a literature study on the most like  
yes, then relevant use cases, so yes, that was why I also let you really finish the task so maybe we'll not like have time  
112 to go through all of them, but I thought according to the slides here, go through the day one use cases maybe, and then  
I'll ask you the same question for each use case, and they are these three questions, so why you chose that particular  
114 use case and if you see any potential cyberthreats or risks with this use case, and if so, are there any security measures  
against these, that's basically the three questions for each use case here then, so if we start with emergency vehicle  
116 intervention, why did you choose this use case  
Yes, I think day one, first [unclear] my logic is that day one use cases to V2X technology is not so mature, and there's a  
118 low market penetration which means that it is not so many cars equipped with this V2X yet, and then I prefer the I2V,  
these kinds of use cases since the infrastructure is somehow centralized with, compared to this how to say this [unclear]  
120 infrastructure side maybe it's easier to adopt the at early phase, and so is [unclear] cannot rely on V2X to provide this  
kind of information to the driver, so [unclear] the first one which is emergency vehicle that we also think could be the  
122 first day one, the first type of cars to equip this V2X, because like ambulance, and different emergency vehicles they are  
centralized on [unclear] maybe by governments or some organizations, then can the first batch of the cars to equip V2V,  
124 and so they have maybe [unclear] think about the possibility which can [unclear] equip cars [unclear] the infrastructure  
they may be equipped with this V2X, and that's why I selected these ones, I think emergency cars they may be (the)  
126 first batch  
Yes, sounds very reasonable, interesting, a good choice so to say, and then, actually if I should take maybe day two use  
128 cases as well, because I'm a little bit interesting of this one since I have read a little bit about it as well, but yes why did  
you choose this day two use case, if we go over to that instead  
130 ...  
...  
132 I think this intersection collision, I think is a quite dangerous scenarios about the safety in real life so then it becomes,  
intersections also have a lot of this kind of traffic (signs), which is infrastructure they may, higher probability to have

134 this V2X adopted, and then I (think in combination) with this dangerous scenarios its [unclear] I think this could be  
interesting use case to implement to day two

136 Yes definitely, I think, yes basically all the use cases are like very important in their own way of course, I bet maybe  
that this task was a bit difficult as well maybe

138 ... the last very general question, and that's basically if you have any additional thoughts or wonderings that you'll like  
to share regarding the things covered in this interview basically use cases from a cybersecurity perspective

140 Yes, I have a lot of answers of security questions, I think that cybersecurity is always the most important thing aspect  
of V2X, because in general cybersecurity we'll consider two dimensions, one dimension is on the safety impact, and  
142 another dimension is the feasibility how a hacker may potentially hack our cars, this how we analyze our vehicle in  
cybersecurity today is that then the V2X will [unclear] two dimensions because it will impact safety a lot considering  
144 the use cases, and on the other hand the connectivity may be very easy to hack, so I think cybersecurity is absolutely  
the most important aspect of V2X and based on my selecting from your, this use cases, I think that basically we can see  
146 the trend from day one to day three is that we will have more, so follow the trend of the more and more autonomous  
driving in the future, which is that I think that in the future if we really want to implement this autonomous drive, it  
148 will of course not only rely on more advanced cars, this is also because the cars will always need the infrastructure  
to help it with driving, so I think then in the future is absolutely, we also have very advanced road with this traffic  
150 infrastructures, and also will assist the autonomous driving, so I think for cybersecurity maybe we can consider some  
future cybersecurity technologies, as I mentioned for the blockchain, I think that also, because different (markets) they  
152 also [unclear] globally other countries is very [unclear] the blockchain and see it as a potential future [unclear] to protect  
the cybersecurity, I think that blockchains could be a very interesting new technology for the future of cybersecurity of  
154 this V2X

Yes, it sounds very futuristic or how to say it

156 Yes, is that question about the future or could I see you question again

Yes, it was basically this

158 Yes I think on the other hand so (today) vehicle cybersecurity is [unclear] mainly how to say involved from IT cybersecurity,  
and that's, but there's a big difference between these two industries, the IT industry and the automotive industry,  
160 because for the car we will impact the safety a lot, but IT we may just lose some money, so that's, you see very big  
difference, so we still need to involve a lot of the IT security technologies into the automotive industry to make it more  
162 efficient and maybe we also, you know IT security is popular of this how to say, zero-trust architecture, but that is also  
very hard for us to implement into the car, because we, we need to consider the cost and also ourselves the architecture,  
164 a lot of [unclear] we need to implement regarding the cybersecurity, but I think that we can both have this involvement  
from the IT security but we really need to keep eyes on this new technology which can simply change the game like the  
166 blockchain

What did you mean with zero trust infrastructure

168 Zero-trust is that, [unclear] for the IT infrastructure that you cannot trust everyone, [unclear] because due to efficiency  
we cannot verify everything, so basically, yes you know if we about to implement that it may still take long time to  
170 implement that into the cars, although IT in the IT world it is also very hard to implement it today...

...

172 ...

## B.3 Interview Candidate 3 (IC3) Interview Transcript

Yes så vi ska bara vänta på den pop uppen här så jag vet att det verkligen är i gång, så då, då IC3 har jag ditt medgivande  
2 med att du är med på den här intervjun och att den spelas in?

Ja

4 Japp, suveränt, då ska jag dela min skärm här nu också för jag har lite slides som jag kommer att utgå ifrån

...

6 ...

- What do you think of the current situation of V2X, så nu går vi direkt över dit då
- 8 Rådande situation, jag är väldigt glad att det äntligen händer, short range för det är det du avser antar jag, för v2x för mig kan både vara long range och short range kommunikation, men jag antar att det är direktkommunikation
- 10 Ja precis alltså det blir ju mest fokus på det eftersom det är mest aktuellt då så att säga, men under use case uppgiften där så finns det ju en del use case där som kan, vad säger man, ämna för long communication
- 12 Long range
- Long range ah precis, ah exakt, men ja det blir ju mest fokus, men utifrån ditt perspektiv liksom så det är jättebra, ta det såsom du ser det
- 14 Men ah om jag tar ur det stora hela perspektivet, cloud baserad V2X kommer mer och mer, men dock så går det väldigt
- 16 trögt att samarbeta med andra OEMer när det gäller att utbyta information över cloud för att alla parter har sitt eget språk, försöka knyta ihop dem här molnen är inte enkelt även om det finns ett projekt inom EU eller en gruppering som
- 18 heter data for road safety, som försöker (facilitera) det här men det går väldigt trögt, tittar vi sen då på short range V2X så är jag väldigt glad att det nu börjar rullas ut i Kina och i Europa så att det kommer, är helt enkelt ett komplement till
- 20 sensorerna som vi har på bilarna som radar och kameror, och kompletterar även med den här cloud baserad V2X:en, och det kommer rädda liv definitivt så det är jag väldigt glad för att det nu äntligen sker, och det rullas ut på bred front
- 22 får man väl säga i Kina och i Europa så har ju Volkswagen lanserat det och tagit nu första steget så att det är väldigt positivt, och det går lite trögare i USA, en annan sida av det här också är att det rullas ut i Kina men på grund av den här China shift algoritm för positionering och kartor som man måste använda i Kina
- Okej ja
- 26 Vilket internationella OEMer följer medans lokala OEMer inte verkar följa så har man två olika koordinatsystem man jobbar efter med vilket skjuter hela V2X ekosystemet i sank i Kina, och det har auktoriseras nu precis och [unclear]
- 28 från General Motors hade en dragning om detta inom 5GAA alldelens nyligen, tar man en annan negativ aspekt i Europa så trots att Volkswagen har rullat ut V2X short range med ITS-G5 teknologin så är det fortfarande en enorm diskussion
- 30 huruvida det är den teknologin som ska gälla eller den 3GPP baserade lösningen LTE-V2X eller 5G-V2X då, så här tar det ju otroligt lång tid för att marknaden får liksom anamma det här pga. den här osäkerheten som 5GAA skapar bland
- 32 annat då
- Japp, så det är liksom, det är en stor debatt som försiggår i liksom Europa om det ska bli, ah om vi säger short range
- 34 ITS-G5 då eller liksom PC5 pratar man om då när man ändå pratar cellulärt
- Ah precis det heter det ju på 3GPP språk då
- 36 Mm
- Ah så det är väl, eftersom 5GAA är aktiva och vissa OEMer är väldigt aktiva så, det skapar en förvirring även om redan
- 38 den ena (tekniken har rullats ut då), vilket inte är bra för oss invånare inom EU helt enkelt, som invånare struntar du fullständigt i vilken radioteknologi som används, det viktiga är use cases
- 40 Ja
- Går vi sen till USA så har det ju också varit en diskussion om teknologier där av nu FCC frekvens-myndigheten då
- 42 bestämt sig att man byter från DSRC till C-V2X i USA, men man tappade samtidigt 40 MHz utav 75 MHz så att, eller man tappade 45 MHz utav 75 så det är bara 30 MHz kvar
- 44 ...
- ...  
46 Ah det är väldigt problematiskt så att, men nu har Ford har ju annonserat sedan tidigare att dem ska lansera det detta året och Audi annonserade bara för ett par veckor sedan att dem ska lansera det 2024 i USA så att vi kommer avvakta
- 48 och se hur det går för dem, för att dessutom förstör vanliga wifi näten C-V2X system i USA pga. out of band emissions kraven är för dåliga i reglementet i USA
- 50 Ja men det är fortfarande dedicated short range som är den liksom, den som är i mest fokus i USA, eller sa du att dem hade övergett den lite och gått på det cellulära
- 52 Ja det är ju fortfarande enligt lagtexten så är det fortfarande så men dem ska byta till PC5 då  
PC5 ah ok
- 54 Hur den här transformationen ska gå till är inte helt utredd, Ford, Jaguar, Landrover och Audi pushar på  
Ja

56 Och sen är det ju ett antal stater då som redan har installerat utrustning som måste ersätta sin utrustning med den nya  
radioteknologin och vill ha ersättning för detta, och dessutom så är det någon radioamatör organisation som har stämt  
58 FCC frekvensmyndigheten i USA av detta så att det är ju en juridisk process som pågår dessutom i USA så att det är  
kaos kan man väl säga

60 Det är lite bröjtigt  
Ah, så med dem här c shift i Kina, teknologidebatten i Europa och att vi tappade frekvensband i USA gör ju inte  
62 situationen särskilt enkel globalt tyvärr  
Nä, och det var lite min andra fråga där som jag tycker vi har coverat ganska bra här nu då  
64 Ah men det, men det är på gång nu ändå, vi vet att det är fler på gång nämligen  
Japp, och den tredje frågan har vi också nämnt lite nu då, men du kanske vill, för det behöver ju inte bara vara OEM:s  
66 då utan det kan ju vara andra involverade om det är någon du vill tillägga och det är främst inte så mycket för arbetets  
syfta utan det är för min egen liksom så här bredda min vy så att säga, liksom vilka är det som är involverade egentligen  
68 i allt det här, så från det att du, från det du sagt liksom är det någon du skulle vilja tillägga  
Nä men jag kan väl säga såhär, tunga fordonsindustrin har väldigt stor nytta av short range V2X i hamnområde i gruvor  
70 och så där finns ett väldigt tydligt business case för det så dem kan ju faktiskt räkna hem investeringen i produkten  
vilket (inte som biltillverkare) kan göra för att här är handlar det, nu ser du inte mig men om jag sätter rädda liv inom  
72 snuttar och det är väldigt svårt att sätta en prislapp på det vad det får kosta nämligen  
Ja det är klart  
74 Men annars alla OEMer är mer eller mindre aktiva, det som är viktigast är att dem stora masstillverkarna som Volkswagen  
har redan börjat men som Toyota, säg Ford och GM liksom de stora märkena börjar rulla ut det och visar vägen för  
76 att (det är ingen mening att) endast en biltillverkare ska rulla ut det här  
...  
78 ...  
Då tänker jag att vi går över till den här lilla uppgiften nu då  
80 Mm  
Och då vill jag att du enligt denna frågan då, så from your perspective of expertise within this area, choose four day one  
82 use cases, four day two use cases and four day three use cases that you consider will have or already has a significant  
role for traffic situations och då är det det Goolge Docset då som jag har och då har jag ju tagit exempel use case från  
84 Car-to-Car deras senaste use case roadmap där då, och här är det ju upp för en själv och tolka lite vad jag menar men  
jag tror ändå att det blir hyfsat bra mätbar data trots att nu mina intervjukandidater har tolkat det lite olika men by  
86 significant role i mean use cases that you consider are the most relevant or predominantly crucial thinking from the core  
of V2X, så alltså traffic och safety då, eller jag vad heter det efficiency och safety, yes och till detta så kommer du få 15  
88 min på dig och om du behöver mer tid så, för jag vill helst att du utför uppgiften så gott du kan då, men sen om du blir  
klar tidigare så är det bara att säga till och då har jag lite frågor om dem use casen sen  
90 ...  
...  
92 Ah nu är jag klar  
...  
94 ...  
Yes då ska vi göra som så att, då är det utifrån dem här frågorna nu så ska vi gå igenom då dem olika, jomen liksom  
96 day one kategorin av dem use case du valt och sen day två och sen day tre och det är det jag tänker vi gör nu på den  
sista tiden så långt vi hinner, så först då, explain a bit of why you chose these four day och så one, day två day tre use  
98 cases och sen ifall du ser några på det övergripande perspektivet några potentiella cyberhot mot fordon utrustade med  
den här tekniken då och if so are there any security measures against these, så om vi börjar då med dina day one du valt  
100 här, lite tankegången kring varför du valde just dem här då  
EEBL för att det kommer vara väldigt bra funktion ur ett säkerhetsperspektiv när våra on board sensorer inte kan  
102 detektera när bilen längre fram den bilen du har precis framför dig gör en panikbroms, dina sensorer du har idag kan  
inte detektera det, och det är en väldigt hög risk att bilen framför dig gör en tvärbräms som du reagerar för sent på

- 104 Så när du säger säkerhet här nu då så menar du då safety  
Ja precis
- 106 Ja men exakt, och, är det någonting mer du vill säga kring dem alla fyra, har du valt dem enligt något  
Ja, om jag fortsätter med nästa då så emergency vehicle approaching, blåljuvarning när man kör på motorväg och så är  
108 det inte alltid så lätt och höra att en ambulans eller polis kommer du sitter och lyssnar på musik och (likadant) du pratar  
i telefon och att kan du få en sän notification så är det väldigt bra
- 110 Mm  
Och den särskilt som poliser så vill dem ju gärna jag har svårt att tänka mig att dem gärna vill lägga det i molnet i en  
112 databas, kör du det lokalt, att när dem slår på sirenerna och slår dem även på en ITS-G5 sändare eller C-V2X sändare  
samtidigt
- 114 Mm  
Det är en helt annan grej ur ett cybersecurity perspektiv då också, det är nämligen  
116 Justeja, så då blir det lite mer, jomen samma funktionalitet menar du där som med hur man hämtar hem jomen weather  
reports och den delen liksom från cloudet att emergency vehicle rapporterar då från där dem är och att man hämtar  
118 det från en databas som du sa  
Ja eller man gör inte det, jag menar
- 120 Ah man gör inte det, utan det blir den liksom direktkommunikationen  
Direktkommunikationen för att jag antar att dem vill inte ha det i en databas för den går ju lätt och hacka  
122 Ja, jomen då förstår jag vad du menar, jomen bra  
Då kan ju bara tjuvarna ha koll på ah okej här är snutarna liksom  
124 Ah men exakt, det var bra att vi förtysligade det  
Nä så att där ser jag fördelar med att det (bara) är direktkommunikation för att slår dem på sirenerna så vill dem ju ändå  
126 göra omgivningen medveten liksom  
Ja  
128 Sen intersection collision warning ah det är också för att minska trafikolyckor här i dolda korsningar eller om du har, vi  
gör en vänstersväng och du har, flera filer i andra motsatta så du är skymd där och en bil kommer och kör för fort eller  
130 natt och du kan liksom få nån varning  
Ja, och denna varning baseras lite då på, eller man kan säga att den, det här use case öppnar upp möjligheten för det  
132 här none line of sight awareness då  
Ja precis, det är ju där vi verkligen då har nytta av teknologin  
134 Amen precis  
Och sen sista SPAT kallar man väl den va  
136 Ah ok, ah det visste jag inte  
...  
138 ...  
Det är mer en bra kundfunktion, när man står vid rödljuset så är det skönt, upplever jag det att det hade varit skönt och  
140 veta är det 5 sekunder kvar eller är det 30 sekunder kvar innan det slår om till rött, eller grönt menar jag  
Mm, nä men superbra, som sagt ur ett cybersäkerhetsperspektiv då nu då har du ju redan nämnd det här då ur ett  
142 cybersäkerhetsperspektiv men om vi tar, omen nån av de andra use casen där då, vad ser du för potentiella risker kanske  
med att införa någon sån här, natt sånt här use case  
144 Inga direkta problem, visst du kan ju alltid, se till och ha en sän notification och skicka ut såna här meddelanden längs med  
motorvägen, men då måste du ju vara där på plats då och ha ställt dit den liksom typ för (och senast kommer du ju  
146 hitta den enheten), annars så har vi ju ett inbyggt PKI lösning så alla utrullade system ska ju vara godkända och liksom  
uppfylla standarder och tillvägagångssättet sen klart det går ju alltid missbruka liksom  
148 Ja, jo precis den tidigare kandidaten jag pratade med sa lite om liksom faulty messages då alltså meddelanden med  
liksom falsk information eller vad man ska säga, och då var han ju inne på det med day one use casen att det är ju inte  
150 en stor, det kanske inte sker någon stor konsekvens för det då riktigt, men då blev jag mer men såhär jomen, kan man  
inte bara utifrån liksom alla andra fordonsinformation liksom pin-pointa det fordonet som ger ut falsk information och

152 blacklista den då, men då var han inne på det där med pseudo anonymiteten då att det blir ju svårt från det perspektivet,  
så då insåg jag lite problematiken där då

154 Ah och du kan ju skicka felaktiga koordinater och sådant där, men du måste ju ändå göra det på plats i den enheten det  
är ju rätt bökigt, du kan inte, fördelen med direktkommunikation, visst du kan lokalt skapa kaos, men du måste sätta dit  
en utrustning där som gör det, du kan inte hacka ett helt land med detta som du kan göra med, eller en hel region som  
Europa om du hackar data för road safety molnet till exempel och dissemenerade felaktig information den vägen

158 Nä justeja, nä det blir ju mer lokalt ja precis, yes, men jag tänker att vi hoppa över till day två då

Ja

160 Varför du har valt dem här use casen

Här tänkte jag mig att vi börjar utbyta, eller vi börjar med första ACC string att vi, ACCn idag låser man på första bilen  
men om man kan låsa ett helt tåg få ännu bättre flöde i trafiken, emergency break assistance att vi faktiskt inte bara  
skickar information utan även bromsar på ett sånt meddelande, där är det ju, där vill man ju verkligen veta att det är  
korrekt information man får emot, eller tar emot, för annars kan ju det vålla stor skada, collective perception service  
för ad, ja att vi faktiskt börjar utbyta information om jag med min radar ser objekt som kanske andra bilar inte ser  
med sin radar till exempel barn som springer bakom en buss eller nått så är det ju väldigt bra att man skickar ut den  
informationen och så får dem den informationen via direktkommunikationen istället då, och sen vulnerable road user  
protection

Om jag avbryter dig lite snabbt där bara, för det var väl lite också med intersection collision warning, vad för nu är det  
ju autonomous driving där då väl som är AD

Ah men för mig är interception collision warning, då är det, där skickar du, bygger bara på att du skickar din riktning  
hastighet och dina koordinater som din egen bil har, i collective perception så skickar du ju din lokala (egna) position,  
riktning och hastighet men du skickar även omgivande objekt som du ser i andra bilar och fotgängare och liknande  
deras riktning och hastighet

Ja justeja

176 ...  
...

178 Collective perception service kan vi jämföra lite med hur Kina gör med road side units, att dem sätter ju upp ganska  
många såna här road side units med en radio i, en C-V2X radio, men även då med en radar eller en kamera som  
detekterar alla objekten i den korsningen och så dissemenerade dem den informationen via radio då så alla bilar i  
området kan ju ta emot information om alla objekt i korsningen vilken rörelse dem har då även fast du inte kan upptäcka  
dem med dina egna radar eller kamera nämligen, så det är ju väldigt fiffigt för att öka man kan väl säga penetrationen  
av, och öka effektiviteten av systemet lokalt då

184 Mm, juste

Sen sista day två vulnerable road user protection tror jag inte så jättemycket på egentligen men jag ville ta upp den  
[unclear] det vore väldigt bra om det funkade att vi kan varna fotgängare och cyklister

Vad är din tveksamhet då?

188 Problemet är positionen av fotgängare eller cyklister är extremt dålig för att dem kommer ju ha en mobiltelefon med  
C-V2X då kanske i framtiden, ITS-G5 mer tveksam, och för jag är lite förvånad att det inte står V2P där, det står I2V  
och V2V nämligen, för mig är det V2P

Ja justeja, jomen så heter det ju väl, ah precis

192 Men då, för att i en bil kan du ju få väldigt bra noggrannhet på positionen för att du använder GNSS du använder dead  
reckoning du använder ah, linjemarkeringar och liknande för att bestämma din position medan din telefon så använder  
du bara GNSS och i en stadsmiljö så har du kanske en noggrannhet på 50 meter så att fotgängare kan likaväl vara  
andra sidan kvarteret som du (varnar om nämligen), så därav, utöver landsbygden i mörker kommer det funka, men i  
stadsmiljö så kommer du inte kunna använda funktionen förrän du har en noggrannhet på bara några få decimeter, du  
vill ju inte varna för alla gående på trottoaren liksom

198 Nä justeja det är ju klart

För jag menar du kommer ju bara stänga av funktionen du kommer få så mycket falskalarm så

200 Ah det behövs ju himla precision där ju

- Ja, men det nämner ju inte Qualcomm och co. när dem marknadsför det här men
- 202 Men ok ah, men det är ju som sagt, ah men som du säger ett väldigt, om det är liksom om funktionaliteten blir så pass  
precisions, liksom, fungerande då är det ju ett otroligt viktigt use case så det är därför du har valt det då, mer eller  
204 mindre
- Ja fast så ville jag ändå att du skulle få denna bakgrund med den här problematiken som finns, men vi i Sverige som på  
206 landsbygden när du kör en bil och det börjar bli mörkt och skumt och du varnar för en cyklist som kommer
- Ah det är ju bra ju, det blir ju lite som den här personal or animal on a road då, den fanns väl på day one också  
208 Ah det gjorde det kanske ja
- Mm, ah men precis, för ja, det kanske är till och med två stycken mer än dig som varit inne på det här i alla fall är det  
210 en i så fall, eller om det är fler, nu har jag inte riktigt koll på alla men dem har inte tagit upp den problematiken så det  
var ju du faktiskt först med här så det var intressant och bra, den senaste pratade mycket om, för han var också skeptisk  
212 till hur man kunde ha det implementerat i mobilen han såg inte det som att det är någonting kanske dem här omen  
mobiltillverkarna skulle nödvändigtvis implementera pga. kostnader och annat då men istället att det skulle vara mer  
214 stationerat i infrastrukturen, men då krävs det ju även där en så himla precision så det är fortfarande samma problem då  
ju
- 216 Ja, men med infrastrukturen, det är eventuellt möjligt med för många 5g telefoner har millimetervågor nu och då kan  
du nog positions bestämma telefonen betydligt bättre än vad du kan göra med GNSS, men det innebär då måste du ju  
218 ha dem här 5g basstationerna eller den här tekniken överallt
- Ah en jätte kostnadsfråga där då
- 220 Ah och den utrullningen går ju inte så där jättefort heller, och det är ju frågan ens om du kommer ha, du kommer ha den  
5g infrastrukturen i köpcentrum och verkligen down town men där kör inte så många bilar liksom så att
- 222 Vad är det 5gn utifrån ditt perspektiv, vad är det den bidrar med främst
- I så fall, om den inte är implementerad [unclear] i mobiltelefonen så skulle om, 5g om man använder millimetervågs-  
224 bandet där så får du mycket större precision på hur du kan bestämma var telefonen är, för du har bättre bandbredd,  
och då kan du få mycket bättre upplösning i tid och vilket du kan då få en bättre upplösning när det gäller position så  
226 då kommer dem infrastrukturen kan bestämma mycket noggrannare var dem olika smartphonesen är någonstans och  
på det sättet då disseminera informationen via V2P då, den informationen då, men det är lite omständligare då ska det  
228 finnas en infrastruktur och andra sidan så ska ha denna kapabilitetens då
- Ja, japp, intressant, svinbra information verkligen, men då går vi över till, eller har du någonting mer att säga om  
230 vulnerable road user
- Nä jag var nog klar där
- 232 Jomen då kör vi slutligen day three då
- Ja, cooperative automated parking tror jag kommer vara en fantastisk bra kundfunktion, för att du kommer till ett,  
234 ska in i stan, det blir färre och färre p-platser du bara hoppar ur bilen och den kör och parkerar sig själv i ett stort  
shoppingcentrum, det kommer vara väldigt uppskattad funktion därför oftast är det du får gå kanske en kvart eller  
236 någonting för och, du sparar tid helt enkelt
- Ja det är ju ett väldigt omen som det både står där då i kategorikolumnen både safety, efficiency och comfort, det blir  
238 ju allting i ett liksom, och det tog också även en annan intervjukandidat upp om att det kommer spara otroligt mycket  
pengar för att liksom små parkeringskrockar kostar liksom, kanske inte sker så stor skada alltså på förare eller end user  
240 då men det är fortfarande otroligt mycket pengar liksom slösas där kan man ju mer se det som, men ja, intressant val  
där, nice och som jag sa också jag märker här nu att ni väljer ändå samma use case i ganska stor utsträckning, så ah, det  
242 är intressant
- ...
- 244 ...
- Det är också spännande, dem tre sista tänkte jag prata om tillsammans nämligen
- 246 ...
- ...
- 248 När vi väl har självkörande bilar i det här fallet är det motorvägar, vi [unclear] i svacka nu efter hypen för några år  
sedan där vi då skulle vi ju redan ha självkörande bilar på motorvägarna nu, men då har man ju insett att det här inte

250 var så enkelt vilket jag trodde det var från början, men då så, vill man ju inte, jag kan ta ett exempel om jag kör mellan  
 Göteborg och Malmö och åker i min självkörande bil då vill inte jag fastna bakom första lastbil på E6an sen blir  
 252 jag liggandes där i 80 km/h ner till Malmö  
 Ja den är dryg  
 254 Då måste ju den självkörande bilen vara så smart att den kan köra om den där lastbilen och hantera bilar som kör av  
 avfarten eller kommer på avfarterna, och göra filbyten kontrollerat, utan att jag som förare behöver göra detta utan jag  
 256 ska kunna läsa min bok eller slappa liksom  
 Ah, jomen verkligen  
 258 Så det är, och alla tre ingår ju liksom i det scenariot, du behöver ju kunna göra filbyte, med självkörande bil behöver  
 kunna göra filbyten utbyta information där, hantera på och avfarter och ha ett samarbete där, och sen även köra om en  
 260 lastbil eller en annan bil liksom som har jag ställt in på 110 jag har svårt och tänka mig att det går att ställa in det på en  
 högre hastighet än skyldad hastighet  
 262 Ja det är väl också ett, jag vet inte vilket day det är, use case men att det är den här, jomen att man ska få, vad säger  
 man, hastighetsgränsningarna direkt i bilen liksom  
 264 Ja, nä men att för jag menar om det är 110 och det är en annan bil som ligger i 100 eller lastbil då eller buss så ska ju  
 den självkörande bilen klara av och köra om bilen eller framförvarande fordon  
 266 ...  
 ...  
 268 Men sen också, jag är lite nyfiken på varför du inte valde platooning  
 Ah jag var inne på det ett tag men sen så (såg jag den här automated parking) för jag tänker det är mycket mer värdefull  
 270 funktion, kundfunktion, så tänkte jag lite mer bilperspektiv, i ett lastbilsperspektiv kommer det funka, om du har en  
 förare i första fordonet, du måste ha föraren någonstans för annars du kan inte ha helt självkörande bilar som åker i  
 272 ett tåg för då kommer det komma ligor som på natten bara kör framför lastbilarna så stannar dem och så tömmer den  
 lastbilarna på lasten och så har du förlorat syftet med den funktionen  
 274 Det var ju en intressant syn på det, det är klart  
 Ja sen för bilar så, ja det går ju hand i hand med ACCn där, du kan inte ligga, platooning tänker jag mig i regel att du  
 276 ligger väldigt nära varandra, det har gjorts ett projekt för många många år sedan, du kan inte lägga en bil bakom en  
 lastbil väldigt nära väldigt länge för att den drar upp så mycket grus så din front är helt sönder så du får lacka om bilen  
 278 efter en resa emellan Göteborg och Malmö nämligen, så att därför så, ACC med liksom längre avstånd, alltså vanliga  
 avstånd men att du liksom optimerar flödet men att du inte, ur ett luftflödes energieffektivitetsprincip så borde du bara  
 280 kanske ha 5 meters avstånd och då skulle du kunna köra, men du sliter sönder lacken på bilarna  
 Ah, det finns väldigt många olika perspektiv och se det utifrån, för det är ju klart också ett problem, det är ju en jättestor  
 282 kostnad där med  
 Ja så jag menar efter att ha gjort det en gång så kommer du ju aldrig göra om det igen  
 284 Nä men jag tänker mig att man kanske inte ligger efter nu när man, liksom nu när man ändå har valet eller vad man ska  
 säga, att man ligger kanske inte efter en lastbil hela vägen då, men just i det fallet med dem här use casen så kanske det  
 286 blir så men ah det får man ju se över  
 Och sen tror jag kanske olika här, ah det är en gränsdragning där mellan ACC och platooning, jag tror vi får börja med  
 288 cooperative ACC så får vi se hur det (använts helt enkelt)  
 ...  
 290 ...

## B.4 Interview Candidate 4 (IC4) Interview Transcript

Tar sin lilla stund innan den här, vad heter det pop-uppen kommer, jag väntar tills den så jag vet, så och då frågar jag

2 dig här nu då ifall det är ok att du medverkar i den här intervjun och att jag spelar in den

Det är ok att du spelar in intervjun och att jag medverkar

4 Ah, super, yes men då ska jag dela min skärm här nu

- ...
- 6 ...
- Ja alltså standarden har ju funnits, nu kan jag inte datumen men, pilotprojekt i, framför allt, USA gjordes ju redan mitten  
8 på, alltså säg från 2005 och framåt, gjordes piloter, och riktiga standarder har ju funnits på plats början på 2010-talet,  
säg 2011, 2012 nått sådär
- 10 Justeja med den
- Och mycket piloter och mycket tester men det har tagit väldigt väldigt lång tid och komma till beslut om vilka standarder  
12 som ska gälla då, äntligen har vi lyckats sätta ner foten, och då pratar jag framförallt då om de här meddelandeprofilerna,  
de här som ETSI och IEEE/SAE har tagit fram i Europa respektive USA, då kom ju det här med vilken bärare man  
14 skulle använda, för fram till dess, fram tills för, vad kan det ha varit, 2018 nått sånt där, då var det rätt så solklart att det  
var 802.11p som gällde, alltså den här wifi baserade kommunikationstekniken
- 16 För oss i Europa då tänker du på
- Njae alltså överhuvudtaget
- 18 Överhuvudtaget i hela världen
- Ja, möjligtvis med undantag av Japan som haft ett eget frekvensband allokerat för safety tillämpningar i, på fordonssidan,  
20 men då, telekombolagen kan man väl säga kom i någon slags allians, gjorde en väldigt, mycket politisk påverkan  
för att förhindra att man började lagstifta om införande av den här tekniken därför att dem ville att man skulle titta även  
22 på deras alternativ då, det som vi kallar för C-V2X eller PC5, med den här side-band peer-to-peer kommunikationstekniken  
som bygger på samma radio som man använder för mobila nätverket då
- 24 Justeja
- Och den striden kan man väl säga den är inte riktigt avgjord än, även om just nu ser det ut som att i USA så kommer  
26 man att köra på Qualcomms teknik dvs. PC5 eller C-V2X, medan i Europa så har man sagt att politiskt vill man inte  
ta något beslut, men den teknik man inför måste vara bakåtkompatibel och eftersom Volkswagen redan har rullat ut en  
28 massa bilar med 802.11p så kan man väl säga att det kommer att bli en de facto standard i Europa
- Ja, det var väl, det var väl väldigt nära att det beslutet togs att det skulle bli liksom short range kommunikation
- 30 Short range, det där är lite farligt, alltså short range är (det ju i bälge fallen), vare sig vi pratar om 802.11p eller PC5  
så (är det) short range, men det här PC5 tekniken bygger på att man kan använda samma radio som man använder  
32 för mobil-nätverkskommunikationen, så att du kan ha en dual mode radio som använder den här mobila nätverks-teknologin, men även pratar direkt med andra bilar, så det är fortfarande short range i det här fallet
- 34 Oj då, det har jag delat upp det som long och short range
- Nä, long range specifikationen är än så länge väldigt o-standardiserad kan man säga, alltså för att undvika missförstånd  
36 så brukar jag försöka undvika termen C-V2X därför att då vet man egentligen inte riktigt vad man pratar om är det  
PC5, dvs. short range mobiltekniken eller är det Uu som är long range mobiltekniken, så PC5 är peer-to-peer, alltså i  
38 praktiken funkar det likadant med alla standarder och meddelandeformat och så ovanpå som 802.11p, medan Uu är den  
här, alltså det vi normalt sett kallar för mobilt internet
- 40 Ja ok
- Och där kan man väl säga att det är först nu som det har börjat komma lite standarder på hur man kan tänka sig  
42 använda det i inom ramen för projekt som CRoads till exempel, annars så är det väldigt mycket (proprietär) tekniker  
som används där, alltså i princip alla moderna bilar som har någon typ av moln-uppkoppling idag kan du (ju säga)  
44 har V2X long range i sig, alltså är det en Volvo som har emergency call eller en BMW som laddar ner kartdata med  
trafikinformation, alltihop det ingår ju i någon mening i ett V2X nätverk, men det är ju inte det vi pratar om här kanske  
46 när vi pratar om det som, det som ETSI eller IEEE har standardiserat och dem use cases vi kommer prata om
- Ah ok
- 48 Det är, om jag får ge dig ett tips så är det väl undvik termen C-V2X, för den är lite farlig, var ganska tydlig med att om  
du pratar om 802.11p, PC5, eller Uu
- 50 ...
- ...
- 52 Ah men, och det är väl litet problem med många av dem här termerna man slänger sig med att beroende på vem man  
pratar med så kan dem ha lite olika betydelse, C-V2X är ett sånt typexempel för, pratar man med svenska vägverket

54 till exempel, dem pratar bara om long range, dem är inte nått intresserade av short range kommunikation, så för dem är  
C-V2X det är självklart att då är det long range man pratar om, men i många andra fall, alltså, om du skulle prata med  
56 Autotalks till exempel, för dem är C-V2X det är definitivt PC5  
Då är det PC5, ah ok  
58 Ja så att, och man bör vara tydlig att presentera, och detsamma gäller ju med dem här, alltså när man pratar om use case  
day one, day två och day tre till exempel, det är lätt att förledas och tro att det är väldigt tydligt definierat vilka use case  
60 som är vilka, och vad day one egentligen betyder, det är ganska luddigt  
Det kan man ju, ja, det tycker jag, kan jag säga, men ja, jätteintressant, vi går vidare här nu då också, men jätterelevant  
62 information där du tog upp, så tack så mycket, och här har vi redan varit inne lite på då den här frågan, men är det  
någonting du skulle vilja tillägga där kanske med liksom i vilken fas V2X är eller nått sånt där du skulle säga om  
64 Ja men det som är positivt kan man väl säga är att Volkswagen har varit så pass modiga att faktiskt rulla ut det här,  
alltså för det är ju verkligen ett hönan och ägget problem, dem rullar ut miljontals bilar på vägarna trots att dem inte har  
66 någon annan att prata med, och lägger ganska mycket prestige och pengar på det här, men någonting som vi alla tror  
jag kommer ha stor nytta utav, för de här innehänder att, möjligtvis tillsammans med kinas och, så går ju Europa i [unclear]  
68 för den här trafiksäkerhetssatsning då som V2X är, vi kommer ligga långt fram, USA kommer ha en lång väg och gå  
i och med att dem har backat nu och förmodligen kommer byta spår på vilken radioteknik man ska använda, och dem  
70 har ju haft mycket problem med sina allokeringar av frekvenser och sånt där, det andra man kan säga är väl, att om man  
ska få det här och gå fort framåt så tror jag att det är dem här alltså krocksäkerhetstesterna, eller trafiksäkerhets, alltså  
72 typ NCAP och Euro NCAP, om man ska verkligen få det här att rulla ut snabbt och bli standard i bilarna så är det ju  
när dem organisationerna faktiskt börjar dela ut poäng för att man har V2X med i sin bil, och det är på gång det har väl  
74 också tagit lite längre tid än vad jag trodde men när det väl kommer, för alla prestige biltillverkare är ju supernoga med  
att ha fem stjärnor på Euro NCAP och NCAP  
76 Justja  
Och det innehänder ju att, då måste, då kommer dem vara tvungna att ha V2X för att kunna få dem här fem stjärnorna, så  
78 det tror jag är nästa stora steg  
Men varför har det liksom, eller ja, det är kanske dum fråga, men varför har dem inte haft det som kriterie lite tidigare  
80 då när man som redan 2017, eller tidigare liksom hade förväntningarna av att det ändå skulle gå lite snabbare än vad  
det har gjort  
82 Jag tror det har att göra med, alltså, bristen på standarder, både ETSI och IEEE, har ju varit ganska duktiga på att tagit  
fram dem här meddelande-standarderna, dem som används då för att alltså i Europa typiskt ETSIs CAM och DENM  
84 meddelanden dem har varit hyfsat stabila under ganska lång tid, men det som inte har funnits på plats har väl varit två  
olika saker, security, hur certifikathanteringen fungera rent praktiskt, där bytte man för några år sedan till en standard,  
86 certifikat-standard och PKI teknik som mer påminner om det som man använder i USA, vilket ju födröjde en del och  
det andra är att dem här meddelande-standarderna är ganska så generösa, alltså det finns mycket tolkningsutrymme,  
88 det finns många olika sätt att göra samma sak både i den amerikanska och den europeiska meddelande-floran, så det  
som har, man har jobbat mycket med nu dem sista åren är ju profilering, alltså vilka, hur ska dem här meddelandena  
90 faktiskt användas för att det ska bli interoperabelt, och det är det som organisationerna som Car-2-Car communication  
consortium, alltså C2C och även projekt som CRoads har jobbat jättemycket med, att tala om att om man ska skicka en  
92 CAM så ska dem här fälten vara ifyllda och dem här fälten ska inte användas till exempel, och likadant Car-2-Car har  
mycket jobbat med hur vad är triggering-conditions för dem här olika use casen, och när man triggar EEBL vilka fält  
94 ska fyllas i, det är jätteviktigt för att det ska bli användbart för annars kommer vi inte ha ett system som är interoperabelt  
och då blir det ju helt meningslöst  
96 ...  
...  
98 Då vill jag att du ska göra följande enligt den här frågan, så from your perspective of expertise within this area, choose  
four day one use cases, four day two use cases, and four day three use cases that you consider will have or already has  
100 a significant role for traffic situations, och då fokuserar på då det med already has vad Volkswagen har implementerat  
då exempelvis, och då kommer jag dela med mig av det här Google docset som jag har gjort, och först vill jag bara  
102 definiera lite vad jag menar med significant role, och då är det use cases that you consider are the most relevant or

predominantly crucial thinking from the core of V2X technology, och då syftar jag lite på det här med traffic efficiency och safety, så det är en, det kan vara en väldigt svår uppgift eftersom att varje use case är ju viktigt på sitt egna sätt givetvis och det du var inne lite på innan med att use case liksom definitionen eller deras beskrivning kan vara lite diffusa även dem

104  
108  
106  
108  
109  
110  
111  
112  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150

Ja, det här med day one, day två, day tre är ju, det är ju väldigt flytande gränser och, som sagt lite beroende på vem man pratar med, vad är det som man egentligen pratar om, men vi utgår från den

Precis, du utgår från det här och det tolkar ju du det på ditt sätt då, såklart, så mycket mer info än så får du inte

...  
...

För det är ju jättesvårt att välja bland day två och day tre eftersom det inte har kommit så långt än, men vi börjar från start med day one use cases, och då är det ju svårt att inte prata om dem sakerna som faktiskt redan är implementerade av till exempel då Volkswagen, så att jag skulle ju säga, sen är det ju uppdelningen här blir ju också lite svår

...  
...

Men ja, vi börjar med EEBL i alla fall

Japp

Den definitivt med, därför att den är ett sånt use case som, dels är det implementerad av Volkswagen och det är väl specificerat av Car-2-Car och det är ett väldigt vanligt use case exempel när man pratar med folk om det här, alltså OEMer och tieretter, det är, EEBL är alltid med i dem diskussionerna

Vet du får jag bara avbryta lite snabbt, för när dem, tanken är att när du sen valt use case ska vi gå igenom dem här frågorna, och dem här två är ju också generella men jag vill gärna höra din syn på det, så då tänker jag att vi kör varje use case och så tar vi dem här frågorna där då

Vi börjar med att välja, då tar vi EEBL

Yes, japp det har jag gjort

Och, emergency vehicle approaching måste ju vara med

Japp

Road works warning, lane closure, och jag fick välja fyra sa du

Fyra av day one ja

Ah då tar vi hazaourdus location weather condition warning då

Då ska vi se, då har du valt EEBL, och emergency vehicle approaching och sen så sa du lane closure

Lane closure precis

Och weather condition sa du

Ja

Japp, ja då har du fyra där

Då går jag ifrån min egen regel och tar dem som Volkswagen har implementerat men, men ja, då ska vi se, day två, motorcycle approaching måste ju definitivt vara med, sen vad som är skillnad på motorcycle approaching information och motorcycle approaching warning vet jag faktiskt inte, jag har inte, för mig är dem där två samma sak, men ta den första där då motorcycle approaching information, eftersom det är den som, nä Car-2-Car säger du ju jobbar på motorcycle approaching warning, ah ta den då

Mm, motorcycla approaching warning and protection, eller or protection

Och sen så måste det ju vara emergency vehicle priority, nä men vänta lite, det är ju en day one, ah jag har råkat sortera om här, ah förlåt, glöm den

Mm

Glöm den, kunde man inte få ta fler av day one istället

Jo alltså, jo jag vet, jag har ju valt lite speciell metod som, men jag tänker jag vill ändå liksom se vad ni väljer på day två och day tre också

Ah, jag förstår, jag förstår, nä men, cooperative acc måste ju vara med i alla fall på day två

Japp

Collective perception, jag tror att den ska vara med

152 Japp  
Och vulnerable road user protection, det var fyra va  
154 Mm, så day tre nu då, eller day tre plus  
Känns väldigt (ovetenskapligt), jag bara sitter här och tar sånna som ger mig en bra magkänsla  
156 Ah jo jag vet, men, omen jag tänker ändå det som känns bra i magen det är ändå utifrån nån slags instinkt där  
Ah, nä men day one är ju lite lättare för där har man ju koll på standarderna så dem är ju rätt så väl utvecklade, men på  
158 day tre så är ju platooning definitivt med, och där med måste man ju också ha cooperative emerging assistance, och jag  
skulle säga även cooperative lane change borde vara med där då  
160 Mm  
Man kanske borde ta något annat också  
162 Mm nu har du en kvar där i så fall ju  
Omen då kör vi, automated green light optimum speed, bara för att den inte fick vara med bland day one så tar vi den  
164 Alltså automated, nä där har vi den, advisory eller with negotiation  
Nä skippa negotiation  
166 Japp  
Vi tar den enklare först  
168 Yes, ah  
Det var fyra va  
170 Bra, det var fyra ja, då kan jag göra som så att vi sorterar dem bara, fyra där, fyra där, ja, suveränt, men då är jag  
intresserad nu då av att höra lite tankegången kring varför du valt just dem här use casen  
172 Då måste jag, då ska vi se, då ska jag dra upp så jag ser ordentligt på min skärm, jo men EEBL är som sagt var, dels  
är det ett use case som, det är redan implementerat av Volkswagen och utrullat på vägarna, det är ett av dem som alltid  
174 nämns när man pratar med OEMer och tieretter om vilka use case dem vill ha, det finns alltid med på den här short  
listen över use cases, och den är väldigt tydligt definierade det finns bra specifikationer från Car-2-Car, och förresten,  
176 om vi bara ska backa ett steg  
Yes  
178 Du har bara valt europeiska use case här nu  
Ja det har jag, men samtidigt så, jag utgick faktiskt från Car-2-Car's där då senaste use case roadmap, och det får helt  
180 enkelt bli att jag snävar in mig på Europa  
Ah men jag tycker det är bra, för det blir genast lite krångligt när man börjar blanda, till exempel EEBL är ju ett sånt  
use case som är tydligt definierat både i Europa och i USA men med lite olika sätt och implementera på och med lite  
182 olika parametrar så att, det finns ju en del andra såna use case också då som heter snarlika saker i USA och Europa men  
184 som är implementerade på lite olika sätt, det är ju bra om du är väldigt tydlig med det i din, när du skriver att nu, det  
här är med europeiska ögon och med ETSI standarder, alltså  
186 Bra synpunkt  
Så att alla är med på det  
188 Ja  
Annars kan det lätt bli lite förvirrat, jo så EEBL är, känns självskrivet, emergency vehicle approaching, lite samma sak  
190 kan man säga, det är implementerat och finns utrullat av Volkswagen, det är väl specificerat både av CRoads och av  
Car-2-Car, det är ett intressant use case på det sättet också att här är det inte självtäckt att man pratar om short range  
192 communication utan den här informationen kan också komma via long range kanalen, och fungera bra i bågge fallen,  
man får lite olika beteenden man får lite olika, alltså responstider så där, men det är värdefullt med den här informationen  
194 i bågge kanalerna, både long range och short range så därfor är det intressant och jämföra det här use case beroende på  
vilken kanal man använder, så att därfor är det ett bra use case, och det är dessutom rätt så, i short range kanalerna är det  
196 inte särskilt väl supportat men om man tittar på long range kanalen så finns det många kommersiella aktörer som redan  
skickar ut den här informationen, och därfor är det bra, ungefär samma resonemang med nästa då, weather condition,  
198 väl specificerat av Car-2-Car, alltså triggering conditions är tydliga, det är många som pratar om det här use case, det är  
användbart, samtidigt så kan man förutom att använda bilarna som sensorer då såsom Car-2-Car har specificerat det så  
200 kan man använda det såsom som CRoads har specificerat det, d.v.s att väghållaren kan skicka ut information om att det

är dåligt vägtag på nått ställe med hjälp av sina vägsensorer då, så att, det är också ett use case som är användbart både  
202 för short range och long range kommunikation, och har goda möjligheter att rädda liv, den sista lane closure har jag  
egentligen valt mest, alltså, det här gäller ju road works warning i största allmänhet, men eftersom du hade valt att dela  
204 upp det i dem alltså, det var olika, alla dem här fyra egentligen då, lane closure, road closure, mobile road works,  
och winter maintenance dem är väl alla egentligen det huvudsakliga fjärde valet då, alltså dem har ju helt liknande  
206 egenskaper men, ja, jag var ju tvungen att ta en så då tog jag en  
Ah men det var bra att du tog upp liksom dem det stod emellan också, det kan vara intressant att ta med sen faktiskt  
208 också, så det var bra  
Dem fyra fungerar ju på (liknande) sätt det är ju egentligen ingen skillnad på dem, förutom, liksom vem det är som  
210 skickar dem och varför man skickar dem  
Alltså liksom informationsbäraren är densamma men informationen är olika liksom  
212 Nä, egentligen är informationen samma också förutom en, att man har olika, vad heter den, SCC, sub cause code tror  
jag  
214 Ok, vad är det för nått  
Alltså i DENMen som man skickar ut så är det en cause code som är, road works warning, och sen en sub cause code  
216 som är till exempel lane closure, road closure, winter maintainence, så att det är ju inte ett sub use case  
Alright, japp  
218 Men i allt väsentligt så fungerar dem likadant  
Mm, men ah jag vet inte, ska vi gå vidare  
220 Om man jämför med den som du hade innan då till exempel hazardous location, det är ju samma sak där, det är ju också  
en cause code, och sen så är dem olika som finns efter där, weather condition warning, fog, precipitation, traction loss,  
222 det är ju också olika sub cause codes  
Justeja  
224 Det är egentligen samma sak som om du hade buntat ihop alla road works warning till en  
Mm jag förstår, det var också ett bra förtydligande  
226 [unclear] beror på att man valde att klumpa ihop dem i CRoads specifikationen av någon anledning som jag inte riktigt  
vet faktiskt  
228 Ok  
Ah  
230 Japp  
Men lane closure, ett bra use case därför att, återigen när man pratar med till exempel svenska vägverket eller  
232 motsvarigheten i Europa, Europeiska länder, så är det här ett väldigt viktigt use case för dem där för att man ser stora  
möjligheter att rädda liv framför allt på vägarbetare som är ute och jobbar på vägen och dem här inbromsningsolyckorna,  
234 påkörningsolyckorna bakifrån när det är vinter, alltså typ snöplig eller sådär som är ute och kör, så är det många  
fall att man blir påkörd bakifrån och det är en helt onödig olycka  
236 Verkligen  
Så att, det är ett bra use case på det sättet  
238 ...  
...  
240 Då får du nog förklara lite mer vad är det du vill veta ur ett cybersäkerhetsperspektiv  
Ja, nä men, ja, för det blir ju väldigt, ah vi kan se hur du tolkar frågan då, men jag tänkte mer liksom, ser du några  
242 potentiella direkta attacker som skulle kunna utföras på liksom dem här servicen som de här use casen använder sig  
utav då  
244 Mhm, ah men vi kanske ska ta det undan för undan här istället för att klumpa ihop det då  
Japp  
246 Ja, det är ju uppenbart att det finns risker med det här då, så länge vi pratar om day one så är väl definitionsmässigt  
är det väl så att risken för att man ska liksom skada sig eller riskera människoliv är ganska låg där för att vi pratar ju  
248 hela tiden med att bara förse en vanlig mänsklig förare med varningar som föraren sen måste reagera på, här har vi  
fortfarande inte kopplat in bilen i loopen på något sätt

250 Så konsekvenserna är lite, dem är lägre här då

De är ju ganska låga om man skulle liksom prata ur någon slags [unclear] perspektiv, men samtidigt så är det klart att en förare kan begå misstag eller bli stressad om det plöstligt börjar skjuta upp en massa EEBL varningar, så det är ju naturligtvis en risk, samtidigt så kan man väl säga att, jag ser egentligen ganska liten anledning för, vad säger man, en adversary, ah, nån som attackerar ett fordon att skicka ut till exempel en EEBL

Yeah, för det blir

256 [unclear] väldigt lite att tjäna på det om man säger så

Men så att, men om vi tänker liksom den här, uppkopplingen liksom emellan då, den som, alltså den som skickar information och den som mottar den, det blir fortfarande liksom en, ser du någon potentiell, alltså öppning där till någonting som skulle kunna utnyttjas i lite större, alltså inte nödvändigtvis, för där när du prata om EEBL då, när liksom spammas ja då antar jag att det blir någon slags förvirring, nån slags DDoS attack ungefär, men ser du att man på något sätt skulle kunna exploatera någonting ytterligare med den här liksom öppnandet av connectivity

262 Om man tittar generellt på tekniken så behöver vi ju inte begränsa oss till när vi pratar day one, day två, day tre, där kan man väl generellt säga att det finns tre hot, det första är naturligtvis som du säger någon slags DDoS attack, ganska enkel att genomföra, alltså vi kan ju lätt störa ut kommunikationen helt och hållet, genom att bara sända ut brus, eller felaktiga meddelanden och därmed sänka kommunikationen, och [unclear] det spelar ju ingen roll om det är day one, day två, eller vilket use case, eller om man använder CAMar eller DENMar eller vad det nu är, det är en väldigt lätt attack och göra, jag ser egentligen inga möjligheter alls att förhindra det, vill man liksom störa ut luftlänken så gör man det väldigt väldigt enkelt, det andra är ju om man skickar in falska meddelanden som tolkas och visas upp för föraren eller i fallet med day två och day tre då faktiskt kanske också påverka bilens beteende, det är ju mycket farligare och där finns det ju möjligheter då och förhindra den typen av attacker men det är ganska svårt med de tekniker vi har idag, alltså både i den amerikanska och den europeiska standarden bygger ju helt och hållet på att vi kan identifiera den som skickar ett meddelande, inte individen men i alla fall med den pseudonym som man använder just för tillfället och kunna lägga upp fordon på spärrlistor men om någon vill skicka falska meddelanden och få tag på certifikat så tar det ju ändå ganska lång tid innan en sån adversary kan spärras i dem här spärrlistorna eller misbehaviour detection, upptäcka att här är det någon som beter sig illa, så att, den typen av attacker är också väldigt svår och skydda sig emot även om det teoretiskt sett går då, men dem tekniker och standarder som vi har valt idag så skulle jag säga att man kan (hålla på) och ställa till med oreda ganska länge innan man blir utspärrad från

278 Ok

Och det är ju det som du är inne på då, kan vi använda den här attackvektorn till något helt annat, alltså kan vi skicka in meddelande i ett fordon som ställer till med annan skada alltså skicka in speciellt konstruerade meddelanden som gör stack overflows eller något sånt där, definitivt men där kan man ju inte säga någonting generellt och det är ju inte heller beroende på om man använder CAMs eller DENMs eller något annat, utan där handlar det ju bara om att den som har implementerat mottagarstacken har gjort ett bra eller dåligt jobb, så på det visst, den attackvektorn är inte annorlunda ut än typ Bluetooth eller wifi eller någon annan liknande

Nä justeja

286 Skillnaden är kanske att man har lite längre räckvidd på 802.11p och PC5 än vad man har på Bluetooth eller på wifi, jag menar vi pratar ju i någorlunda rimliga fall om att åtminstone 500 meter kanske, ah pratar vi long range kommunikation så ser det helt annorlunda ut, men då ser jag också säkerhets, alltså

Safety då menar du

290 Vad man har för möjligheter att skydda sig ser ju helt annorlunda ut där också, nu kan vi hålla oss till short range för tillfället

292 Yes, jo men det låter rimligt

Ja, så det är ju lite generellt oavsett vilket use case man pratar om, så dem i olika fallen eller jag kan komma på just nu, och som sagt var dem två första skulle jag säga, i praktiken omöjligt eller svårt att skydda sig emot, det tredje, måste man skydda sig emot, men det finns inte mycket generellt att säga om det utan det handlar ju om den som implementerat det

298 Snyggt, snyggt diskuterat där, då, nä men jag tycker, för där tog vi också upp som du sa där, där var ju mer generellt för alla då

Ja

300 Då spelar det ju ingen roll vilket use case inom vilken kategori av day one, two, tre det handlar om utan, jag fick in väldigt bra överblickande syn på det där med ditt svar

302 Egentligen när man pratar om individuella use case så är det väl det andra fallet då att man faktiskt skickar in giltiga meddelanden men med felaktigt innehåll

304 Ja

Alltså man har ett certifikat som är giltigt vilket gör att mottagaren kommer att ta emot det men man förser det med innehåll som inte är korrekt, och det är ju då dem här olika use casen faktiskt kan vara intressanta, vad är det för skada man eventuellt skulle kunna ställa till med genom att göra en sån attack då

308 Nä men precis, nä men sen du var inne lite på det här som med säkerhetsåtgärder, nu är det ju väldigt svårt som du säger och motverka liksom brus och den biten, men om du tittar på säkerhetsåtgärder då är det just, då är det liksom den här PKI, vad säger man, kan man säga PKI infrastruktur, det blir lite dubbelt, men det och certifikathanteringen som vi pratade om, det är liksom, för jag tänker också att för om det är liksom flera cooperative vehicles i ett område då och det är någon som skickar ut falsk information, borde man inte ganska snabbt kunna utifrån de andra fordonens, alltså så att det inte blir någon slags, alltså utgå från att, omen här har vi liksom annan information som inte stämmer överens med det fordonet som skickar ut falsk information, kan man inte ganska snabbt black lista den då eller liknande

...

316 ...

Jag vet bara att vi kommer från dem här PKI, från PKI servern eller från PKI infrastrukturen kommer vi ladda ned dem certifikat vi själva ska använda men även då dem här spärrlistorna, men hur dem i sin tur konstrueras är för mig, fortfarande lite av en gåta, vi har ju, i våran implementation igen misbehaviour detection implementerad över huvud taget, därför att vad jag vet så finns det ingen, ah standard för hur det ska gå till, utan det man kan göra är ju som du säger, i alla fall inte, om någon påstår att någonting har hänt på ett visst ställe men alla andra säger att nä det har inte hänt, då kommer man ju inte och liksom lägga någon större vikt i det, men ändemot så har vi idag ingen implementerad [unclear] rapporterar det tillbaka till PKI till exempel, jag gissar att det kommer och bli så, men just nu är det inte så

324 ...

...

326 Men jag tänker just, för du pratade om day one då varför du valt just dem, men jag tänker du kan ju berätta lite om day two och day three då

328 Det kan jag göra, men eftersom jag inte har listan framför mig då så får du läsa upp för mig vad jag valde  
Ja, ok justeja, då är det cooperative acc först

330 Jo men det är också ett sånt use case som man pratar ganska mycket om i branschen om man säger så, och där man ser att det finns goda möjligheter att, alltså, när man pratar om att den här tekniken faktiskt ska få påverka bilens beteende så känns det som att det här är ett rätt så solklart och ganska enkelt fall och implementera därför att det finns redan grundbultarna till det, dem flesta har ju ändå någon typ av acc fast baserat på radar eller andra sensorer då, och att tillföra då V2X som ytterligare en informationsbärare eller liksom ytterligare en sensor in i den här känns som ganska enkelt och ganska låg risk, därför att du kan hela tiden falla tillbaka på om en sensor säger att det är på ett visst sätt och en annan sensor säger något annat så litar man inte på informationen, därför är det ett ganska bra use case på det viset, man tillför ytterligare en informationskälla eller ytterligare en sensor till en funktionalitet som redan finns och som folk redan är vana vid

336 Ja, och sen ser jag här på adopted messages att den använder IVIM, vad är det för skillnad på den jämförelse med CAM  
340 då, som det också står med, det står både CAM och IVIM

På den, det var konstigt, det måste ju vara fel, det vågar jag faktiskt inte säga vad det skulle vara

342 Men vad är ens IVIM

Ah ok, jo, IVIM är in-vehicle-information, typiskt såsom man talar om alltså skickar ut vägskyltar och annan information

344 Ah okej

346 Så att det, alltså, om du elektroniskt ska skicka ut att det är 50 på en viss sträcka så är det IVIM du använder, eller att på motorvägarna där du har såna här skyltar som kan ändra text, eller ändra hastighet, så är det ju det man använder, man

348 använder också ofta IVIM i kombination med road works warning use case då att du förutom att tala om då att här är  
ett vägarbete så kan du tala om alltså vad är det som häller på att hända, man kan skicka fritext med hjälp av den, så  
350 att på det viset är IVIM ett ganska användbart meddelande, och jag ser här i din, den beskrivningen du har klippt in att  
man kan tala om vart det är tillåtet att använda cooperative acc, alltså typiskt så skulle man väl kunna säga att det här  
352 är en bra idé o använda på motorvägar och större vägar men ganska dålig idé och använda i stan till exempel, och då  
skulle man kunna använda IVIM för att tala om, man skulle kunna göra typiskt nån slags, zoner då där det här inte är  
354 okej att använda till exempel

Justeja

356 Det är min gissning utifrån den texten du har skrivit där, jag har bara

Ah, för att förtärliga så är det ju inte jag som har skrivit texten då heller utan det är ju C2C som jag tagit den listan  
358 ifrån, eller den här listan

Ja, och det är väl därför det står day 2 ivim också där att, det här, dem tänker sig nog använda saker som inte finns i  
360 standarden idag, och det är likadant, det saknas en del saker i CAM meddelandet för att göra det här riktigt effektivt,  
och det är därför man vill göra utvidgningar i det, och det är därför det står day 2 CAM

362 Ja justeja, det blir ju

Det går nog att [unclear] det blir mycket bättre om man kan införa mer, eller lägga in mer information om vad det är  
364 för typ av bil och vad den har för egenskaper, alltså typiskt om du vill kunna ligga närmare en bil, nu närmar vi ju oss  
platooning, alltså ett platooning use case, då är det viktigt och veta liksom hur hårt kan man bromsa, vad är det för vikt  
366 på en bil och så där, för att du ska kunna räkna på fordonsdynamik och så där

Mm, nä men nice, då tänker jag att vi går över till andra då som är collective perception service for automated driving

368 Mm, där är också ett sånt use case som man pratar ganska mycket om, jag har inte sett det användas i verkligheten  
men vi har stöd för det i våran produkt till exempel, och där handlar det ju om att man ska förlänga räckvidden eller  
370 förlänga seendet på fordonets sensorer så man delar med sig av, om jag har på mitt fordon, om jag har en radarsensor  
som upptäcker nånting på vägen framför mig, en fotgängare som går ut i gatan, eller någonting som är i vägen, då kan  
372 jag skicka ut information till bilar runt omkring då, framför allt bilarna bakom, eller dem som kan vara skydda av andra  
fordon, fast här, på den här platsen på vägen så finns det någonting som inte borde vara där eller som man bör se upp  
374 med [unclear] sensorseendet helt enkelt

Ja juste, så det här är ett, verkligen ett sådant use case där det liksom blir det här, å vad är det det heter nu, alltså när det  
376 inte är line of sight utan att det är även utanför det

Ah precis, så att om du är skynd av ett hörn eller av ett annat fordon så kan du ändå bilda dig en uppfattning om vad  
378 som finns där bakom höret till exempel då, det är ju rätt så viktigt för dem här självkörande bilarna som idag förlitar  
sig helt och hållt på till exempel kamerasensorer

380 Ja, jag tänkte precis fråga det en liten, liten annan, eller ah det är ju en fråga relaterat till detta, men vilka är dem liksom,  
dem primära sensorerna för ett sådant här fordon, liksom vilka är det dem använder sig utav, vilka olika finns det

382 Alltså det man pratar om är ju dem som man brukar prata om när det gäller självkörande fordon alltså typiskt kamera,  
radar och lidar, det är väl dem tre som är

384 Det är dem tre mm

Teoretiskt sätt så skulle man väl kunna tänka sig ultraljudssensor men dem är ju bara när det är väldigt väldigt nära, så  
386 ja, jag skulle säga att det är kamera, lidar, och radar

Ja, och då går vi över till, nu har vi pratat om två stycken day två, så vi har två kvar då, så då är det motorcycle  
388 approaching, tredje

Ja, och det vet jag egentligen inte riktigt varför det ligger som day två use case för det pratar man ganska ofta som  
390 day one också, men problemet är att det saknas, man tänkte nog inte riktigt på motorcyklar när man skapade framför  
allt CAM meddelandet, så att till exempel, återigen fordonsdynamik där då, en motorcykel svänger ju på ett helt annat  
392 sätt än vad en bil gör, man kan inte titta på liksom rattutslaget för att avgöra hur en motorcykel kommer att svänga  
därför att du kan svänga bara genom och luta fordonet till exempel, så att du behöver ha lite mer information i CAM  
meddelandet för att kunna dra viktig nytta av det, samtidigt så kan jag tycka att, ja men bara att veta att det finns en  
394 motorcykel i närheten kan ju vara tillräckligt bra och det kan vi ju varna redan för idag med dem CAM meddelanden  
som finns, men för att göra det vettigt och för att kunna dra (riktig) nytta av att till exempel undvika den här typen av

vänstersvängskrockar och sådär, då behöver man lite mer information, och återigen det är ett jätteviktigt use case för  
398 två hjulingar, det är väl det viktigaste use caset för två hjulingar som man tittar på, dem som jobbar med det, Yamaha till exempel är ju väldigt aktiva i det här området, dem pratar mycket om hur man ska få dem här standarderna och  
400 funka även för motorcyklar

Ja det är ju klart, det är ju också en OEM då liksom involverad i detta trots att det inte handlar om just större fordon eller tyngre fordon eller vad man ska säga

Precis

404 Ah det är ju klart  
(Det är väl dem som är) mest aktiva när det gäller motorcyklar om jag minns rätt, (har för mig det)

406 Ah, nä men nice, bra och veta såklart, sen det står här i messages igen då, då har vi day one och day två CAM, men sen har vi en till som är CPM, vad är det för meddelande

408 Det är nog det här collective perception message, som är kopplat till det use caset vi pratade om alldeles nyss då  
Jaa ok

410 Där man skickar ut vad andra sensorer upptäcker  
Ja just nu, det ser jag ju här nu, ja men bra, och då har vi CPM message här nu igen nu då på vulnerable road user protection

Och återigen det är väl för att det är ett intressant, där har man inte kommit särskilt långt, återigen då det finns mycket  
414 standarder och titta på men det är också ett sånt use case man pratar mycket om, alltså hur ska vi få med annat än i första hand så pratar vi ju om bilar, i andra hand motorcyklar, men sen har vi ju alla dem här andra då dem som cyklar  
416 och dem som går, och då finns det ju olika sätt att angripa det här problemet och det ena som man pratat rätt mycket om är att man ska använda folks mobiltelefoner och förse dem med V2X funktionalitet, vilket är en möjlighet, den andra  
418 möjligheten är att man har sensorer på viktiga ställen då alltså typiskt vägkorsningar övergångsställen, som ser att det finns människor i närheten av ett övergångsställe och därmed skickar ut varningar till dem fordon som närmar sig

420 Mm och det kan i så fall, eller ja, det blir kanske troligtvis första steget då i den utvecklingen att det blir först infrastrukturen eller

422 Jaa, det, alltså, jag har ju svårt och tro att man kommer att i närtid bygga in korthållskommunikation alltså V2X radio i mobiltelefonen även om det skulle vara det uppenbart enklaste sättet och implementera det här, därför att det tillför en kostnad, och lite oklart hur man ska använda, alltså man vill ju gärna varna även fotgängaren men det är ju svårt att göra det, man vill ju inte att folk ska gå och titta på sina mobiler hela tiden, så det är lite

426 Vilket vi gör ändå egentligen  
Jaha jo, precis, men alltså, nä jag tror också att det i stadsmiljö så kommer kanske det här att sätta upp sensorer till  
428 exempel vid övergångsställen att va det första sättet att lösa det här problemet, och i andra hand så kanske man kan tänka sig att man skickar ut long walks, alltså långhållskommunikation då att man använder mobilnätverket för att skicka ut  
430 var fotgängare befinner sig, men då har lite privacy frågor som kommer in där som är inte helt lätt och lösa, man vill (ju kanske inte) bli spårad hela tiden, jag vet inte om det är i ditt arbete också att titta på privacy, men det är ju nästan väl  
432 så intressant som security

Ja men verkligen, och ja både liksom privacy, ja [unclear] men det blir ju privacy-perspektiv på hela V2X teknologin  
434 där då ja såklart och inte bara om det hade införts i mobiler, men ja, nä det ingår inte riktigt i så stor utsträckning nu utan nu kollar jag främst på liksom, ah men jag vill se vilka use case då ni väljer och sen kommer jag att fokusera mer  
436 på dessa use case utifrån ett säkerhetsperspektiv av liksom attack vektorer, på det sättet

Det (kan ju vara) bra att ha det i bakhuvudet för att alltså när man pratar om vad man har för möjligheter till exempel  
438 att stänga ut, att svartlista dem som beter sig illa då kommer ju privacy in där för att det är ju, att man har valt det systemet med pseudonymer är ju för att uppnå viss privacy men det gör ju också att det här med svartlistningen blir  
440 mycket svårare

Japp, nä men du har ju en jätterelevant poäng där, så det är definitivt någonting jag kommer ta upp i exempelvis min  
442 diskussion och liksom future work då eller liknande, så jag kommer ju inte undvika det helt på det viset, men ja, omen  
då fortsätter vi till day tre nu då, då har vi automated glosa, eller green light optimum står det, jag trodde det var  
444 optimazation, men optimum speed advisory då

Precis, det tog jag med mest för att jag fick inte med det bland day one use casen, det är egentligen ett viktigt, alltså  
446 GLOSA är egentligen ett rätt viktigt use case för day one också, men kanske blir det ännu intressantare när man faktiskt  
börjar automatiskt att förse fordon med en bra hastighet för att leda dem igenom en korsning eller igenom en serie av  
448 korsningar, då kan man spara rätt mycket bränsle, och få en bättre trafikmiljö i största allmänhet  
Ja jomen verkligen, den är lite samma, fast den kanske är mer lite typ safety på något sätt, ah den kanske är både safety  
450 och efficiency, men med liksom automated parking också att det blir den här liksom, jomen att det blir den här, vad ska  
man säga, det blir rätt från början eller vad man ska säga, den liksom mest effektiva parkeringen eller vad man ska säga,  
452 och så slipper man själv tänka på det, ja men...  
GLOSA tror jag alltid kommer vara alltså, för det har ju, används ju redan om man tittar på både BMW och Audi har  
454 ju det idag fast med långhållskommunikation då och med privata tjänster så dem funkar ju i ganska få städer idag men  
det är ju onekligen en bra tjänst, så att när den kommer som day one så tror jag att den kommer bli väldigt uppskattad  
456 och som sagt var, den stora samhällsnytan kommer ju när man får med dess, att man faktiskt styr bilarna till att hålla  
rätt hastighet och därmed kan få mycket bättre flöde i innerstadstrafik framför allt, så det är ett viktigt use case  
458 Ah nä men jättebra, och tre till day three då, eller tre kvar, och då har vi cooperative lane change  
Ah egentligen om man börjar med platooning då, för jag tog väl platooning, lane change och merging va  
460 Japp det gjorde du  
Och, alltså dem funkar ju inte utan varandra kan man säga [unclear] platooning i sig det är ju ett jättebra use case  
462 framför allt för lastbilar för att spara bränsle och för att få en effektivare transportkedja då, och tittar man på längre sikt  
så är det ju även för åkarna då att man kan spara ganska mycket personalkostnad, och tid, att dem som sitter i fordonen  
464 längre bak förmodligen inte ens behöver hålla i ratten då utan dem kan använda det som viotid, så att det finns ganska  
mycket pengar och spara på det, både bränsle och personalkostnader, men för att det ska funka, platooning är bra i  
466 sig, men för att det ska funka riktigt bra så behöver man även dem två andra tjänsterna, dvs att det ska funka även när  
man kommer till en korsning eller till en på- och avfart att andra bilar ska kunna komma in på vägen och automatiskt  
468merga in i en sän, antingen i en platoon, eller att man splittrar en platoon och tar in en annan bil emellan då om det är  
nödvändigt för att få bra flöde på trafiken, och likadant lane change är ju också nödvändigt då för att man ska kunna få  
470 nägorlunda naturligt beteende i trafiken, så att  
Justeja så dem här tre use casen, det är, lite, definitionen, alltså use case, vad ska man säga, det är lite definitionen av  
472 automated driving liksom, det är dem här som på något sätt uppnår det syftet då  
Ja alltså du kan använda, alla tre use casen funkar för sig, men det blir riktigt bra först när du har dem tillsammans  
474 Ja nä men snyggt, bra, men då har vi ju täckt dem tre use casen här nu då också skulle jag ju säga  
Gött  
476 Så jag har en sista fråga här bara, men det känns som jag fått väldigt mycket info redan, så det är om du verkligen har  
någonting allra sista här, ska vi se vad det var, do you have any additional thoughts or wonderings that you would like  
478 to share regarding the things covered in this interview, basically use cases and their cybersecurity  
Nä alltså jag tycker att den här, den svåraste delen eller vad ska man säga, den luddigaste delen alltså hur kan man  
480 använda den här attackvektorn på andra sätt än att bara köra DDOS eller skicka, spamma med felaktig information, dvs  
liksom hur man kan uppnå någonting annat än vad liksom detta use case syftar till egentligen  
482 Ja alltså hur, hur försäkrar man sig om att man har en bra implementation och vad finns det för verktyg och metoder,  
hur mäter eller utvärderar man det, det tycker jag är jätteintressant, jag tittar ju ganska mycket på liksom olika fuzzing  
484 approacher och sådär mer eller mindre intelligenta sätt att skicka in skadlig data i systemet, och vad man kan säga där är  
väl att generellt sätt, det är ganska lätt att få ett system och krascha fortfarande, men då har man egentligen inte uppnått  
486 så mycket mer än det man kan uppnå med att bara skicka ut brus eller nått annat DDOS liknande, (dvs) att systemet  
inte gör det det ska längre, men i och med att man kan få det och krascha så misstänker jag att man borde kunna göra  
488 annat med den här attackvektorn också, men där har jag inte jobbat särskilt mycket mest för att jag inte haft tid med det  
helt enkelt så där tycker jag det ska bli jättespännande och se vad du kommer fram till  
490 Ah men kul och höra, jätteroligt, ah det känns ändå som att jag, för i början var det lite svårt med hur jag skulle liksom  
inriktta mig på det här området, men mer om mer nu så börjar det känna som att det kan bli någonting bra det här, så  
492 det är superkul

...

494 ...

## B.5 Interview Candidate 5 (IC5) Interview Transcript

Se så det kommer igång här bara, brukar ta lite, så, då frågar jag igen, är det okej med dig att du är med i den här intervjun och att jag spelar in den

Absolut, helt ok

4 Ja, suveränt

...

6 ...

Då kommer general questions about V2X här nu då, och då utifrån ja helt enkelt ditt perspektiv, så what do you think of the current situation of V2X?

Ja

10 Det är en väldigt generell fråga

Ja den är väldigt generell men ganska bra, såhär då, man kan ta olika perspektiv på det här, man kan ta ett perspektiv i penetration, där vi ser att vi har ganska låg penetration av V2X i nya bilar

Och penetration menar du med implementering då eller

14 Ja att det finns V2X i nya bilar

Ja precis

16 Idag så de bilar som levereras med V2X är ju egentligen bara Volkswagens Golf och ID3 och ID4 som har V2X, och då har dem ju 802.11p, heter ju den standarden, alltså short range, och här finns det ju då ett annat krig på marknaden mellan short range och long range kan man säga, emellan nätverksoperatörerna och nätverkstillverkarna som står på 5g sidan, där Ericsson ju är en drivande kraft såklart, och sen har vi short range läget som är dem här lite mer [unclear] kan 20 man väl säga, alltså det måste funka, vi kan inte vänta, 5g det blir ju så otrolig operation liksom innan vi kan komma igång med en bil som kan köra med V2X så ska det upp med basstationer och det ska liksom, det är infrastruktur som 22 ska rullas ut, det är långt framåt

Ja, men det är ändå fortfarande, alltså den här liksom, vad säger man, debatten är då inom Europa också skulle du säga 24 Absolut, i högsta grad [unclear]

För som jag förstod det enligt min uppfattning så var det mer fokus på short range i europa med liksom ETSI standarden 26 och allt det där och mer long range i usa, men det är fortfarande ändå

Absolut och EU var ju, är ju, hade ju en delegated act som det heter, att tala om att vi ska jobba med short range i EU, 28 men natten innan, [unclear] detta kan säkert någon annan berätta mer om, men natten innan som jag förstått det så föll den, och det tror man beror på då lobbying av dels dem som tillverkar nätverksutrustning [unclear] och operatörerna 30 som ju då, det finns ju ett problem då, på, i marknaden för 5g, och det är ju att dem inte vet vad vi ska ha 5g till, vi har ju investerat sjukt mycket pengar i samhället i 5g, men det finns liksom inget sådär killer use case

32 Nä, alltså då tänker du liksom generellt, inte bara inom fordonsindustrin

Nä men vad ska en mobiltelefon, varför ska den ha 5g, duger utmärkt med 4g, det finns ingen, det som du kan få med 34 5g är ju extremt låg latency till exempel och det har vi ju inte användning av sådär jätteofta, om man ska vara helt ärlig, utan det är ju väldigt specifika applikationer och då måste man ju då, i så fall, hämta hem hela investeringen på 5g 36 utvecklingen på väldigt specifika applikationer, och det vill man undvika för då blir det ju skit dyrt, så man vill hitta liksom generella use case och ett sånt skulle kunna vara V2X då, som skulle kunna ge pengar

38 Och när du pratar om dem här basstationerna det är mycket för att den här alltså, 5g:s räckvidd inte räcker till helt enkelt Det är ju ett helt, ja det finns ytterligare då en teknisk del i att man kan köra 5g peer-to-peer, men låt oss släppa den, men 40 ändå man behöver ju infrastruktur för att jobba med 5g, så är det ju, och sen finns det ju operatörer med i det här då, som vill ha en del av kakan, i ett 802.11p scenario så finns det ju inga operatörer, utan bilarna kommer ju kommunicera 42 autonomt med varandra och med infrastruktur och det finns ingen som tar del av kakan, men i ett 5g scenario så behöver ju varje bil ha ett abonnemang och varje lyktstolpe eller trafikskylt och vad man nu har kopplat upp måste ju ha liksom

- 44 ett abonnemang på nått sätt, så nä men det finns nog både randiga och rutiga skäl till varför vi står där vi står, det som  
45 jag tror är vägen framåt, lösningen framåt, det är ju att glömma tekniken, strunta i det just nu, kör på på nått och då  
46 kanske 802.11p är det man ska köra på kortsiktigt på, och sen jobba med politikerna, med den här säkerhetsaspekten,  
47 hur många liv kan vi egentligen spara, vad kan det här bidra med, då när vi har kommit dit att det här bidrar till att  
48 höja säkerheten då kommer tekniken att lösa sig liksom, då kommer man komma överens, man måste liksom skifta  
49 fokus här tror jag i branschen, vi måste hjälpas åt och skifta fokus och lite grann är det här symptomatiskt för att det är  
50 mest ingenjörer som är intresserade just nu och ingenjörer är rätt intresserade av teknik och att brottas med teknik, men  
51 dem som kanske borde vara intresserade här är ju nationalekonomer, hur mycket kan vi egentligen spara här med hjälp  
52 utav V2X, och jag tror att det är ganska mycket man kan spara, både i termer av minskat lidande, liv och olyckor, men  
53 också i termer av pengar i att vi kan effektivisera våra trafiklösningar, vi kanske inte behöver bygga nya vägar om vi  
54 kan optimera flödena på dem vägarna som vi har [unclear]
- Ah väldigt intressant perspektiv, med just nationalekonomiska och politiska där, och då till nästa fråga, what do you think is the biggest challenge so far for V2X, nu har vi ju varit inne lite på det då, både med liksom infrastruktursdelen och engagemanget då som jag förstår det i sin helhet liksom
- 55 Ja, precis, men jag tror att den största utmaningen just nu det är att få upp penetrationen och uppnå liksom en kritisk massa
- 56 Alltså och där dem kör på liksom, samma teknologier då helt enkelt
- Ja precis, så dem kan kommunicera så att det faktiskt händer någonting i bilen det är liksom första utmaningen, det  
57 finns ju, man kan säga att det är väldigt två parallella spår här, vi är ju, alla som jobbar i automotive är väl ganska  
58 överens om, tror jag, att autonoma fordon kommer inte fungera med line of sight sensorer, över tid, utan man kommer  
59 behöva kommunicera på något sätt mellan fordon och uttrycka intentioner mellan fordon, och vi jobbar jättehårt på  
60 autonoma fordon idag i en silo, och så jobbar vi i en annan silo med V2X kommunikation, och jag tror att man behöver  
61 bygga mognad i kommunikationssiloen innan man är framme på samma ställe i autonomisiloen så att säga, man kan  
62 inte liksom, det är två problem som man inte bör [unclear] samtidigt utan man bör ha en stabil liksom, en stabil  
63 kommunikationsplattform först och sen kan man lägga på autonomi, autonoma fordon på den istället för att parallellt  
64 hålla på och försöka lösa problem i två, på två ställen, det är sällan en bra lösning
- 65 Nä det var det som jag blev så himla förvirrad om i början av, när jag liksom gav mig in på det här ämnet, för jag tänkte  
66 att, när jag liksom läste om V2X så var det så ganska mycket, ja men, att det här, man måste uppnå som du säger en  
67 bra kommunikationsform för och kunna implementera vissa automation, men jag tänkte liksom att, det var, för det var  
68 det jag pratade lite med en annan kandidat också, och då var det såhär, eller jag var lite såhär vad är skillnaden mellan  
69 autonom teknologi och V2X då, liksom det ena behöver ju verkligen det andra, men då var han ändå såhär att jo men  
70 med V2X kan man uppnå det här och det här, det man liksom på ett sätt bygger på först då för och sen kunna ta nytta  
71 av det i den autonoma tekniken och då liksom hajjade jag till
- Och det finns ju ganska tydligt i om man tittar på use casen, day one use casen är ju helt informativa use case för föraren  
72 i en normal bil liksom, och sen så när man kommer
- Liksom notifikationsmeddelandena osv.
- 73 Ja, och det funkar ju idag, det skulle man ju idag kunna rulla ut på bred front och det skulle lira liksom, det har man ju  
74 gjort, tycker jag, tillräckligt många storskaliga försök för att, jo det kommer fungera, vi var med och gjorde ett försök,  
75 där man har byggt ITS korridorer igenom ett visst område och det hade funkat, man kan få en varning om att det är  
76 någon som bromsar framför en och man kan få en varning om någon har stannat på motorvägen, man ska stanna på  
77 motorvägen, knäppa upp säkerhetsbältet och öppna dörren, då triggars varningen för att det är någon på vägen
- Jaha, men inte, men det är också när liksom någon gör en hastig inbromsning också eller
- 78 Men det är ju lite olika informationsnivåer liksom, man pratar ju om två informationsbärare, en som heter CAM och en  
79 som heter DENM, där CAM är liksom ett rått, man säger, en rå data som bumpas ut, medan en DENM är en tolkad  
80 informationspusselbit liksom att, nu kan vi tala om att det här har hänt
- ...
- 81 ...

Men största utmaningen skulle jag väl säga det är nog att få upp penetrationen och att släppa teknikfokuset, att liksom  
92 blunda för det, hur jobbigt det än känns som ingenjör eller som tekniskt intresserad, bara skita i det för nu, och fokusera  
på vilka vinster kan vi uppnå i samhället

94 Mh, jättebra svar, verkligen, och sen till sista frågan här, som du får köra på typ 3 minuter så det är nästan så att du bara  
får rabbla upp företag i så fall

96 Ah alltså nästan pass får jag väl säga, jag är inte jätteinblandad i liksom chipset utveckling, men jag har ju förstått  
Autotalks är långt framme, till exempel, jag skulle ju vilja lägga till där att, biggest influence ja men alltså Ericsson  
98 har ju jättestor influence på den tekniska utvecklingen, om det är positivt eller negativt det kan jag inte riktigt uttala  
mig om, men det är ju definitivt så att Ericsson är med och spelar här, kanske den största spelaren just nu som trycker  
100 branschen framför sig det är ju Volkswagen, som är dem enda som liksom har vågat satsa på riktigt, som har tryckt ut  
det här i riktiga bilar

102 ...  
...  
104 Så jag vill att du ska välja fyra day one use cases, fyra day two use cases, och fyra day three use cases, that you consider  
will have or already has a significant role for traffic situations, och till det då så har jag den här Google sheetet som jag  
106 ger dig 15 minuter till att fylla i  
Då kanske jag ska mutera mig och sätta mig och se om jag kan titta på det helt enkelt  
108 Japp, men du kommer få tid för dig själv ja precis, du får 15 minuter och så mutear vi varann, men först bara så här då,  
by significant role I mean use cases that you consider are the most relevant or predominantly crucial thinking from the  
110 core of V2X technology, och då liksom traffic efficiency och safety då, som jag tänkte där utefter, sen får du tolka det  
såsom som du vill det är lite tanken med uppgiften också  
112 Det här blir nog svårt för mig eftersom jag inte har jobbat så mycket med use cases, men jag ska göra en ansats  
Ja, jo men precis, nä men gör det absolut, det behöver inte, du gör så gott du kan helt enkelt, men om vi går in i  
114 dokumentet båda två så ska jag visa hur du ska göra bara när du väljer use cases, har du  
Den låg i inbjudan  
116 Ah jag kan skicka det i Teams med här, ska vi se  
Juste, där kom den, tack, då ska vi se, oj, ja du, det här blir inte lätt, det här har jag ju knappt jobbat med  
118 Ah ok, nä då kan det bli lite svårt ja, men tänk lite mer då på liksom vad som låter bekant kanske, alltså det som du har  
hört talats om tidigare också, liksom köra på det, eller köra utifrån det, och ja, alltså helst vill jag att du verkligen utför  
120 uppgiften så gott du kan där då, så om du känner att 15 minuter inte blir tillräckligt så kör en extra 5 minuter där då så  
du hinner välja fyra från day one fyra från day two, och fyra från day three  
122 ...  
...  
124 Nu tror jag är i princip klar  
Nice, suveränt  
126 Även om jag gissade lite, men ja  
Nä men det gick ju snabbt det  
128 Japp, kanske lite väl fort  
Ah men suveränt, bra, och då kommer vi till nästa fråga då helt enkelt, helt enkelt, fasen vad jag säger det nu hela tiden,  
130 varför gör jag det, och då är det dem här tre frågorna jag kommer ställa för varje use case kategori, så först då vill jag  
veta varför du har valt dem just day one use casen du valt och sen ifall du ser några potentiell cyberhot och då är det bara  
132 generella exempel i så fall och vilka säkerhetsåtgärder dem skulle kunna ha mot sig i så fall, men det mest intressanta  
är varför du har valt just dem här day one use casen därå, bara höra någon liten tanke bakom det  
134 Ja, jomen jag har ju utgått ifrån, alltså, för mig så är den kollektiva säkerheten det är det som får vara prioritet, och  
dem, personlig bekvämlighet får komma i andra hand, så en del av dem use casen är kanske lite tråkiga men jag tror  
136 att de bidrar positivt till trafikmiljön eller till säkerheten på väg, och EEBL är väl en typiskt sådan, där vi vill generera  
en varning när man visar upp, man bromsar hårt helt enkelt, den andra där är ju, farliga platser, och emergency vehicle  
138 approaching och det är ju också något sånt som jag tror kommer bidra positivt till trafikmiljön, att få information om  
det tidigt gör att du kan planera, i day one så är det ju fortfarande att man själv planerar sin körning, och att du då kan

140 planera att ställa dig på en shoulder och släppa förbi helt enkelt, stationary vehicle är ju också en sån sak, det är farligt  
och ha en bil som står på vägrenen, och kan jag få reda på det i god tid så har jag en möjlighet att glida ut i vänsterfilen  
142 och se till att inte smasha in i den  
Och det var detta use case du var lite inne på innan fast inte då liksom notifikationsdelen för nu är det ju då bara  
144 notification på det, men för det var den du prata om innan, där med stationary vehicle, att den, men då att den också  
reagerar självt fordonet  
146 Precis, så för att helt tekniskt för att fordonet ska skicka den där DENMen så måste ett antal scenarion vara uppfyllda i  
själva fordonet, så det är inte bara att ha stannat  
148 Nä justeja  
Cybersäkerhetsmässigt här då, jag är ju för dåligt påläst, det jag kan se här är ju att, att injicera felaktiga varningar  
150 skulle ju få allvarliga konsekvenser på systemet, både i form av att man inte litar på systemet längre, och att systemet  
kan triggas att göra dumma grejer  
152 Det var samma svar jag fick av förra kandidaten också  
Men hur ett angrepp skulle kunna gå till ja det är ju lite teoretiskt idag då  
154 Ja det blir ju det eftersom, alltså det blir ju future studies mer eller mindre  
Jaa  
156 Eftersom det inte finns riktigt den utsträckningen  
Nä det man kan säga är väl att tittar man, svensken är ju dålig eftersom vi har samma ord för safety och security  
158 Ja de är  
Vi kallar ju allt för säkerhet, men om man tittar, tittar man safetymässigt så är ju konsekvensen av ett cyberangrepp  
160 mindre i day one och till viss del i day two än i day three, det är ju först i day three som konsekvenserna drar iväg  
Ja, för det är då den liksom autonoma tekniken mer implementeras i samband med dem här day three use casen då  
162 Precis då kommer ju fordonet själv ta action, eller trafiksystemet ta action på den data som kommer in, och man då  
manipulerat den data ja då, eller saknar data för det är ju också alltså, man kan ju tänka sig ett DDOS scenario är ju  
164 inte alls orimligt här att spamma sönder nätverket med meddelanden eller med vitt brus, det är ju inte svårare än så och  
störa ut, man kan ju fundera mycket på hur man ska injicera meddelanden och göra det väldigt elegant, men den, de  
166 råaste och fulaste här är ju bara vitt brus liksom, hela spektret, förstöra hela spektret  
Och då mera att den går miste om då, helt enkelt, alltså herregud, nu får jag sluta säga det  
168 Ja då blir det ju ingenting  
Nä, då blir det ju ingenting, att den kan basera liksom sina beslut på snarare än om det då det blir en DDOS attack slår  
170 ju ut systemet då också givetvis på det sättet  
Men problemet med en DDoS attack är ju i dem här fallen att själva meddelandena kommer ju vara ganska säkrare, det  
172 kommer nog inte vara så lätt att DDOSa grejer här för att det kommer finnas krypton och nycklar och det kommer vara  
knepigt, det är jag rätt säker på, däremot så är jag ganska säker på att det kommer gå liksom, ja blåsa på med vitt brus  
174 på radion och så  
Jag förstår, störningar då  
176 Ja precis, och i och med att det är short range, så är det ju, du utsätter dig för en ganska liten risk genom att störa liksom  
Juste, ja nä men jättebra, och sen, då var du ju också inne lite på securityn här med både day two och day three, speciellt  
178 att konsekvensen då såklart ökar, men om vi tittar, ja bara generellt här nu då varför du valt dem här fyra day two use  
casen, det jag också ser här från safety då främst liksom  
180 Ja det blir ju mycket safety och, ja men här, dem är ju lite mer avancerade men det är fortfarande säkerhetsrelaterade  
event som vi idag vet är problematiska, vi vet om att blind spot är en stor anledning till olyckor till exempel  
182 Och här har du ju den då, som du, det här är väl exakt det du nämnde innan  
Ja precis exakt ja  
184 För då är den semi assistant här då, eller vart läste, nej semi automation där då ju, så semi automation reaction, ja  
justeja, nä men bra  
186 Functional safety problemet också ja  
Och så tar vi dem här day three use casen också, för dem vill jag gärna prata lite om

- 188 Den första där är ju, bryter jag ju helt mot min egen teori där, men, jag tror att ur ett samhällsperspektiv så, alltså  
189 parkeringsskador kostar väldigt mycket pengar, det är dyrt med parkeringsskador, så att ska man börja spara pengar  
190 också och få med liksom den delen då är det nog inte så dumt och ha det där för att på en parkering så skulle man nog  
191 kunna automatisera själva parkeringsförfarandet om det inte får köra några andra bilar där, utan det är bara automatisk  
192 parkering, så hade det nog funkat ganska bra och du hade kunnat optimera parkeringen på ett ganska schysst sätt, så att  
193 där, spara lite plåtskador, jag tror att man kan spara mycket pengar där
- 194 Ja nä det var ju ett smart val utifrån det, nu vet jag ju inte vilka det stod emellan den här och vilka andra det potentiellt  
195 kan ha varit, nä men intressant val hur som helst, och sen tar vi, vi kan ju ta den klassiska då platooning, varför du valt  
196 den
- 197 Där är ju också jättestora pengar som finns att spara, och miljövinster såklart, det är ju också en del, vi lever ju i ett  
198 mer sustainability-medvetet samhälle och möjligheten att platoona fordon tror jag, det är en viktig del, det är också,  
199 man kan tänka sig, alltså platooning historiskt har ju oftast rört sig om liksom Volvo som ska flytta motorer mellan två  
200 fabriker liksom, och så platoonar man ihop fordon, jag tror att platooning kommer att ha användningsområden även  
201 om man tänker, idag, den semi-nära logistiken i ett samhälle att du köper hemkörsning, mat på hemkörsning från ICA,  
202 så idag så packas den ju oftast i din lokala butik liksom, och körs hem, det är ganska ineffektivt, så kommer vi inte  
203 kunna ha det framåt när vi ska optimera våra system utan då kommer ju, man kommer ha speciella enheter där man  
204 packar dem här ordrarna, och då kanske man har en sån i, säg att man har den i Jönköping då får ju den serva då bort till  
205 Halmstad kanske, och då, i Jönköping ligger ju centralt liksom så det är ett smidigt ställe att köra och då kanske man  
206 platoonar ihop alla dem transportbilarna som ska till Halmstad och Varberg och Falkenberg och liksom, i ett fordonståg,  
207 du kanske inte har en förare i varje bil, utan föraren hoppar på där nånstans i Nissastigen när det är dags och liksom  
208 distribuera ut, och sen när man ska åka hem igen, med alla dem här distributionsbilarna så platoonar man ihop igen och  
209 kör tillbaks fordonståget, så att, det tror jag definitivt är ett framtidsscenario, även om det är ett svårt scenario
- 210 Om vi pratar nu framtidsscenario, när tror du liksom en sån här, alltså när tror du en sån här vad säger man, teknik, när  
211 tror du den kommer finnas på ett ungefär, hur långt fram är det liksom
- 212 Jag tror det är ganska långt fram tyvärr, Elon Musk har ju varje år de sista 10 åren sagt att det är ett år kvar till  
213 självkörande bilar, och det finns lite information i det, att det är mycket svårare än vad vi trodde, nu tror jag, hade du  
214 frågat mig för 2 år sedan så hade jag sagt att nä men det svåraste kommer att vara juridiken, vem ska ta ansvar här, det  
215 ser jag att det viker, det är lättare och lättare, utan nu börjar man nog komma till liksom läget att, ah men det här är ju  
216 tekniskt svårt, det här ju ganska lätt på en provbana, eller i småskaligt, och i fint väglag och ljust och fint och i ökenen i  
217 USA liksom, ah det är inget svårt och ha självkörande bilar
- 218 Ja, det är väldigt intressant för också som jag har förstått det med dem här day one use casen att dem ansågs också från  
219 början var liksom no big deal så att säga, men nu i efterhand liksom att dem fortfarande inte är implementerade i full  
220 skala och att det fortfarande är otroligt svårt ur den synpunkten
- 221 Och rent tekniskt är de ju ingen big deal, rent tekniskt så, så
- 222 Ah ok, så dem är mer, ja justeja, ah precis, det är ju mer att OEMsen ska, och standardiseringorganisationer, alla ska  
223 samarbeta mer
- 224 Och där är det ju, alltså jag tror att standarden är framme, det är inget problem, och kan man bara komma överens om  
225 att man ska använda [unclear] radiostandard så kommer man kunna implementera det där, men frågan är ju är värdet av  
226 dem där use casen tillräckligt högt för att man ska vilja ha in det i sin fordonsplattform
- 227 Där wrappa du ihop det bra ja
- 228 Så tror jag, sen kan man ju spekulera då, man kan ju vara lite såhär konspirationsteoretisk och tänka ja men Volkswagen  
229 har ju gjort det här dem har ju liksom tagit första steget, har dem nått sånt här killer use case, som bara sitter och väntar  
230 på att penetrationen ska vara tillräckligt hög då kommer man kunna låsa upp det här skit fiffiga use caset, som är liksom  
231 nån kanske någon kombo av day one use case som gör att man kan göra nått, troligtvis inte, det känns orimligt, men  
232 man börjar ju fundera, vad var det som gjorde att dem tog det här steget liksom, det är ju väldigt framsynt
- 233 ...
- 234 ...
- 235 Vi går vidare till den allra sista frågan här och den är bara en sammanfattande fråga om ifall du har några additional  
236 thought or wonderings that you would like to share regarding the things covered in this interview, basically use cases

and their cybersecurity, nu har vi ju varit inne på cybersäkerhet på ett väldigt högt plan så, men det var också lite, för  
238 det blir svårt också lite djupdyka kring den här tekniken och cybersäkerhet utifrån min kunskapsnivå också, så det är  
typ här jag håller mig lite

240 ...

...

242 Det viktiga, man kan dela in liksom, man säger, själva connectivityutvecklingen i fyra faser, grovt, som jag har gjort  
här då, och säga att vi har en första generation som egentligen är legacy bilar där dem, bilar är uppkopplade via  
244 bluetooth eller fysisk kabel, och det är ju gammalt, generation två så kopplade man upp med ett backend och man har  
ett infotainment och man har en OBD2 port, och det är ju ungefär nu, det är lite gammalt men idag har ju alla bilar är  
246 ju uppkopplade idag, dem har ju ett eget modem, så att nu börjar ju riskvikten gå upp liksom, cybersäkerhetsriskvikten  
gå upp, där man i generation tre så kommer ju ditt V2X in, och man börjar koppla upp sig mot andra system inte bara  
248 mot exempelvis Volvos egna back end, utan man kanske också kopplar upp sig mot, man har konstant uppkoppling mot  
Spotify, och man har konstant uppkoppling mot smart infrastruktur, så vägsystem och så där, utanför V2X eller inom  
250 V2X, och sen i nästa nivå då så har man ju autonoma fordon, här kan man ju se liksom när det börjar, tittar du på den  
kurvan jag ritat här så kan man ju se att det tar fart här, och mixen här där man både har connectivity från flera håll i  
252 bilen, du har ju inte bara den lokala connectiviteten i form utav Bluetooth, det är ändå en hanterbar risk, och så lägger  
du på ODB2 porten som är direkt interface till CAN nätverket i bilen, det är ju fullkomligt livsfarligt och värdelöst, och  
254 på det så lägger man alla dem här nya trådlösa teknikerna, och så kommer det, gör man det med autonoma fordon  
Ja det låter ju helt galet

256 Precis, det blir liksom riskvikterna tar iväg, drar iväg i en sån riktning som gör att det blir väldigt svårt att hantera, vi  
kommer ha det svårt att hantera det i framtiden, därför kommer du och dina kollegor som jobbar med cybersäkerhet ni  
258 kommer ha en jättestor roll här i automotive, för automotive ligger idag kanske 15 20 år efter liksom desktop världen,  
vi kan inte patcha våra bilar till exempel, det finns ingen strategi för det utan bilar patchas lite när man vill, och berättar  
260 man det för någon som jobbar med drift så bara skrattar dem ju åt en liksom, så att, och vi har ingen säkerhetstänk när  
det gäller att välja ut leverantörer, det är jättemånga idag då som sitter och funderar på är det så att det finns hotaktörer  
262 som har lagt in bakdörrar i våra bilar, idag då när bilarna inte är autonoma så, förmögligen kan man ju inte orsaka så  
mycket olyckor så, men du skulle ju mycket väl kunna ställa till det

264 Ja definitivt

Du skulle kunna bara liksom, du skulle kunna ställa till det så att bilen inte går att öppna, det vore ju trist, du skulle  
266 kunna ha en ransomware attack där man säger att ja men du ska betala ett antal pengar kryptovaluta för att få tillgång  
till din headunit igen

268 Eller bara liksom tänk på personlig data när man kopplar upp sin mobil till bilen, det är inte så mycket  
You name it

270 Ja vissa OEMs använder kryptering för den data som liksom, storas då på, inom bilen, men jag läste ett annat kandi-  
datarbete från jag tror det var två år sedan där dem åkte till en bilskrot och så hämtade ut infotainmentsystemet från  
272 vissa bilmärken då, vissa hade krypterat sin data, vissa hade helt öppet bara klartext, och där information med folk som  
hade kopplat upp sig med sin mobil då, så det är ju också helt sjukt kan man tycka

274 Man kan tycka det är helt sjukt men samtidigt så kommer man från en embedded miljö som dem flesta som utvecklar  
infotainmentsystem i bilar gör så är det så man jobbar, det finns ju ingen som har, historiskt har krypterat databaser i  
276 embedded system utan man har ju bara räknat med att det här är security [unclear], det finns ingen som kan ta sig in i  
vårt system, så att det, nä det är en ny värld nu helt enkelt

278 ...

...