Is a V2X-enable Critical Mobility Infrastructure a Critical Information Infrastructure? A Literature Review

Bachelor Thesis

by

Jan Kiefer

Degree Course: Informationswirtschaft

Matriculation Number: 2057390

Institute for Applied Informatics and Formal Description Methods (AIFB)

KIT Department of Economics and Management

Advisor:	Prof. Dr. Ali Sunyaev
Second Advisor:	Prof. Dr. Andreas Oberweis
Supervisor:	M. sc. Maximilian Renner
Submitted:	14. April 2021

Abstract

The mobility infrastructure is very important for our every day's life. This infrastructure influences not only human mobility, but also human prosperity and almost any part of our life. As the digitalization and networking do not stop ahead of this infrastructure, new technologies emerge in this sector. One of them being vehicle to everything (V2X) communication, which enables communication among different entities of the traffic (e.g., vehicles, pedestrians, infrastructure) (Zhou et al., 2020, p. 309). By means of this communication, for example, road accidents can be reduced by about 80% (Ghosal & Conti, 2020, pp. 1–2) and cooperative driving can be enabled (MacHardy et al., 2018, p. 1863).

However, to enable V2X communication, the existing mobility infrastructure must be expanded with the ability of communication. A mobility infrastructure with this ability is called V2X-enable CMI. Like any new technology, also V2X communication entails new challenges (Lu et al., 2014, p. 292). In order to better understand and detect the new challenges and especially to better understand V2X-enable CMIs, a categorization of the challenges and characteristics according to the characteristics of critical information infrastructures (CII) may help.

In this work, the most crucial challenges of V2X communication are presented and finally V2X-enable CMIs are categorized into CIIs or not, based on the key characteristics of CIIs.

Table of Contents

List of Abbreviations

CI	Critical infrastructure
CII	Critical information infrastructure
CMI	Critical mobility infrastructure
C-V2X	Cellular V2X
D2D	Device to device
DSRC	Dedicated short range communication
eNB	eNodeB
OBU	On-board unit
PPT	Microsoft Power Point Presentation
RSU	Roadside unit
V2B	Vehicle to broadband
V2G	Vehicle to grid
V2I	Vehicle to infrastructure
V2P	Vehicle to pedestrian
V2S	Vehicle to sensors
V2V	Vehicle to vehicle
V2X	Vehicle to everything

List of Figures

List of Tables

1. Introduction

1.1. Motivation

The mobility infrastructure is very important for our every day´s life. Parts of the mobility infrastructure are, for example, the road and the rail infrastructure (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2020). Besides human mobility, this infrastructure also influences human prosperity and almost any part of human's life. An example to show the importance of the mobility infrastructure is grocery shopping, which is an essential activity for human health. Because nowadays nearly nobody plants all of their groceries at home. In 2011, 70% of the people in Germany mostly used the car for grocery shopping (Statista, 2011). Without an intact road infrastructure, driving to the grocery store would not be possible. In addition, the grocery stores also need the road infrastructure to get supplied. This example shows our dependency on the mobility infrastructure.

Nowadays the digitalization and networking progressively effect the mobility infrastructure. An emerging technology in this sector is vehicle to everything (V2X) communication (Zhou et al., 2020, p. 309). Vehicles not only have access to the internet and communicate with each other, but also communicate with the infrastructure and pedestrians, for example. This kind of communication might reduce the number of road accidents by 80% (Ghosal & Conti, 2020, p. 2) and can reduce the amount auf energy needed to drive due to platooning (Boban et al., 2018, p. 113). Like any new technology, V2X communication also entails new challenges and weak points like security issues (e.g. attack prevention, trust and privacy, etc. (Ghosal & Conti, 2020, pp. 10–11)), that are typical for wireless technology, ensue (Ghosal & Conti, 2020, p. 1).

To enable this kind of communication, the mobility infrastructure has to be expanded with the ability of V2X communication. Out of that arises a mobility infrastructure that enables V2X communication (V2X-enable CMI), which needs to be understood to face these new challenges. In research, V2X technologies receive more and more attention. There is, for example, a massive increase of 5G patents for car applications (Statista, 2019), which can be helpful for cellular V2X communication (MacHardy et al., 2018, p. 1859). However, to better understand V2X-enable CMI and detect the most crucial challenges, a categorization of the challenges and characteristics of the V2X-enable CMI according to the characteristics of critical information infrastructures (CII) may help. CIIs require a higher level of security to be usable also in case of critical incident i.e., blackouts or hacker attacks. Currently there is no categorization, whether a V2X-enable CMI is a CII or not, which leads me to the research Question: Why is a V2X-enable CMI a CII or not?

Today, the mobility infrastructure is categorized as a critical infrastructure (CI) (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2020). However, a V2X-enable CMI expands a classic mobility infrastructure in many ways through the communication of vehicles, pedestrians and the infrastructure.

Hence, I am going to classify V2X-enable CMI into CII or non-CII. Therefore, characteristics and challenges of V2X-enable CMI need to be examined. As no consistent definition of CII exists (CIPedia, 2020), I will focus on key characteristics of CIIs mentioned in previous research to classify V2X-enable CMI (Dehling et al., 2019, pp. 325–327).

1.2. Objectives

To achieve the main objective: Why is a V2X-enable CMI a CII or not? I set two subobjectives.
First, I will show the most crucial challenges of V2X communication to get an impression of actual problems that have to be solved before the V2X-enable CMI can be successfully implemented nationwide. Second, I will compare typical characteristics of V2X-enable CMIs with the key characteristics of CIIs. After this comparison I will be able to infer an answer to the main objective.

1.3. Structure

The work is built up as follows. In the next chapter "Theoretical Foundation" I will give a brief introduction in V2X communication. I will not only present how it works, and which technologies are appropriated, but I will also introduce benefits of V2X communication. To limit this section, I do not explain every part of V2X communication, rather the two most crucial ones Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. In this chapter, I will also explain some fundamentals of CIIs. Therefore, I will put them in relation to critical infrastructures.
In the next section I will introduce the methods I used, and I will show the search strings as well as the way I worked with them to collect the state-of-the-art knowledge. The most crucial challenges of V2X communication are explained in chapter 4.1., followed by the main part of this work, the classification of the characteristics of V2X-enable CMI regarding to the key characteristics of CIIs. Especially there I will decide whether a V2X-anable CMI may be CII or not. Finally, I will discuss my results and draw a conclusion of my work.

2. Theoretical Foundation

2.1. A brief Summary of V2X Communication

2.1.1. Reasons for using V2X Communication

In 2016, 1.35 million people died in road traffic accidents worldwide (World Health Organization, 2018, p. 3). This makes road traffic accidents the 8th leading cause of death. For children and young adults (5-29 years) it ranks even higher (leading cause of death) (World Health Organization, 2018, p. 3). Besides the high number of deaths in traffic, also the amount of traffic congestions in urban roads and highways is increasing, which causes major socioeconomic issues (Ghosal & Conti, 2020, pp. 1–2). To improve the traffic flow and decrease the amount of people dying in road accidents, until one day the ultimate goal of zero accidents is reached (Faezipour et al., 2012, p. 91), a new technology is needed that improves the ability of communication among all the traffic participants and the infrastructure (Ghosal & Conti, 2020, p. 2). Therefore, V2X communication seems to be a crucial technology. V2X communication creates a cooperative environment that improves the communication and collaboration between vehicles, pedestrians and the road infrastructure (Ghosal & Conti, 2020, p. 2). To enable this kind of communication, vehicles need to be equipped with wireless communication capabilities, which is also seen as the frontier for the next automotive revolution (Lu et al., 2014, p. 289).

The benefits of V2X are varying and results of many different intelligent applications (Ghosal & Conti, 2020, p. 9). Overall, the applications can be divided into three categories: safety-related, traffic-related, and infotainment-related.

Safety-related applications aim to reduce the probability of accidents and protect the vehicle from danger (Alnasser et al., 2019, p. 7). Thereby, property damage and human deaths and injuries can be reduced (MacHardy et al., 2018, p. 1863). Either the driver is getting informed about dangerous situations (e.g. slippery sections) or safety systems are triggered (Chiara et al., 2009, p. 226). The required information is received by sharing information periodically between vehicles and road units (Alnasser et al., 2019, p. 7; Karagiannis et al., 2011, p. 585).

Some examples of safety applications are cooperative forward collision warnings and traffic violation warnings (Zaidi & Rajarajan, 2015, p. 260). In particular accidents through lane changing and inattention of the driver (Bulumulle & Bölöni, 2016, pp. 13–14) as well as secondary accidents can be reduced by V2X-based safety applications as resent research shows (Chiara et al., 2009, p. 230). It is estimated that about 80% of road accidents could be avoided by V2X communication (Ghosal & Conti, 2020, p. 2).

Traffic-related applications aim to improve the traffic flow and reduce congestions on the roads by traffic management (Shrestha et al., 2018, p. 1). These kind of applications send collected traffic information to remote servers wirelessly (Alnasser et al., 2019, p. 7). The server then analyzes the information and send the results, for future usage, back to the vehicle. Furthermore, there are many other applications like system-level coordination of intersection timing or route planning in order to achieve environment-friendly use of the vehicle's engine (MacHardy et al., 2018, p. 1863). Generally traffic-related applications can be separated into two subcategories: speed management applications and cooperative navigation applications (Karagiannis et al., 2011, p. 586). Speed management applications help the driver to adjust the speed of the vehicle to prevent avoidable stops (Karagiannis et al., 2011, p. 586). For example, advising the optimal speed to arrive at intersections within green light intervals. Cooperative navigation applications can manage the navigation of vehicles. Platooning is just one example of many, which not only improves the traffic efficiency, but also reduce the energy consumptions of the vehicles within the platoon (despite the first vehicle) (R. Q. Malik et al., 2019, p. 126762; Zaidi & Rajarajan, 2015, p. 262).

Infotainment related applications aim to improve the driving experience that are typically not driving related, rather enhance entertaining or informative services for the passengers (MacHardy et al., 2018,

p. 1862). This type of applications is often coupled with internet access and used for video streaming, weather information (Alnasser et al., 2019, p. 8) or location based advertisements like information about the nearest restaurants or the nearest gas stations (Ghosal & Conti, 2020, p. 10).
Consequently, V2X communication offers various benefits in different areas.

2.1.2. How V2X Communication works

V2X communication comprises various kinds of communication, which are sometimes named differently in papers. Overall, there are the following communication pairs: Communication among vehicles (V2V), between vehicles and the infrastructure (e.g., traffic lights, sights) which is called V2I, between vehicles and pedestrians (V2P) and between vehicles and in-vehicle sensors (V2S), as well as communication between vehicle and the grid (V2G) in case of electric charge vehicles (Alnasser et al., 2019, p. 6) and vehicle to broadband communication (V2B) (Faezipour et al., 2012, p. 91). All of the road entities (e.g., vehicles, pedestrians, infrastructure units (Alnasser et al., 2019, p. 4)) are generating data that is exchanged via messages and are used to support the intelligent applications (Alnasser et al., 2019, p. 6).

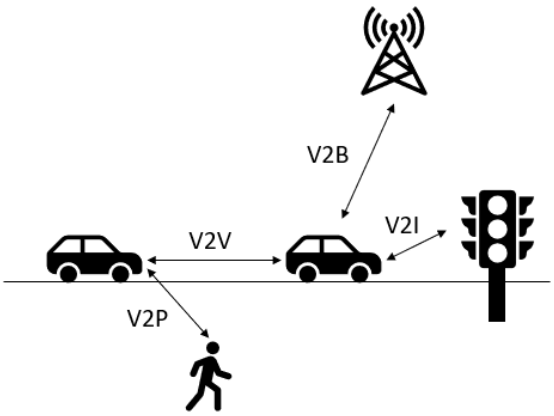

Figure 1: Simplified illustration of V2X communication

Generally, the vehicles send different types of messages. Periodically (in intervals of 100ms to 1s) status messages that contain information about the speed, position and direction (Alnasser et al., 2019, pp. 6–7). This kind of message is called a periodic message or beacon and is sent as broadcast to all vehicles in the neighborhood, for example, to anticipated dangerous situations (Alnasser et al., 2019, p. 7). In case of local events like critical warnings or intersections, local event-triggered messages are sent. Due to the critical warnings, it is necessary that these messages can be transmitted with low latency (100ms). In contrast to local event-triggered messages, global event-triggered messages are distributed over a wide area to inform other vehicles, for example, about congestions. To decrease the critical time needed by emergency vehicles to arrive at the destination, emergency vehicles send emergency vehicle messages. Emergency vehicle messages improve the traffic flow on the road ahead to smooth the vehicle's movement and are sent only by emergency vehicles.

To transmit the messages, there are currently two different technology available. A Wi-Fi solution, which is based on the "IEEE Standard for Wireless Access in Vehicular Environments (WAVE), including the IEEE 802.11p for PHY and MAC layers and the IEEE 1609 family for upper layers" (Lu et al., 2014, p. 293), also called dedicated short-range communication (DSRC). The other solution is based on cellular communication through LTE, also called C-V2X (Bazzi et al., 2019, p. 2). Other technologies (e.g., Bluetooth) do have inevitable limitations (MacHardy et al., 2018, p. 1859).

DSRC enables ad-hoc communication between vehicles, low communication latency, rapid connectivity, and fast communication especially for safety applications (Ghosal & Conti, 2020, pp. 3–4). Roadside components/units (RSU) have to be installed at important points like intersections (Ghosal & Conti, 2020, p. 3). The RSUs communicate with the on-board unit (OBU) of vehicles for information exchange and internet access (Ghosal & Conti, 2020, p. 4). However, communication is only feasible when the vehicles (or RSUs) are in neighborhood of about 300m to 1000m due to the coverage limit of DSRC (Ghosal & Conti, 2020, p. 3; Zaidi & Rajarajan, 2015, p. 258). Other disadvantages like performance limitations in scenarios with a high density of vehicles, problems for maintaining connections in highly dynamic scenarios, and limited bandwidth hinder the implementation (Ghosal & Conti, 2020, p. 6).

Since the successor of 3G cellular, which was not able to satisfy the requirements of V2X communication (Shrestha et al., 2020, p. 2), was launched, cellular V2X raises the focus of research (Huang et al., 2020, p. 258). Primarily because of the higher transmission data rate and the more extensive coverage area that comes with LTE.

Moreover, the next generation of cellular communication (5G) is very promising for the future usage in C-V2X as tests showed that 5G-V2X enables "uninterrupted connections with consistent data transmission rate at Gb/s level […] the transmission latency is controlled in a few milliseconds" (Huang et al., 2020, p. 259). In contrast to DSRC, C-V2X also provides direct access to the cloud and the internet enabling more features for commercial applications like voice and data access based on existing cellular networks (Shrestha et al., 2020, p. 6).

C-V2X has two different communication methods, cellular-based communication and direct Device-to-Device communication (D2D) also called side-link (Alnasser et al., 2019, pp. 10–11). Cellular-based communication via LTE is used for two-way communication between road entities (Alnasser et al., 2019, p. 10). In this mode, the vehicles have to be inside the network coverage and communicate over an eNodeB (eNB) (Zhou et al., 2020, p. 313). D2D communication in C-V2X allows direct communication among neighboring road entities without an eNB (Shrestha et al., 2020, p. 7). It has a better network throughput, lower energy consumption, lower delay performance and a better spectrum utilization (Zhou et al., 2020, p. 313) . However, an additional interface is required for D2D communication that implements Wi-Fi Direct or Bluetooth (Alnasser et al., 2019, p. 11).

The different stages of envisioned applications for C-V2X, is shown in figure 2. This figure underlines also the process of vehicles becoming cooperative autonomous, and the supposed evolution of the capabilities provided by V2X communication in future.

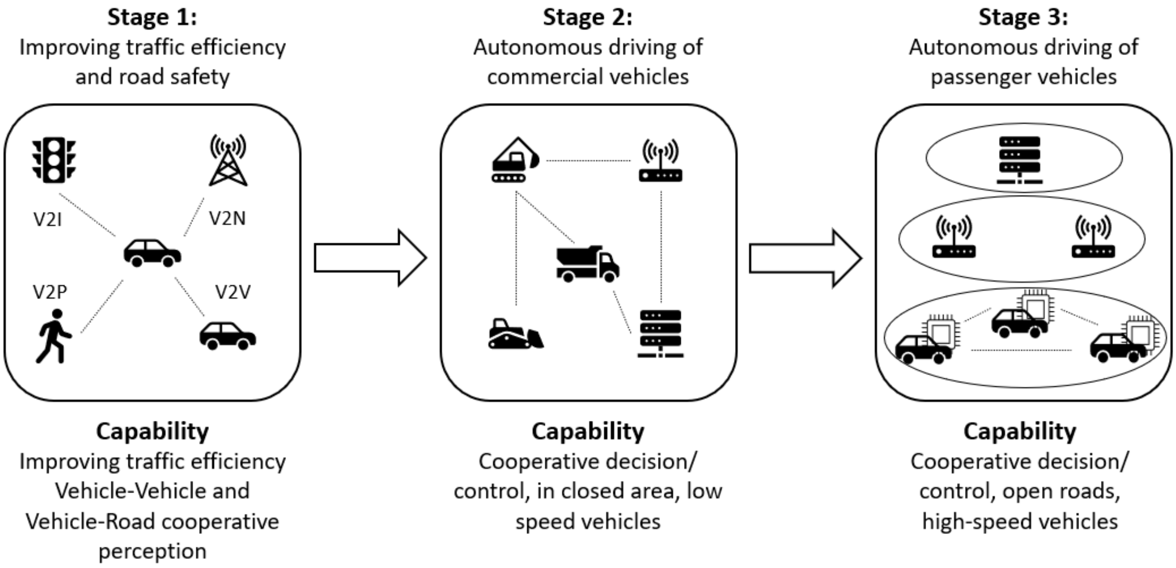

Figure 2: Envisioned application phases of C-V2X (see Chen et al., 2020, p. 3879)

2.2. CI in Relation to CII

The functionality of critical infrastructures (CI) is vital for human's well-being because malfunction or failure of these infrastructures have huge impact (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2020) on quite any part of human life. CIs are categorized into eight sectors: Energy, transport and traffic, information technology and telecommunications, finance and insurance industry, health, government and public administration, water, media and culture, and food. Any infrastructure, which is described in the definition can be classified into one of these categories.

In Germany CIs are defined as "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences" (Federal Office for Information Security, 2021). This definition mainly focuses on physical infrastructures and less on virtual information systems which are not tangible on the first view. For sure that is not unexpected because CIs got defined in 2003 (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2020). Back then, internet did not play such a big role, as it does today, as the development of internet users worldwide shows. Correspondingly the number of internet users did more than triple in the period from 2005 to 2019 (Statista, 2020). Since then, the digitalization has increasingly influenced human life and has created new virtual infrastructures human depend on (Dehling et al., 2019, p. 321). Nevertheless, the new infrastructures cannot be clearly classified as a CI like, for instance, the business management solutions SAP Hana. For further classification of these kind of information infrastructures a new term is needed. Here, the term critical information infrastructure (CII) gains importance. In contrast to the focus of the infrastructure layer in CI, CII focus on the application layer (Dehling et al., 2019, p. 320). Though, it does not mean that CIs and CIIs are complementary, CIIs are rather a subset of CIs. Furthermore, CIs create the required environment so that CIIs are able to work.

CIIs have four main functions (Dehling et al., 2019, pp. 320–321). Firstly communication, information is transferred between machines and/or humans by communication infrastructures. There are three different communication systems, machine communication like GPS, private communication systems (e.g., chats) and public communication systems (e.g., emergency broadcast). Secondly, CIIs can act as governance infrastructures (information systems) to control other infrastructures, including control information systems (to ensure other infrastructures staying within parameters), autonomous information systems and monitoring systems which also alert in case of violations. Thirdly, CIIs act as knowledge management systems to preserve information for the future. These systems can support decision making, do information retrieval and build knowledge repositories. Lastly, CIIs collect information for further processing from sensor networks and data aggregation systems, for example.

In chapter 4.2, I will explain the key characteristics of CIIs in detail. Nevertheless, it is obvious that these systems already have a big impact on humans and that they will impact humans in the future even more (Dehling et al., 2019, p. 321). Consequently, these CII should be protected to be available anytime.

3. Methods

3.1. Literature Review

Searching for relevant literature

To achieve the aim of the work and categorize V2X-enable CMI into CII or not, I needed to find characteristics and challenges of V2X. The research is restricted by my focus on the two main components of V2X, namely V2V-and V2I communication. Therefore, I did a literature review and used six of the seven main databases of computer science: ACM, EBSCOhost, Emerald Insight, IEEE, ProQuest and ScienceDirect. My first search string (V2X in all possible fields, no restrictions at all) provided only eight results at AIS eLibrary. None of them were peer-reviewed. So, I decided to not use this database.

Next, I started to build up the main search string. As mentioned before, the goal was to find challenges and characteristics of V2X, so I searched in all possible fields for V2X and synonyms (e.g., V2V, V2I, …) and restricted the titles on challenges and characteristics as well as synonyms of V2X. If possible, I also delimited the keywords (on challenges and characteristics) and enclosed only peer-reviewed paper, to ensure high quality of papers. The final search string of each database and the number of results I received, is shown in appendix A. By all databases together, I found 532 potentially relevant papers. To identify the relevant ones, I first checked the title and abstract of each paper. Most of the papers (283) were technical and explained, for example, specific algorithm or models/schemas for technical optimization. Another big group of papers have been off-topic (140). Moreover, 36 papers were duplicates and another 28 papers turned out to be actually no real papers, instead some kind of cover sheet of a conference without any relevant content or a PPT-presentation. Two papers were not in English and one paper which seemed to be relevant was not available to me. After all, only 42 papers remained relevant.

For the next step, I read these papers in detail.

In this step, I excluded papers that were off-topic (e.g., vision about C-V2X in China or power management of hybrid electric vehicles) (6), were about specific parts of V2X (e.g., reducing side-sweep accidents) (6), were technical (e.g., V2V channel modeling and measurements) (4), I had no access to (2). In addition, I excluded a paper which was too old (published in 1994) and furthermore was not related to V2X in particular. In conclusion 23 paper remained relevant, as shown in figure 3.

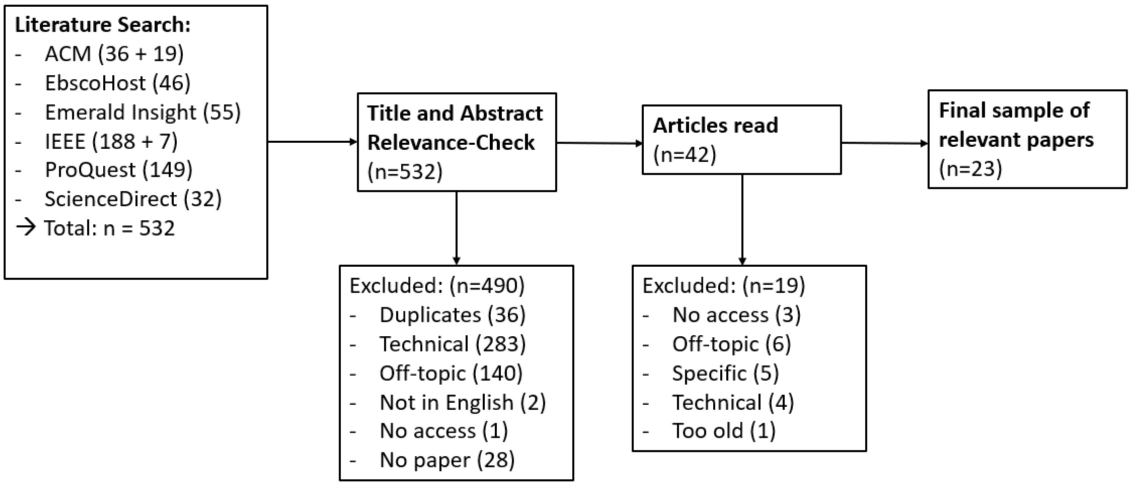

Figure 3: Illustration of the Literature Selecting Process

Classifying the information into Master-Constructs

To retrieve systematically information about characteristics and challenges of V2X, I decided to build up master-constructs similar to the method of Lacity et al., 2010, p. 398 for every different challenge/characteristic. Each master-construct is a union of similar challenges/characteristics referred to a specific topic. Sometimes they are named differently in various papers, so this kind of categorizations helps to provide an overview over all points mentioned in the papers. Thus, the master-constructs facilitate not only to comprise similar challenges/characteristics, but also to validate the importance of each master-construct. A master-construct which is coded in 10 papers, for example, is more important than a master-construct only coded twice. While reading the relevant paper, I created a new master-constructed for each new challenge/characteristic in order to V2X communication that could not be assigned to an already existing one. Finally, after reading all 23 relevant papers, I identified 15 different master-constructs (see table 1). For all identified master-constructs, I defined a name and a brief description which is shown in table 1. The most relevant master-construct is Data security and privacy, which was coded in 18 of 23 paper.

Table 1: Overview of all Master-constructs

Master-construct	#-coded	Description
Information Overload to manual Driver	1	Information overload to the driver when using V2X applications.
Lack of Applications	1	Many applications exist only in theory, how to facilitate the development of new ones.
Network scalability	2	Scalability challenge of V2X communication.
Adaptability to future technologies	2	Refers to the ability to be compatible with future technologies.
Prioritization	3	Refers to challenges in order to priorization of messages.
Location awareness	4	Extents to challenges of location awareness.
Obstacles	5	Extent to challenges occurring in communication through obstacles.
Infrastructure	8	Refers to challenges in order to the infrastructure needed for V2X.
Heterogeneous	8	Extent to different devices, technologies, and policies.
Standardization	8	Refers to the challenge to achieve standards that ensure interoperability among systems.
Legal Responsibility	9	Extents to challenges that belong to technical aspects like legal responsibilities and security policies.
Data (Computing, Aggregation, Transfer)	9	Refers to the challenge how to handle the amount of data.
Mobility	10	Refers to the vehicle's mobility and the challenges coming along thereby.
Communication-Form	12	Extent to new communication form (e.g., routing protocols) needed to support the new requirements that ensue with V2X communication.
Data Security and Privacy	18	Comprises any part of data security and privacy to ensure safe communication.

4. Results

4.1. Crucial Challenges of V2X

As already the number of master-constructs shows, there are many challenges regarding V2X communication, that have to be resolved before implementing this technology into a mobility infrastructure. If V2X communication is implemented into a mobility infrastructure then I call it a V2X-enable CMI, but in the following I am going to consider only V2X communication.

First, I start with some minor important challenges i.e., challenges that refer to master-constructs that were only coded once. It will take more time until every car drives autonomously (Bulumulle & Bölöni, 2016, p. 1) but before this happens, V2X communication can be implemented and assist the manual driver (Lu et al., 2014, p. 289). So, the manual driver can use and benefit from this technology. Nevertheless, when using V2X applications, more information gets offered to the manual driver. This increases the driver's workload, because the driver has too much information to handle which has a contrary effect on the traffic safety (Lu et al., 2014, p. 296). Thus, V2X applications need to be designed to not overwhelm the driver but assist him with the crucial information, otherwise they will miss their aim and impact the safety negatively. Another challenge accordingly to V2X applications is that the applications only exist in theory (Kehal & Zhang, 2018, p. 227). New business models need to be invented by the car manufacturers and governments to make it easier to develop new applications and take advantage of all opportunities that come along with this V2X communication.

An even more important challenge (twice coded) is to be adaptable to future technologies and trends. As seen for instance in cellular, technology changes fast (Bundesregierung, 2021). 3G was established in Germany in 2004 with a maximum bandwidth of 42 Mbit/s. Six years later, LTE was established and brought a bandwidth about three times as big as 3G to Germany. In 2014, LTE advanced was installed, another improvement of cellular. Since 2019, 5G exists and enables a bandwidth of 10 Gbit/s in theory. Through these changes in the recent years, new technologies like C-V2X were feasible (Shrestha et al., 2020, p. 2). To be able to adapt future platforms, also besides 5G, the V2X communication and security architecture should be built in a way, that it can be adapted to future platforms and benefit from them (Ghosal & Conti, 2020, p. 11).

Although the number of in-vehicle sensors is going to increase, that entails a huge amount of data collected by them (Shrestha et al., 2018, p. 3). Network intelligence is needed in future to preprocess this data right before the data is shared.

For enabling correct functional V2X applications, there is, besides information/data exchange, another important challenge that needs to be resolved, especially for traffic safety and traffic efficiency applications. Data does not only have to be exchanged, but also to be prioritized according to their importance (Karagiannis et al., 2011, p. 599). Usually, data packets carrying safety or traffic efficiency information are more important than others. Thus, this data needs to be prioritized and faster transmitted, otherwise relevant data might come late and an accident is unavoidable (Ghosal & Conti, 2020, p. 11). Also for ensuring a robust and efficient data communication, buffering and queuing techniques should be implemented (Faezipour et al., 2012, p. 96). These two techniques can help that data packets do not get lost and further get transmitted in the right order if other data packets get prioritized.

Another challenge in order to prioritizing data packets is to avoid channel congestions in case of an emergency (Karagiannis et al., 2011, p. 599). The challenge is that every vehicle, located in the area of the emergency, broadcasts emergency messages. This could end in a huge number of messages congesting the channel and other relevant data cannot be transmitted.

Location awareness is another crucial challenge. Vehicles need to be able to track exactly their geo-addressee (Karagiannis et al., 2011, p. 597). Especially applications for cooperative coordination of vehicles like applications for Platooning need to have the exact position of the vehicles (R. Y. Ali et al., 2015, p. 3; Shrestha et al., 2018, p. 3). In Platooning, vehicles drive in a very tight formation, thus the gap between vehicles is very small to reduce the energy consumption of the vehicles by minimizing air resistance of each vehicle besides the first one (MacHardy et al., 2018, p. 1863). If the positions of the vehicles cannot be determined with high accuracy at any time, a platoon formation would not be realizable because accidents might occur quite often due to the small distance between vehicles. GPS which may seemed to be the logical solutions for this problem, has a technical burden. For accurate service, GPS requires a clear line of sight (R. Q. Malik et al., 2019, p. 126767), which is not always available. For instance, if a vehicle drives through a tunnel, then the line of sight is interrupted, and a determination of the exact position is not possible anymore. Furthermore, areas exist with weak satellite reception that also hinder a fast and exact determination of the vehicle's physical position. Generally, for these kind of problems "dead reckoning" methods exist, that calculate the current position based on the last signal and speed (R. Y. Ali et al., 2015, p. 3). However, these methods have some limitations according to speed changes of the vehicles due to e.g., weather conditions. Moreover, the vehicle's mobility/speed does impede the tracking and managing of the exact physical position (Karagiannis et al., 2011, p. 597).

Besides GPS performance, another open challenge in V2X communication is the negative effect of obstacles on V2V communication (Goyal et al., 2019, p. 39). Obstacles can be different. In urban scenarios the impact of buildings especially at intersections, when buildings block the line of sight between two vehicles, should not be underestimated (Lu et al., 2014, p. 292). Buildings lead to signal fading between two communicating vehicles that decreases the efficiency of the communication. Surely not only buildings might be obstacles for communication between vehicles, also other vehicles in between can have a negative impact on the communication (Lu et al., 2014, p. 292). On highways trucks may block the communication path and thereby have bad impact on the communication. As field tests have shown, also the high mobility of the vehicles and the urban environment lead to several problems in communication (e.g., doppler effects, intermittent links). Consequently the impact of these unavoidable obstacles has to be considered in the development of V2X in particular V2V communication (Jimenez, 2015, p. 539) otherwise there will be some major problems in the increasing traffic of cities nowadays.

Heterogeneity of V2X is an even bigger challenge (coded eight times). There is heterogeneity in different ways. The most obvious one, is the technology deployed. To communicate, the same V2X technology is required (Bazzi et al., 2019, p. 2). If a vehicle uses, for example, DSRC and another uses C-V2X than these two cannot communicate with each other. Consequently, vehicle manufacturers have to implement the same technology, which is another challenge I will carry on later. Furthermore, different countries have different policies for security and privacy and the available infrastructure also differs, which makes it difficult for the manufacturers (Goyal et al., 2019, p. 39). Driving with a car abroad might make the usage of V2X communication impossible or may lead to high latency because different protocols are used. As mentioned before, safety applications, for instance, do need low latency for fast transmitting of data packets otherwise these applications lose their impact on road safety (Alnasser et al., 2019, p. 37). Moreover, a proper synchronization of different V2X technologies based on different manufacturers is difficult to achieve (Ghosal & Conti, 2020, p. 11).

Additionally, V2X means not only communication between vehicles or between vehicles and the infrastructure, but also between vehicles and pedestrians or cyclists (Shrestha et al., 2020, p. 2). Pedestrians do not have an OBU with them rather a smartphone which has other technical specifications than OBUs (Alnasser et al., 2019, p. 37). The challenge is to ensure V2X communication also between these heterogeneous devices (Alnasser et al., 2019, p. 8).

To do so, standardization is a big aim to achieve that facilitates interoperability among the heterogeneity as described before (Axelrod, 2018, p. 35). Missing standards hinder the development and implementation of the V2X architecture as well as the development of applications therefore (Kehal & Zhang, 2018,

p. 226). Missing standardization and agreements of the type of hardware, software, frequency, protocols etc., results in different usages of technologies by the manufacturers that makes interoperability among vehicles of different manufacturers even more complicated.

Besides the challenge of missing standardization of technology, also the conditions of simulations vary a lot, especially in security simulations (Huang et al., 2020, p. 262). Consequently, it is hard to compare different approaches and find the best one for improving the technology. Everyone tries to build up conditions that show the best possible results. However, a general simulation platform with V2X use-cases and typical scenarios is necessary to better compare different approaches and evaluate them fairly. For developing standards (technical and for simulations) it is recommended to create a group of all involved interest parties (e.g., manufacturers and politicians) (Axelrod, 2018, p. 36). An EU-wide standardized vehicular communication architecture that also includes a standardized security level/solution remains a big challenge (Papadimitratos & Hubaux, p. 61). However, finally it is essential for successful deployment (Jimenez, 2015, p. 538).

Furthermore, there are many legal responsibilities that have to be clarified before implementation (Karagiannis et al., 2011, p. 587). Therefore, a system management framework needs to be established that defines roles and different responsibilities (Axelrod, 2018, p. 35). Roles to clarify, for example, who is responsible for the maintenance of the infrastructure outside the vehicles and who has to pay for it. To respect customers privacy, policies need to be created as well as security policies to define rules for security mechanisms (Ghosal & Conti, 2020, p. 27; Karagiannis et al., 2011, p. 587). Thus, these policies can act as guard rails for designing applications for V2X. There already exists security policies for DSRC in particular but not for C-V2X (Ghosal & Conti, 2020, p. 27). Especially due to C-V2X is currently seen as the preferred technology that will be implemented (Ghosal & Conti, 2020, p. 8), it is a problem that there are no policies yet. Besides the beforementioned policies, liability has to be clarified (Axelrod, 2018, p. 35). Especially in case of human driver involvement, for example, if an accident of vehicles equipped with V2X technology occurs and the liability has to be clarified. Do drivers can rely on V2X notifications or do V2X applications only act as an additional safety-system without liability. So, the driver needs to check everything by himself to be absolutely sure as he is liable for any driving behavior, like it is currently the case in Germany for example (Eskandarian, 2012, p. 1529). Until all vehicles are fully autonomous and able to communicate with the infrastructure and other vehicles, human intervention will continue (Axelrod, 2018, p. 23). As long as human drivers are not allowed anymore, there will be a mixture of fully autonomous vehicles and not fully autonomous vehicles, driving will may become more unpredictable and more cognitively challenging for the human driver (Bulumulle & Bölöni, 2016, p. 1).

Thus, it must be clarified, for example, who is liable in the stage of available V2X communication and human drivers. Other unsolved problems are the certification of vehicular applications (Papadimitratos & Hubaux, p. 60) and validation of V2X technology which has become more difficult due to wide range of scenarios of V2X (Liang et al., 2015, p. 9). Validation is important to discover unknown properties of the technology and to adjust in case of undesirable behavior. For successful implementation also public acceptance is needed because the penetration rate among vehicles influences the results of V2X communication (Jimenez, 2015, p. 538). Human acceptance depends on the trust in a new technology which can be achieved by i.a. validating the functionality (Koester & Salge, 2020, p. 1). Hence, the human factor is not only a challenge in driving behavior and road safety (R. Q. Malik et al., 2019, p. 126765) but also crucial when it comes to new technology's acceptance like V2X communication (Jimenez, 2015, p. 538; Koester & Salge, 2020, p. 1).

The mobility of vehicles is even more challenging for V2X than legal responsibilities as the number of being coded shows (10 times). Vehicles are very dynamic as they move with high speed which has impact on links between nearby vehicles and links between vehicles and RSUs (Liang et al., 2015, p. 1). Also the network topology changes fast and becomes instable due to the trajectory and the vehicle's mobility (Lu et al., 2014, p. 292; MacHardy et al., 2018, p. 1866). This leads to several problems like very short connections, which has impact on routing and addressing of messages. In some cases, connections are also served before they can be used. Vehicles leave the limited communication range of RSUs or other vehicles quickly, which results in interruptions of established connections, thus, data flow disconnections occur (Lu et al., 2014, p. 292; R. Q. Malik et al., 2019, p. 126766). In addition, there may be higher latency due to frequently connecting and disconnecting of connections (Goyal et al., 2019, p. 39).

The network density of each RSU is also challenging and varies a lot depending on the traffic (Goyal et al., 2019, p. 39). Further factors are the location of a RSU (e.g., urban or rural area) or the daytime (e.g., less traffic in the night than in the daytime). With increasing density of vehicles, the existing requirements of location awareness, mobility, and latency can be barely satisfied (Shrestha et al., 2018, p. 2).

This leads to the next challenge, comprised as the communication form. V2X applications require different QoS means that applications need, for example, different transmission data rate and varying fulfillment delay, which has to be guaranteed for successful deployment (Zhou et al., 2020, p. 315). To handle the mobile environment, heterogenous systems and diverse QoS requirements, new efficient routing protocols and forwarding algorithms need to be designed, which is very challenging (Goyal et al., 2019, p. 39; Karagiannis et al., 2011, p. 611). Furthermore, to reduce latency it should be clarified which data has to be transmitted and which data has to be preprocessed (Ghosal & Conti, 2020, p. 11). Preprocessing of data might reduce the total amount of transmitted data and relieve the connections. Moreover, V2X communication does not have a central bandwidth coordination (Goyal et al., 2019, p. 39). This may result in congestions in high density areas due to limited bandwidth. To reduce a delay of messages in the mobile environment, the challenge of bandwidth coordination has to be resolved (Liang et al., 2015, p. 8). Additionally, various interfaces (e.g., DSRC, C-V2X) have to be implemented to enable connectivity, which increases the costs and also hinder the development of connected vehicles (Lu et al., 2014, p. 296). Providing a unified solution for V2X would solve this problem.

Computing and aggregation of data is another big challenge as implied before. As a connected vehicle produces about 30 TB of data each day, it is obvious that this becomes a challenge (Shrestha et al., 2020, p. 15). Further, vehicles collect data from nearby vehicles, so the amount of data increases (R. Q. Malik et al., 2019, p. 126765). Aggregating the data is quite challenging but helps to minimize data source inaccuracy and unreliability. Nevertheless, information aggregation primitives are required to reduce the overhead of information, which is becoming a challenge in order to the overhead that is already added for communication security (Papadimitratos & Hubaux, p. 61). Furthermore, various data about speed, direction and the current position of the vehicle, for example, need real time computing (Goyal et al., 2019, p. 39). Therefore, high computational ability is required, which is a big challenge. Further, there is some more open research to do when it comes to processing of data (Faezipour et al., 2012, p. 95). For instance, it has to be clarified which data has to be processed in-vehicle and which data has to be processed in a data center that might have unlimited processing power (Faezipour et al., 2012, p. 95). These data centers first have to be built, which is another challenge. Fog Computing may be a promising technology that might help in order to data processing (Shrestha et al., 2018, p. 6).

Finally, the biggest challenge is security and privacy like the table of master constructs shows (18 times coded). With an increasing number of connected cars communicating wirelessly (e.g., with V2X communication), it also provides access for hackers to manipulate car data (Ghosal & Conti, 2020, p. 27). Attacks in V2X can be varied and might have devasting impact on road safety and/or driver judgement (Faezipour et al., 2012, p. 92). Some examples are disseminating of false data that could harm the traffic flow, interception of private information and using them against other users, or intentional flooding of the communication network with junk data that might end in denial of service and finally could result in a collapse of the network (Faezipour et al., 2012, pp. 97–98).

To avoid attacks and provide a safe trustworthy communication, the following six requirements have to be met (Ghosal & Conti, 2020, p. 12). First, there has to be authentication to guarantee that a message is sent by a real sender. Second, integrity of messages must be ensured. Modifying messages after sending should not be possible for anyone. Third, access control is required to avoid unauthorized access to the communication network. Fourth, it should be guaranteed that the messages are not shown to anyone else than the defined receiver. Fifth, communication should be available at any time, also in case when faults occur thus fault tolerance is required. Lastly, privacy and anonymity of the users have to be protected. Personal and private information should not be revealed. Achieving this level of security and privacy is a huge challenge to be resolved especially when it comes to the characteristics of V2X because traditional solutions do not perform as expected (Alnasser et al., 2019, p. 35).

The lack of consistent infrastructure and unstable topology due to the vehicle's high mobility impede the performance (Alnasser et al., 2019, pp. 36–37). Further, V2X does consist of different road entities with different capabilities and resources. For instance, vehicles and road infrastructures do not have problems related to power consumption but V2X also consists of mobile phones used by pedestrians or cyclists. However, mobile phones have a limited battery. Thus, security models have to be light weighted.

Generally, adding security also means adding high overhead in terms of communication and processing (Calandriello et al., 2011, p. 898). Consequently it is a big challenge to achieve a good tradeoff between security and QoS (Huang et al., 2020, p. 249).

The majority of security systems can be divided into two different schemes, cryptographic and trust based schemes (Huang et al., 2020, p. 245). Cryptographic schemes like public key infrastructure (PKI) can be used to ensure privacy and trust in the received message (Karagiannis et al., 2011, p. 599). These systems are robust and efficient against outside attacks (Huang et al., 2020, p. 245). Nonetheless, large communication overhead and unavoidable computing time also come along due to the encrypting and decrypting process (Alnasser et al., 2019, p. 37; Huang et al., 2020, p. 249). Trust based schemes are used to complement cryptography schemes and determine the trust of a vehicle or a message by a reputation score without cryptography involved (Huang et al., 2020, p. 255). This score is "accumulated and calculated by a reputation serve based on the feedback given by other users" (Huang et al., 2020, p. 255). Hence, a higher verification efficiency can be achieved.

The usage of anonymous vehicle identities is an approach to achieve a high level of privacy (Karagiannis et al., 2011, p. 599). Further, there is always a tradeoff between privacy and liability because anonymous identities cannot be followed up. Because of that, many solutions use pseudonyms instead (Huang et al., 2020, p. 245). Therefore, authorities are needed that trace the real identities of vehicles, especially in case of malicious vehicles. Nevertheless, pseudonym solutions face several challenges when it comes to reveal sensitive data due to the location and time where a vehicle occurs. Moreover, frequently changing of pseudonyms when sending messages can facilitate identifying the vehicle based on the speed and direction transmitted by messages. However, all the solutions do have some limitations, that hinder successful deployment (Huang et al., 2020, p. 248).

Furthermore, every security system has some weak spots where attackers may break into the system (Huang et al., 2020, p. 262). Consequently, mechanisms have to be designed that detect illegal intrusion and defend against them (Ghosal & Conti, 2020, p. 12). In addition, anomaly detection systems might be helpful in order to behavioral analysis of attacks and identification of suspicious situations to raise the alarm and better protect the vehicle from attacks and failures (Faezipour et al., 2012, p. 98). There are some open challenges when it comes to attack identification because it is often difficult to distinguish between an attack and a malfunction (Papadimitratos & Hubaux, pp. 60–61). Further, revocation mechanisms are required to exclude malicious messages or vehicles from the network and recover from the attack (Huang et al., 2020, p. 261).

4.2. Classifying V2X-enable CMIs Characteristics regarding CIIs

Now I am going to classify the characteristics of V2X-enable CMI regarding to CII. In contrast to the chapter before, I do not only focus on V2X as a communication technology. I rather focus on a mobility infrastructure that enables V2X communication. A CII has ten key characteristics according to recent research (Dehling et al., 2019, p. 325). To check if V2X-enable CMI comply with these characteristics, I will proceed as follows. I will go on for each characteristic of CIIs separately. First, I am going to explain a characteristic, then I will have a look on how it might be in V2X-enable CMI. Does V2X-enable CMI also have this characteristic or not and in which manner? Afterwards, I will go on with the next key characteristic. In the end, after I have checked every characteristic, I will draw a conclusion and classify V2X-enable CMI accordingly.

Socio-technical is the first key characteristic of CIIs (Dehling et al., 2019, p. 325). It means that a CII consists of different parts of social and technical nature that are interdependent. Technical structures belong to CII as well as regulations, laws, and organizational processes. Consequently, the two parts (social and technical) have to be considered when a CII will be improved.

V2X-enable CMIs consist of the road infrastructure (e.g., streets, traffic lights, traffic signs), vehicles and pedestrians. Vehicles can communicate with another and the infrastructure (Alnasser et al., 2019, pp. 5–6). Additionally, they can also communicate with pedestrians or cyclists, for example, via mobile devices like smartphones (Alnasser et al., 2019, p. 37). Avoiding accidents and thereby saving lives and avoid injuries is the aim of V2X communication and reason for inventing V2X communication (Ghosal & Conti, 2020, p. 2). Therefore, vehicles and the infrastructure are equipped with technology that enables communication as explained before. Thus, technical parts of CIIs are given in the context of V2X-enable CMI.

V2X-enable CMIs aim to transport people safely and improve traffic efficiency and be more environment friendly (R. Y. Ali et al., 2015, p. 1). One day, all cars drive fully autonomous, manual drivers are required to drive the vehicles. In this case, the driver uses the road infrastructure with the vehicle and receives information/notifications by the V2X communication of his vehicle, for example, to better judge in critical situations before a crash might occur or to select the fastest route to the destination (Karagiannis et al., 2011, pp. 585–586). In the case of fully autonomous and cooperative vehicles (due to V2X communication), human drivers are not needed anymore. People use vehicles only as a passenger to get to the destination.

The V2X communication becomes more important because the only passenger's choice might be the destination. Maybe it is possible to include a preference route-characteristics as well as the most environment-friendly route (R. Y. Ali et al., 2015, p. 1). All choices regarding driving are at the vehicle's responsibility (Koester & Salge, 2020, p. 1) and are influenced by the information disseminated by other vehicles, the infrastructure, pedestrians when using cooperative autonomous driving (S. Liu et al., 2019, pp. 1709–1710).

As the main aim of this infrastructure is to safely transport people, first in an assistant manner in manual driving and later as a crucial part of cooperative autonomous driving (S. Liu et al., 2019, pp. 1709–1710; MacHardy et al., 2018, p. 1860), the reference as a social part is already the case. Other parts referred to as the social part also exist. Regulations are required to implement the infrastructure successfully and the liability has to be clarified (e.g., in case of accidents or data lacks/abuse) (Axelrod, 2018, p. 35; Karagiannis et al., 2011, p. 587). Beyond regulations and liability, some organizational concerns need to be clarified in order to responsibilities such as the responsibility for the maintenance of the infrastructure required for V2X communication (Axelrod, 2018, p. 35; MacHardy et al., 2018, p. 1858). So, the social part of CII is given in the context of V2X-enable CMI as well. Consequently V2X-enable CMIs are socio-technical and the characteristic “socio-technical” applies.

The next key characteristic of CIIs is “interconnected & interdependent” (Dehling et al., 2019, p. 325). This characteristic means that the social and technical parts are all interconnected. These interconnections could also belong over boundaries of countries. Thus, even small changes to specific parts of the CII can have huge consequences because of the complex network formed by a CII. So, any part might depend on another party that is not visible without further contemplation.

In the context of V2X-enable CMI, for instance, technical solutions for securing the V2X communication and providing privacy will exist. These solutions have to guarantee a specific level of protection according to the laws of security and privacy, which have been created by the politicians of each country or in case of the European Union (EU) by the corresponding deputies of the European countries together (Ghosal & Conti, 2020, pp. 27–28; Papadimitratos & Hubaux, p. 61). If solutions exist that do not guarantee at least this level of security and privacy, then they cannot be deployed as a consequence of violation of the law. Further, any technical solution of V2X communication has to satisfy appropriated regulations to be deployed. Moreover, new technologies such as V2X always have to comply with current regulations otherwise users do not have trust in the technology and avoid using it (Koester & Salge, 2020, p. 1). Consequently, the successfully introduction would fail.

As the road network does not stop at a country’s boarder but also continuous in der neighboring country and vehicles from abroad also use the roads in foreign countries, the used technology in a V2X-enable infrastructure has to be interoperable with the ones from abroad (Axelrod, 2018, pp. 35–36; Papadimitratos & Hubaux, p. 61). Otherwise, vehicles of a country cannot communicate with foreign vehicles and the infrastructure might not work as well as before anymore. Thus, there exists a dependence of technical parts like security solutions of V2X-enable CMI on social parts like laws, regulations, and potential user’s trust in a country and even across borders.

The second part of the characteristic is the consequences of small changes in relation to the complex network’s functionality. As V2X-enable CMIs are complex systems including various social and technical parts, small changes might have significant consequences.

It is actually very challenging to design security and privacy mechanisms that provide a security level according to current regulations in combination with the required performance for the V2X environment, as the remaining challenges show (e.g., Ghosal & Conti, 2020, p. 12). Small changes/intensifications in the regulations later, might affect the ornately designed mechanisms. Consequently, these mechanisms may need to be a little adjusted to satisfy the higher requirements. Supposed that security mechanisms are just a little adjusted to meet the law again without having a look at the consequences of the adjustments. In that case, the security mechanism’s necessary changes might increase the processing time of each message due to a higher security level (Calandriello et al., 2011, p. 898). An increased processing time due to a more complex security mechanism has also impact on each application QoS, which is crucial for the successful functionality of safety applications, for instance (Alnasser et al., 2019, pp. 36–37). If messages of safety applications do not get processed in the defined time interval, the vehicle (the driver in a manual vehicle) may not respond in time. Finally, an accident may not unavoidable. Thus, a small change in the laws might have devasting consequences on vehicle's safety using the V2X-enable infrastructure, if there is no adjustment of the entire infrastructure.

As shown above, the different parts of V2X-enable CMIs are interconnected in various ways and even across the boundaries of a country. Additionally, already small changes have huge consequences on the complex network as the example of changes in the security law shows. Consequently, the characteristic "interconnected & interdependent" complies to V2X-enable CMIs.

Synergetic is the next key characteristic of CII (Dehling et al., 2019, p. 325). This characteristic means that a CII creates a value for the users more significant than the aggregation of the values produced by the different parts. Moreover, a disruption of the tasks executed by the CII would have a critical impact on various aspects of human life.

The vehicle of a user of a V2X-enable CMI can communicate with other vehicles and exchange messages about the vehicle's speed and direction and information about hazardous situations (Liang et al., 2015, p. 2). Further, the traffic flow might be improved by cooperating with the communication forms of V2X-enable CMIs (Ghosal & Conti, 2020, pp. 9–10; Karagiannis et al., 2011, p. 586). The user can also benefit from proper information about the closest restaurants or gas stations, which are available through the applications based on V2X communication of the vehicle (Huang et al., 2020, p. 244). Not to forget about the roads used from the vehicle to drive that are also part of the V2X-enable CMI. These individual opportunities served by V2X communication and the roads have just some little benefits for the user. It is, for example, nice to know how fast the vehicle next to one is driving and in which direction (Alnasser et al., 2019, p. 7) but is supposed to have no further impact on the manual driver. The information per se is less helpful for the driver. However, in combination with smart applications and information from all neighborhood vehicles, more information can be obtained to the driver, which supports the driver's decision in critical situations (e.g., side-sweep or turns) and might avoids accidents (Faezipour et al., 2012, p. 91). Looking at the whole, accidents on the road infrastructure that occur as a consequence of missing information due to false adjusted mirrors or drivers inattention, can be reduced (Bulumulle & Bölöni, 2016, pp.°7–8, 14). For cooperative autonomous vehicles, a V2X-enable CMI constitutes as a central part besides in-vehicle sensors to enable cooperative autonomous driving (S. Liu et al., 2019, pp.°1697-1698, 1709–1710). Thus, the effect of all vehicles using the V2X-enable CMI, is even more significant than the simple exchange of messages while driving on the road.

Further, the yearly economic loss due to motor vehicle accidents on highways, for example, in the USA is estimated to be 836$ billion and it is expected that the number of accidents can be reduced by 80% using V2X communication (Ghosal & Conti, 2020, p. 2). Consequently, V2X-enable CMI does not only have an impact on the safety of the roads but also does have serious economic benefits. Hence, the value created by a V2X-enable CMI is greater than the sum of the individual part's value. Next, a disruption of the tasks performed by V2X-enable CMI needs to have critical consequences. A disruption might be a breakdown of the communication, means vehicles cannot communicate.

Here, it also has to be distinguished between the case of cooperative autonomous vehicles and the case of vehicles with manual driver. In the first case (cooperative autonomous vehicles), the consequences might be even more critical because without the option of communicating, the vehicles only have their own sensors that deliver data for judging how to drive (S. Liu et al., 2019, p. 1709). The driving system depends on the communicated data from other vehicles and the infrastructure as well as the data obtained by in-vehicle sensors (Cui et al., 2019, pp. 2–3). A failure of one component (e.g., in-vehicle sensor or false data distribution) has impact on the vehicle 's driving decision and on the neighborhood vehicles driving decision due to wrong information will be exchanged (Cui et al., 2019, pp.°2,4). This would lead to a major safety loss and hazardous situations would occur, so the likelihood of accidents increases (Cui et al., 2019, pp.°2,4,6).

In case of manual drivers, it depends on the kind of how the driver got used to the notifications that help him to keep track over the complex situations in traffic (e.g., line sweeping). If the driver relies on the notifications he receives at line sweeping, for example, it would result in an accident (Bulumulle & Bölöni, 2016, p. 7). Supposed, the driver might avoid having a close look at the situation by his own, instead the driver relies on the notification that arises if a hazardous situation would occur and consequently more accidents would happen. Nevertheless, driving would still be possible.

Further a disruption of the communication in V2X-enable CMIs could have different kind of consequences that may be more critical in case of cooperative autonomous vehicles than in case of manual driven vehicles. Finally, the key characteristic "synergetic" can be confirmed in V2X-enable CMI.

The fourth key characteristic of CII is called "multifaceted" (Dehling et al., 2019, p. 326). CII perform various tasks, perceived differently by the stakeholders. Further a CII serves "various purposes for various stakeholder without any central governing authority" (Dehling et al., 2019, p. 326).

A V2X-enable CMI has different tasks. First, part of a V2X-enable CMI is the road infrastructure for sure. The road infrastructure is needed for the vehicles to drive. Another task of a V2X-enable CMI is to reduce accidents by enabling communication between vehicles and their environment including other vehicles and the road infrastructure, until one day the ultimate goal of an "accident-free environment" (Faezipour et al., 2012, p. 91) is achieved. Due to the communication among the different entities participating in traffic, an increased awareness of the position and direction of adjacent vehicles arises that helps in accomplishing the task of creating a safer traffic on the roads (R. Y. Ali et al., 2015, p. 1). For the user this might be seen as a progress in traffic safety. Despite for the government, this could be seen as a monetary benefit as the high economic loss due to accident shows (about 836$ billion (Ghosal & Conti, 2020, p. 2)).

Besides that, another task of V2X-enable CMI is to improve the traffic flow (e.g., in the areas of intersections) and avoid congestions by better signal and traffic control (R. Y. Ali et al., 2015, p. 2). Further, V2X-enable CMIs could help to get closer to the goal of energy independence by reducing fuel consumption of vehicles and thereby reduce air pollutant emissions (R. Y. Ali et al., 2015, p. 1). This might be another task which is seen differently by the stakeholders. On the one hand side the driver/passenger may enjoy the benefits of a better traffic flow and less fuel consumption. On the other hand side, the nation's government, for example, gets a step closer towards energy independency and less air pollutions by vehicles.

Advertisements also can be transmitted via V2X-enable CMI (Faezipour et al., 2012, p. 91) such as, for example, information about nearby services like restaurants or gas stations (Huang et al., 2020, p. 244). So, besides the driver/passenger of the vehicle themselves benefit from a V2X-enable CMI, also the owner of services in the neighborhood and/or on the route of the driver's/passenger's destination might benefit. Consequently, a V2X-enable CMI performs different tasks perceived differently by different stakeholders. Hence, CII do not have a central governing authority (Dehling et al., 2019, p. 326). The communication of vehicles in a V2X-enable CMI occurs in an ad-hoc manner without the coordination of a central authority. Vehicles connect with other vehicles or the infrastructure "as they come within the communication range" (MacHardy et al., 2018, p. 1860). From this point of view, a V2X-enable CMI acts like a CII but to achieve the required level of trust within the network, for instance, a trust authority might be needed to manage the registration of vehicles and applications (Huang et al., 2020, p. 246). Nevertheless, the characteristic of multifaceted can be applied in the context of V2X-enable CMIs, because to perform the main functionality (communication) a central governing authority is not required.

The fifth key characteristic is called "opaque" (Dehling et al., 2019, p. 326). As explained in the second characteristic, a CII is a complex system with different parts that are all connected and dependent among themselves. This characteristic leads to opaque although different purposes of the system are easy to identify. Especially the collaboration of the different parts is not easy to understand.

When examining the key characteristic "interconnected & interdependent", it turned out that V2X-enable CMI do have this characteristic. Further, different purposes of V2X-enable CMI have been explained recently. To mention a few, reduction of the number of accidents on the roads, improvement of the traffic flow and reduction of the fuel consumption (R. Y. Ali et al., 2015, p. 1). Thus, the purpose of V2X-enable CMI is perceivable as well as the interconnection of the different parts used therefore, as I have explained before.

Next, it has to be difficult to understand how these different parts work together. The crucial part that might be difficult to understand is V2X communication, which expands the mobility infrastructure and enables communication among the different entities (e.g., vehicles, road infrastructure). V2X communication consists of different parts which have sometimes different tasks and sometimes their tasks imbricate (Faezipour et al., 2012, p. 91). So, there is no total separation of tasks which makes it not easy to understand. As an example, have a look at the two crucial ones, V2V and V2I communication. The task of V2V communication is to enable communication between the vehicles so various applications receive information from nearby vehicles to support driving decisions of the driver (in case of cooperative autonomous vehicles: for the driving system) and overall to avoid accidents by delivering the needed information in time and at the right place (Faezipour et al., 2012, p. 95). Therefore, vehicles exchange different kind of messages such as about their speed and direction (Alnasser et al., 2019, p. 7) or messages about actual road conditions and safety warnings (Faezipour et al., 2012, p. 91). V2I communication also enables transmitting real-time information about the road condition, actual weather, and safety warnings but further V2I communication enables transmitting traffic data, advertisements and obstacle/pedestrian detections (Faezipour et al., 2012, p. 91). Hence, these two different kinds of communication do not have only complementary tasks to accomplish.

However, strictly separated tasks increase the comprehensibility of a system, which is not the case in V2X-enable CMIs. Moreover, the example mentioned above shows only an extract of the operative layer and not even the technical implementation, which is still in research as the many open challenges show. Consequently, V2X-enable CMIs are not easy to understand for layman. Because of that, it can be said that V2X-enable CMIs are opaque in a similar way like CIIs are.

"Inconspicuous" is another key characteristic of CIIs (Dehling et al., 2019, p. 326). As the goal of designing an information infrastructure is usually not to design a critical one, an information infrastructure rather becomes critical over time. Since they often operate unnoticed, their importance only becomes feasible when their tasks are disrupted or other negative consequences manifest. The Cambridge Analytica scandal is a good example to show clearly. Many have been surprised by how easy public opinion can be manipulated by a social network.

The main goal of designing V2X communication and implementing it into a mobility infrastructure as it might be done in V2X-enable CMIs, is to reduce the number of accidents on the roads until one day accident-free traffic and cooperative automated driving is reality (Boban et al., 2018, p. 110; Ghosal & Conti, 2020, p. 2). Thus, V2X communication is going to be designed to have a crucial proportion in achieving this goal. Further, reducing the number of accidents on the roads and thereby saving lives and avoiding injuries through accidents, is already a goal of critical extent. Since V2X communication might be also deployed in case of manual drivers (MacHardy et al., 2018, p. 1860), the impact of V2X communication on the road safety might not be that crucial. V2X communication may influence the driver's decision by notifications being obtained from V2X applications (Karagiannis et al., 2011, pp. 585–586). For example in case of a lane changing, V2X communication can improve the communication between drivers by transferring more information (e.g., ensuring that the information is received by the destination vehicle or directly transmitting the following vehicle's velocity) than by setting the turning lights (Bulumulle & Bölöni, 2016, pp.°3-4,7-8). Further, blind spots will not avoid the communication. An on-board application judges, based on the transmitted relative vehicle velocities, if an accident would occur. If that is the case, the application would prevent the driver to initiate lane changing, for example, or a coordinated course of actions would be negotiated. Thus, in case of manual drivers, V2X manifests in assistance applications for users (Goyal et al., 2019, p. 41) without having conclusive impact on the actual drivers behavior, because the driver still can ignore the notifications (Bulumulle & Bölöni, 2016, p. 1). Further, the driver will probably not distinguish between notifications from internal assistance systems without external data and assistance systems based on external data from V2X communication. Thus, V2X-enable CMIs operate unnoticed to the driver and might be only noticed if notifications do not occur anymore as a result of service disruption in V2X communication.

One day, when all vehicles drive cooperative autonomously, the impact of V2X communication might be even higher. The driving system will judge rationally based on the available information. This information will be obtained by inter-vehicle sensors and as well by data received through V2X communication (S. Liu et al., 2019, pp. 1697–1698). Furthermore, a disruption of V2X communication might have even more devasting consequences because the information needed for judging while driving may be incomplete or false (Cui et al., 2019, p. 2). This may lead to wrong driving decisions ending in accidents. Because passengers of cooperative autonomous vehicles have no influences on driving decisions (Koester & Salge, 2020, p. 1), a disruption of V2X communication also will be only noticed in case of disruptions.

Besides disruptions of the services based on V2X-enable CMIs, they can be also noticed in case of attacks on the data. For example, if sensitive data is stolen and abused against the users (Faezipour et al., 2012, pp. 97–98). Besides stealing data, also false data can be disseminated to control the traffic. There are plenty of other options how V2X-enable CMIs might be noticed negatively due to attackers may be able to break into the system, no matter how strong the security mechanisms will be (Huang et al., 2020, p. 262).

Thus, V2X-enable CMIs operate largely unnoticed until their tasks are disrupted. Especially in case of cooperative autonomous vehicles getting the importance of the V2X communication apparently, because the passengers cannot intervene in driving decisions as the driver of a manual car can do. In consideration of this, V2X-enable CMIs are designed to support also in critical situations but will become even more critical when driving autonomously prevails. Accordingly, V2X-enable CMIs are inconspicuous like CIIs are.

The seventh key characteristic of CIIs is "evolving" (Dehling et al., 2019, p. 326). CIIs do not stay the same all time, instead they are evolving. New technologies replace old ones and services get improved, new features added Moreover, new purposes for CIIs are employed as a result of new stakeholders engaging with them. Sometimes also new regulations/laws force the changes.

As V2X-enable CMI are not deployed nationwide yet (Ghosal & Conti, 2020, p. 2), they are still a very immature technology. Nevertheless, this does not mean that they did not change a lot since the release of the initial technology for V2X-enable CMIs in 1999 (Zhou et al., 2020, p. 309). Starting with DSRC, V2X communication changed a lot in the past years. Besides improvements of DSRC, which is based on the IEEE standards 802.11, also new approaches evolved with the evolution of cellular especially due to 4G (C-V2X) (Shrestha et al., 2020, p. 2). As 5G is being deployed at the present, it also finds the way to V2X-enable CMIs (Zhou et al., 2020, p. 309). 5G is seen as the technology that evolves V2X technology to the next stage, supporting wider range of automotive applications (e.g., cooperative autonomous driving) and has a higher and more consistent data transmission rate as well as a transmission latency of a few milliseconds (Huang et al., 2020, p. 259; Zhou et al., 2020, p. 309) . Thus, the first requirement (new technology replace old ones and services get improved) of this characteristic applies to V2X-enable CMIs. Next, new features evolving over time constitute the seventh characteristic of CMIs.

In the context of V2X-enable CMIs, already an evolution of features is visible. Starting with the goal of enabling communication between vehicles and vehicles with the infrastructure to reduce the amount of road accidents and improving traffic flow (Ghosal & Conti, 2020, p. 1), V2X has evolved. Now, for example, cooperative autonomous driving is an emerging feature (MacHardy et al., 2018, p. 1863). Also new stakeholders engage with V2X-enable CMIs. For instance, electric vehicle manufacturers engage with the technology, which might be a key technology to improve the charging of the electric vehicles and enable new features for better energy management through power grid (C. Liu et al., 2013, pp. 2409–2414). So, new stakeholders engage and evolve new features.

Lastly, legal regulations also have impact on the evolution of CIIs. In case of V2X-enable CMIs, it is obvious that there are especially in regard to security and privacy many regulations (according to local or regional laws) that have big impact on the technology. Since the biggest recent challenges occur related to security mechanism and privacy preservations. Satisfaction of very high requirements are expected which already can be preserved in other use-cases with more homogenous and less mobile parameters (Alnasser et al., 2019, p. 37). Thus, the already existing technologies to provide security cannot be deployed and new ones have to be developed (Huang et al., 2020, p. 248).

Hence, a V2X-enable CMIS also satisfies the requirements of this key characteristic as the technology of V2X communication changes and improves, new features are being developed also by new stakeholders and legal regulations have impact on the evolution of the technology.

Another key characteristic of CIIs is adaptability (Dehling et al., 2019, p. 326). In case of failure of some parts of the functionality, the failed function can be replaced by other parts (technical or social). So, the CII is able to continue offering the services. Devising actions to avoid disruptions is a big challenge. Therefore, an overview of redundancies within a CII is needed.

Due to the possible critical consequences of a V2X-enable CMI that might occur if services are disrupted, it is desirable to have an emergency plan that allows to continue the concerning services. As shown in the characteristic “opaque”, there is no strict separation of tasks into the different parts of V2X respectively V2X-enable CMIs. Some parts have some tasks in common, for example V2V and V2I communication both disseminate safety/warning messages and both disseminate real time road conditions to their environment (Faezipour et al., 2012, p. 91). Consequently, if a RSU cannot disseminate data regarding the actual road condition due to a malfunction of the corresponding sensor, then the data can be disseminated also by vehicles.

Nevertheless, not for every task of V2X there is a certain other part of V2X with an adequate replacement (Axelrod, 2018, pp. 30–34). As there is currently a lack of external systems (e.g., V2X-enable CMIs), vehicle manufacturers and software companies create complex inter-vehicle systems which are able to compensate this lack. Consequently, the replacement of a failed V2X application is an in-vehicle application based on the vehicle's in-vehicle sensors. Thus, in case of cooperative autonomous vehicles, the vehicle often depends on the in-vehicle applications, if a part of V2X communication fails. However, in case of manual driver there is besides the inter-vehicle application also a human that has a look at the actual situation and is able to adjust the driving behavior accordingly. Anyway, there should be another or additional replacement especially in case of cooperative autonomous vehicles.

However, in-vehicle systems are often the data source of the V2X messages (Lu et al., 2014, pp.°289, 292), so these are kind of part of the V2X-eneable CMI. Thus, this characteristic applies in a limited way to V2X-eneable CMI.

The next key characteristic of CIIs is "data-amassing" (Dehling et al., 2019, p. 326). CIIs process information. Therefore, CIIs hoard huge amount of data, which requires a lot of storage and processing power/techniques as well as a high level of security to avoid information privacy violations. Violations easily result in trust problems and can finally lead to rejection.

The key trait of V2X-enable CMIs is communication of the different entities participating in the mobility infrastructure (Zhou et al., 2020, p. 309). The exchange of messages is crucial to achieve various goals. Every message contains data that is processed at least by the receiver and has impact on driving decisions (Alnasser et al., 2019, p. 6; Faezipour et al., 2012, p. 95). The huge amount of data within the network gets visible especially in the fact that each connected vehicle produces about 30 TB of data each day (Shrestha et al., 2020, p. 15). Thus, on the one hand side very high bandwidth is required to transmit the data in a reasonable time, so the different required QoS can be achieved (Zhou et al., 2020, p. 315). On the other hand, these huge amounts of data have to be processed to infer information (Goyal et al., 2019, p. 39; R. Q. Malik et al., 2019, p. 126765).

As V2X-enable CMIs are not in the final stage to be implementable, current research has to resolve many challenges regarding data processing (Faezipour et al., 2012, p. 95). Open research areas are, for example, whether the data should be processed in-vehicle or in datacenters and in a distributed manner or in a centralized manner. In contrary to vehicles, which have very challenging processing power in regards to the large number of sensors they are equipped with (Goyal et al., 2019, p. 39), data centers might have unlimited processing power (Faezipour et al., 2012, p. 95). However, some other emerging technologies such as fog computing might be a crucial support. Fog computing adds an additional layer between central data centers and the vehicle itself (Hu et al., 2017, pp. 28–29). This layer is called fog layer and consists of various widely geographically distributed fog nodes (e.g., routers, gateways, access points) that are able to compute and temporary store data. Thus, fog computing supports "big data analytics by examining the raw data to draw conclusions about a specific information based on inference and enhances data processing at the edge in real time" (Shrestha et al., 2018, p. 6). The fog layer is also connected to the cloud layer to transmit the data and accomplish more powerful computing or storage tasks (Hu et al., 2017, p. 29).

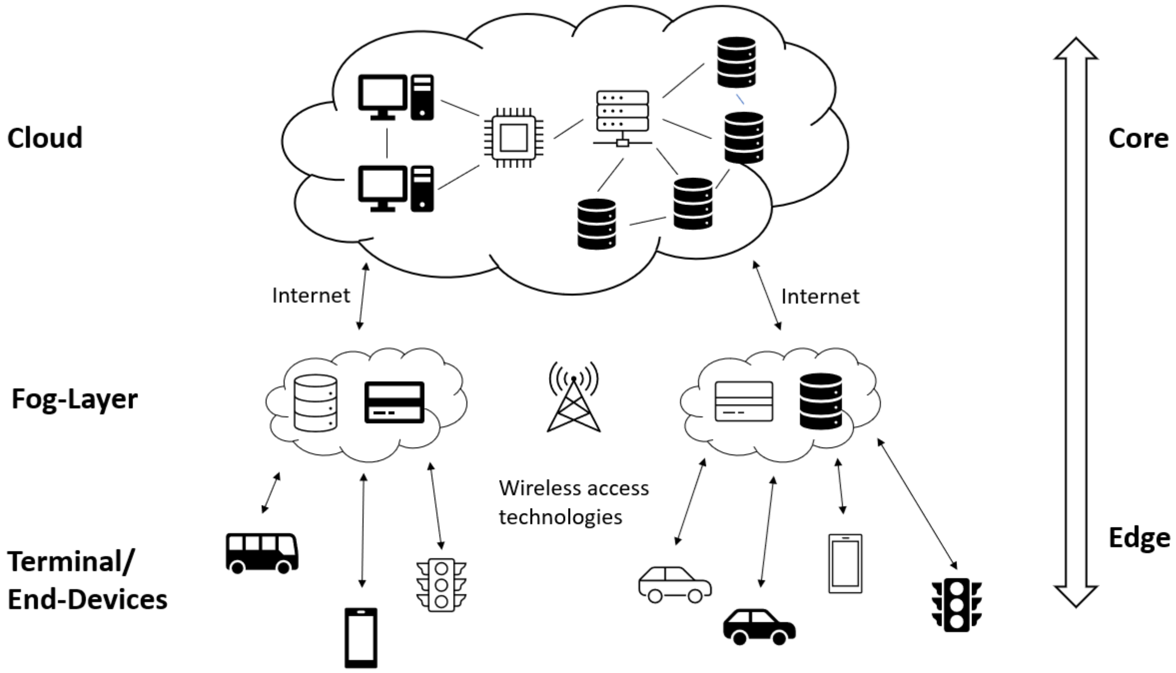

Figure 4: Hierarchical Architecture of Fog Computing (see Hu et al., 2017, p. 29)

This might facilitate real-time processing of big amount of data. Nevertheless, fog computing also faces some open challenges that need to be resolved until it can be implemented (Hu et al., 2017, p. 40), but it provides some promising features to support V2X-enable CMIs in the future (Hu et al., 2017, pp. 37–38).

Besides computing and storing of data, also data security and privacy is a big challenge in V2X-enable CMIs, as the chapter about challenges of V2X communication shows. In V2X-enable CMIs, safe communication is very crucial for successful deployment and to inspire trust (Kehal & Zhang, 2018, p. 228; Koester & Salge, 2020, p. 1). As mentioned before a V2X-enable CMI faces many challenges to enable a safe and trustworthy communication that also protects the privacy of the users. Therefore, another emerging technology, for example, blockchain could be helpful. Blockchain increases trust among vehicles without a central authority and provides privacy and anonymity of the user information (Shrestha et al., 2020, pp. 18–20). Further, data is stored in a transparent and immutable manner. Moreover, the data stored in a blockchain can be considered as true and is traceable. These opportunities that come along with the blockchain technology makes blockchain a promising support to guarantee a high level of security and privacy in V2X-enable CMIs. A high level of security and privacy is crucial to avoid successful attacks on a V2X-eneable CMI that can have devasting consequences like denial of service or eavesdropping (Ghosal & Conti, 2020, pp. 13–14).

As shown above, V2X-enable CMIs amass huge amount of data, hence, data processing and storage are of crucial importance as well as security and privacy of data. Indeed, the final technical solution therefore is not yet available, it is obvious that these are central parts of a V2X-enable CMI. Consequently, also the key characteristic “data-amassing” applies.

The final key characteristic that has to be fulfilled for a CII is “information-disseminating” (Dehling et al., 2019, pp. 326–327). This means, that new available information to a CII can be disseminated quickly to all other parts of the infrastructure.
In V2X-enable CMIs it is very important that new information is disseminated quickly to provide the required information in time to achieve the goals (R. Q. Malik et al., 2019, p. 126767). Nevertheless, some information is more critical and has to be distributed faster than other information (Karagiannis et al., 2011, p. 599). Information gets transmitted via messages as a part of V2X communication in V2X-enable CMI. Thus, there exist different kinds of messages to satisfy each requirement of QoS by the applications and to avoid message-congestions or losing data integrity due to an attempt of fast transmission of all messages within a V2X-enable CMI (Alnasser et al., 2019, p. 6; Zhou et al., 2020, p. 315). Messages such as status messages of vehicles which broadcast information like speed location and direction in regular intervals, are not that time critical (Alnasser et al., 2019, pp. 6–7). Though, the data of these messages should be transmitted within 300ms to enable other vehicles to anticipate, for example, dangerous situations. However, local event triggered messages are time critical and have to be transmitted very fast, in detail within 100ms (Alnasser et al., 2019, p. 7). The information of these messages comprises critical warnings or intersections assist and is sent locally to vehicles or pedestrians only. Especially this kind of information is required quickly by the neighborhood area to avoid accidents. These two kinds of messages are examples to show that information gets disseminated quickly in the corresponding vehicle’s neighborhood. Besides that, in V2X-enable CMIs there are also messages that are disseminated over a wider area. Within these messages, information about global events like road constructions or road congestions are disseminated, so the vehicles route can be adjusted accordingly. Thereby also the roadside infrastructure supports the dissemination of the information to attain a wider area.
Consequently, these different kinds of messages show how new information can be disseminated within the V2X-enable CMI and how fast this happens or rather how fast this communication has to happen when the infrastructure is implemented. Thus, the key characteristic also applies to V2X-enable CMIs.
Now, all ten key characteristics of CIIs in regards to recent research (Dehling et al., 2019, pp. 325–327) have been evaluated. Since all key characteristics of CIIs can also be applied in the context of V2X-enable CMIs, it can be said that V2X-enable CMIs also may be CIIs in relation to the similar characteristics. Thus, they can be classified accordingly as a CII.

5. Discussion

As the current transport and traffic infrastructure is categorized as a critical infrastructure (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2020), I investigated the future V2X-enable CMI regarding to its critical influences on human’s life, and focused on the research question, if V2X-enable CMIs are CIIs or not. I examined V2X-enable CMIs in regards to the crucial key characteristics of CIIs according to previous research (Dehling et al., 2019, pp. 325–327). In comparison to critical infrastructures (e.g., the current traffic infrastructure) that focus on the infrastructure layer, CIIs focus even more on the application layer (Dehling et al., 2019, p. 320).

First, I examined V2X communication for the most crucial challenges due to their characteristics. Therefore, I did a literature review according to Lacity et al., 2010, p. 398 and classified the found challenges into several master-constructs. The number of codes of a master construct points out the relevance of each. Afterwards, I focused on a V2X-enable CMI and examined this kind of infrastructure regarding the key characteristics of CIIs.

The examination of V2X-enable CMIs shows, that they satisfy all key characteristics of CIIs. However, two key characteristics (adaptive and multifaceted) may be applied only in a limited way, I think. V2X-enable CMIs are only in a restricted way adaptive, because not every task of V2X communication can be replaced by another part of V2X communication (Axelrod, 2018, pp. 31–34). Often in-vehicle systems replace a disrupted V2X tasks and not another part within V2X communication. Anyway, also the data of inter-vehicle sensors are used by V2X applications, so in-vehicle systems are kind of part of V2X communication and thereby part of V2X-enable CMIs (Lu et al., 2014, pp.°289, 292). From this point of view, V2X-enable CMIs are adaptive.

The other key characteristic that applies in a limited way to V2X-enable CMIs is multifaceted. The limitation of this characteristic is the supposed need of a central authority to provide a high level of privacy and trust according to some current research (e.g., Huang et al., 2020, p. 246). However, for providing the tasks of V2X communication, a central authority is not imperatively needed because new technologies such as blockchain might avoid the need of a central authority (Shrestha et al., 2020, p. 20). Thus, V2X-enable CMIs may be possible without a central authority in the future and by that, the key characteristic multifaced applies unmitigated.

Nonetheless, V2X-enable CMIs may be classified as CIIs. Thus, V2X-enable CMIs might have critical influences on human's life in future and should be handled accordingly with high prudence.

The reader should bear in mind that this examination of V2X-enable CMIs is based on characteristics which I have discovered in the literature review. Further, there is no nationwide implementation of a V2X-enable CMI yet (Ghosal & Conti, 2020, p. 2), but only research about how this infrastructure could be implemented (e.g., Goyal et al., 2019, p. 38). Consequently, I examined V2X-enable CMIs based on assumptions on how they might be in future, with regards to the current state of research (2020). Furthermore, the key characteristics of CIIs are based on one source (Dehling et al., 2019, p. 325) because there exist no commonly spread characteristics due a missing common definition of CIIs (CIPedia, 2020).

As chapter 4.1 shows, there still exist many open challenges (e.g., processing of data, security and privacy), that should be resolved before the implementation of a V2X-enable CMI could start. The number of codes of each master-constructs underlines the importance of further research in each area. Especially the master-construct security and privacy, I would like to emphasize. Security and privacy will be crucial for successful implementation and additionally crucial to achieve acceptance by the users and establish trust in this new infrastructure (Koester & Salge, 2020, p. 1). Moreover, the master-construct standardization may be of even higher importance than the number of codes shows, I think. This kind of infrastructure should not be implemented nationwide only, but rather in a more transnational way. Thus, usage with foreign vehicles might be possible. Though a coordination across boarders would be essential. Therefore, all different interest parties should work together and build legal and technical guidelines (Axelrod, 2018, p. 36). To design technical solutions, I think there should be a wider view on other emerging technologies (e.g., fog computing and blockchain), which could be helpful to resolve the remaining challenges. In addition, researchers and manufacturers should always keep in mind that they design not just an information infrastructure, but a critical information infrastructure. CIIs might have devasting consequences in case of disruptions or other illegal abuse. Especially in the future with regards to cooperative autonomous vehicles, when human's interventions in driving decisions are not possible anymore.

6. Conclusion

This thesis aimed to classify V2X-enable CMIs into CIIs or not, to enable a better understanding of future V2X-enable CMIs. Based on a literature review of six main databases of computer science (ACM, EBSCOhost, Emerald Insight, IEEE, ProQuest, and ScienceDirect), I first pointed out the most crucial challenges of V2X communication. The biggest challenges are data security and privacy, high mobility of different entities in V2X communication, processing of data and legal responsibilities as well as standardization. The number of different remaining challenges shows clearly, that this technology is still in an immature stage and requires further research until the final implementation could start.

In the next step, I examined V2X-enable CMIs regarding CIIs to respond to the research question, if V2X-enable CMIs are CIIs or not. The examination was based on my assumptions in order to the characteristics and challenges of V2X communication and the classification of the mobility infrastructure into critical infrastructure. The result is, that V2X-enable CMIs have the same key characteristics as CIIs. Thus, I have shown that V2X-enable CMIs may be CIIs and should be handle accordingly.

This classification shows that a failure of V2X-enable CMIs would have critical consequences in various dimensions (e.g., direct human harm, economic loss etc.) like CIIs have (Dehling et al., 2019, p. 320). Consequently, these critical impacts should be kept in mind when designing different parts of the infrastructure like security mechanisms. Before implementation, there should be extensive tests that confirm the expected functionality of this infrastructure and prevent critical consequences, for example, by malfunctions.

Future work should focus on the remaining challenges like security and privacy and also include other emerging technologies in consideration to overcome the challenges (e.g., Fog computing and Blockchain). Furthermore, a future collaboration of all different involved parties (e.g., manufacturers, politicians) might be desirable. Thus, all parties of the collaboration could benefit from the individual competencies. Thereby they could accelerate not only the process of creating this infrastructure but also to enable interoperability among V2X-enable CMIs of different countries.

Appendix

A. Appendix A

The table shows the final search strings of each database I used and the number of results I received.

Table 2: Overview of the Search Strings and the Number of Results

Search String	Restrictions	Database	Number of Results	Date	Annotation
(("V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle") AND (TI "challenges" OR "characteristics" OR "characteristic"OR "risk")) AND (TI "V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle")	scholarly (peer reviewed)	EBSCOhost	46	16.11.2020	with duplicates 72 results
(("V2X" OR "V2V" OR "V2I") AND ti("challenges" OR "characteristic" OR "characteristics" OR "risk")) OR ti("V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle")	checked by experts	ProQuest	149	19.11.2020	
((("Document Title":"challenges" OR "characteristic" OR "characteristics" OR "risk") AND ("Document Title": "V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle")) OR (("Document Title": "V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle") AND ("Author Keywords":"challenges" OR "characteristic" OR "characteristics" OR "risk")))	no	IEEE	188	19.11.2020	Only 150 journals and 38 papers of vehicular technology conferences included. There are 622 results without this restriction.
(AllField:("V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle") AND Title:("challenges" OR "characteristic" OR "characteristics" OR "risk")) OR (Title:("V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle") AND Keyword:("challenges" OR "characteristic" OR "characteristics" OR "risk"))	no	ACM	36	19.11.2020	
Title, abstract, keywords: "challenges" OR "characteristic" OR "characteristics" OR "risk" Title: "V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle"	no	ScienceDirect	32	19.11.2020	
("V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle") AND (title:"challenges" OR "characteristic" OR "characteristics" OR "risk") OR (titel:"V2X" OR "V2V" OR "V2I" OR "Vehicle-to-Vehicle")	no	Emerald Insight	55	19.11.2020	only articles
		Sum:	**506**		

B. Appendix B

The tables show the assignments of papers to the master-constructs.

Table 3: Assignments of Papers to Master-constructs (Part 1/2)

Titel of the paper	Advantages	Data (Computing, Aggregation, Transfer)	Heterogeneous	Communication-Form	Prioritization	Obstacles	Mobility	Location awareness	Adaptability to future technologies	Network scalability	Data Security and Privacy	Infrastrucuture	Information Overlaod to manual Driver	Standartization	Human Factor and Legal Responsibility	Lack of Applications
Future Connected Vehicles: Challenges and Opportunities for Spatio-temporal Computing	1	1						1								
Cyber security challenges and solutions for V2X communications: A survey	1		1								1					
Survey and Perspectives of Vehicular Wi-Fi versus Sidelink Cellular-V2X in the 5G Era	1		1									1				
Reducing Side-Sweep Accidents with Vehicle-to-Vehicle Communication	1														1	
INTEGRATING IN-VEHICLE, VEHICLE-TO-VEHICLE, AND INTELLIGENT ROADWAY SYSTEMS	1										1	1		1	1	
Progress and challenges in intelligent vehicle area networks	1	1	1	1	1		1				1					
On the Performance of Secure Vehicular Communication Systems		1					1				1					
Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions	1		1	1	1		1	1			1			1	1	
Security issues and challenges in V2X: A Survey	1		1	1	1		1		1	1	1	1		1	1	
Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey	1	1	1	1		1	1				1					
Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities	1	1		1												

Table 4: Assignments of Papers to Master-constructs (Part 2/2)

Titel of the paper	Advantages	Data (Computing, Aggregation, Transfer)	Heterogeneous	Communication-Form	Prioritization	Obstacles	Mobility	Location awareness	Adaptability to future technologies	Network scalability	Data Security and Privacy	Infrastrucuture	Information Overlaoad to manual Driver	Standartization	Human Factor and Legal Responsibility	Lack of Applications
Recent Advances and Challenges in Security and Privacy for V2X Communications	1		1								1			1		
Connected Vehicles, V2V Communications, and VANET				1		1								1	1	
Social internet of vehicles: an epistemological and systematic perspective	1								1	1	1	1		1	1	1
Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends	1			1			1				1			1	1	
Connected Vehicles: Solutions and Challenges	1			1		1	1				1		1			
Report on the "Secure Vehicular Communications: Results and Challenges Ahead" Workshop	1	1		1							1			1	1	
Mapping and Deep Analysis of Vehicle-to-Infrastructure Communication Systems: Coherent Taxonomy, Datasets, Evaluation and Performance Measurements, Motivations, Open Challenges, Recommendations, and Methodological Aspects	1	1		1		1	1	1			1	1			1	
Challenges of Future VANET and Cloud-Based Approaches	1	1	1	1			1	1			1					
Evolution of V2X Communication and Integration of Blockchain for Security Enhancements	1	1									1	1				
Securing Vehicles against Cyber Attacks											1					
V2X Access Technologies: Regulation, Research, and Remaining Challenges	1			1		1	1				1	1				
Vehicular Internet: Security & Privacy Challenges and Opportunities	1										1	1				

References

Ali, R. Y., Gunturi, V. M. V., Shekhar, S., Eldawy, A., Mokbel, M. F., Kotz, A. J., & Northrop, W. F. (2015). Future Connected Vehicles: Challenges and Opportunities for Spatio-temporal Computing. In M. Ali, Y. Huang, M. Gertz, M. Renz, J. Sankaranarayanan, J. Bao, & C. Sengstock (Eds.), *Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems - GIS '15* (pp. 1–4). ACM Press. https://doi.org/10.1145/2820783.2820885

Alnasser, A., Sun, H., & Jiang, J. (2019). Cyber security challenges and solutions for V2X communications: A survey. *Computer Networks*, *151*, 52–67. https://doi.org/10.1016/j.comnet.2018.12.018

Axelrod, C. W. (2018). Integrating IN-VEHICLE, VEHICLE-TO-VEHICLE, AND INTELLIGENT ROADWAY SYSTEMS. *International Journal of Design & Nature and Ecodynamics*, *13*(1), 23–38. https://doi.org/10.2495/DNE-V13-N1-23-38

Bazzi, A., Cecchini, G., Menarini, M., Masini, B. M., & Zanella, A. (2019). Survey and Perspectives of Vehicular Wi-Fi versus Sidelink Cellular-V2X in the 5G Era. *Future Internet*, *11*(6), 122. https://doi.org/10.3390/fi11060122

Boban, M., Kousaridas, A., Manolakis, K., Eichinger, J., & Xu, W [Wen] (2018). Connected Roads of the Future: Use Cases, Requirements, and Design Considerations for Vehicle-to-Everything Communications. *IEEE Vehicular Technology Magazine*, *13*(3), 110–123. https://doi.org/10.1109/MVT.2017.2777259

Bulumulle, G., & Bölöni, L. (2016). Reducing Side-Sweep Accidents with Vehicle-to-Vehicle Communication. *Journal of Sensor and Actuator Networks*, *5*(4), 19. https://doi.org/10.3390/jsan5040019

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2020, December 2). *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe - Kritische Infrastrukturen*. https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html Accessed on 02.12.2020.

Bundesregierung. (2021). *5G – Eine kurze Geschichte der Mobilfunkgenerationen*. https://www.bundesregierung.de/breg-de/aktuelles/deutschland-spricht-ueber-5g-1832800 Accessed on 23.02.2021.

Calandriello, G., Papadimitratos, P [Panos], Hubaux, J.-P., & Lioy, A. (2011). On the Performance of Secure Vehicular Communication Systems. *IEEE Transactions on Dependable and Secure Computing*, *8*(6), 898–912. https://doi.org/10.1109/TDSC.2010.58

Chen, S., Hu, J., Shi, Y., Zhao, L., & Li, W. (2020). A Vision of C-V2X: Technologies, Field Testing, and Challenges With Chinese Development. *IEEE Internet of Things Journal*, *7*(5), 3872–3881. https://doi.org/10.1109/JIOT.2020.2974823

Chiara, B. D., Deflorio, F., & Diwan, S. (2009). Assessing the effects of inter-vehicle communication systems on road safety. *IET Intelligent Transport Systems*, *3*(2), 225–235. https://doi.org/10.1049/iet-its:20080059

CIPedia. (2020). *Critical Information Infrastructure*. https://websites.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure Accessed on 09.12.2020.

Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2019). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, *90*, 101823. https://doi.org/10.1016/j.adhoc.2018.12.006

Dehling, T., Lins, S., & Sunyaev, A. (2019). Characteristics of Critical Information Infrastructures. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 325–327). Springer Fachmedien Wiesbaden.

Eskandarian, A. (2012). *Handbook of Intelligent Vehicles*. Springer London. https://doi.org/10.1007/978-0-85729-085-4

Faezipour, M., Nourani, M., Saeed, A., & Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communications of the ACM*, *55*(2), 90–100. https://doi.org/10.1145/2076450.2076470

Federal Office for Information Security. (2021, January 20). *Critical Infrastructures*. https://www.bsi.bund.de/EN/Topics/Industry_CI/CI/criticalinfrastructures_node.html Accessed on 15.02.2021.

Ghosal, A., & Conti, M. (2020). Security issues and challenges in V2X: A Survey. *Computer Networks*, *169*, 107093. https://doi.org/10.1016/j.comnet.2019.107093

Goyal, A. K., Agarwal, G., & Tripathi, A. K. (2019). Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey. *International Journal of Computer Network and Information Security*, *10*(10), 37. https://doi.org/10.5815/ijcnis.2019.10.05

Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network and Computer Applications*, *98*, 27–42. https://doi.org/10.1016/j.jnca.2017.09.002

Huang, J., Fang, D., Qian, Y., & Hu, R. Q. (2020). Recent Advances and Challenges in Security and Privacy for V2X Communications. *IEEE Open Journal of Vehicular Technology*, *1*, 244–266. https://doi.org/10.1109/OJVT.2020.2999885

Jimenez, F. (2015). Connected Vehicles, V2V Communications, and VANET. *Electronics*, *4*(3), 538–540. https://doi.org/10.3390/electronics4030538

Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys & Tutorials*, *13*(4), 584–616. https://doi.org/10.1109/SURV.2011.061411.00019

Kehal, M., & Zhang, Z. J. (2018). Social internet of vehicles: an epistemological and systematic perspective. *Library Hi Tech*, *38*(1), 221–231. https://doi.org/10.1108/LHT-12-2017-0259

Koester, N., & Salge, T. O. (2020). Building Trust in Intelligent Automation_ Insights into Structura. *Forty-First International Conference on Information Systems*.

Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of Information Technology*, *25*(4), 395–433. https://doi.org/10.1057/jit.2010.21

Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends. *International Journal of Distributed Sensor Networks.* Advance online publication. https://doi.org/10.1155/2015/745303

Liu, C., Chau, K. T., Wu, D., & Gao, S. (2013). Opportunities and Challenges of Vehicle-to-Home, Vehicle-to-Vehicle, and Vehicle-to-Grid Technologies. *Proceedings of the IEEE*, *101*(11), 2409–2427. https://doi.org/10.1109/JPROC.2013.2271951

Liu, S., Liu, L., Tang, J., Yu, B., Wang, Y., & Shi, W. (2019). Edge Computing for Autonomous Driving: Opportunities and Challenges. *Proceedings of the IEEE*, *107*(8), 1697–1716. https://doi.org/10.1109/JPROC.2019.2915983

Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected Vehicles: Solutions and Challenges. *IEEE Internet of Things Journal*, *1*(4), 289–299. https://doi.org/10.1109/JIOT.2014.2327587

MacHardy, Z., Khan, A., Obana, K., & Iwashina, S. (2018). V2X Access Technologies: Regulation, Research, and Remaining Challenges. *IEEE Communications Surveys & Tutorials*, *20*(3), 1858–1877. https://doi.org/10.1109/COMST.2018.2808444

Papadimitratos, P [Panagiotis], & Hubaux, J.-P. Report on the "Secure Vehicular Communications: Results and Challenges Ahead" Workshop.

R. Q. Malik, R. Q., Alsattar, H. A., Ramli, K. N., Zaidan, B. B., Zaidan, A. A., Kareem, Z. H., Ameen, H. A., Garfan, S., Mohammed, A., & Zaidan, R. A. (2019). Mapping and Deep Analysis of Vehicle-to-Infrastructure Communication Systems: Coherent Taxonomy, Datasets, Evaluation and Performance Measurements, Motivations, Open Challenges, Recommendations, and Methodological Aspects. *IEEE Access*, *7*, 126753–126772. https://doi.org/10.1109/ACCESS.2019.2927611

Shrestha, R., Bajracharya, R., Nam, S. Y., & Orhan Gazi (2018). Challenges of Future VANET and Cloud-Based Approaches. *Wireless Communications & Mobile Computing (Online)*, *2018*, 15. https://doi.org/10.1155/2018/5603518

Shrestha, R., Nam, S. Y., Bajracharya, R., & Kim, S. (2020). Evolution of V2X Communication and Integration of Blockchain for Security Enhancements. *Electronics*, *9*(9), 1338. https://doi.org/10.3390/electronics9091338

Statista. (2011). *Lebensmitteleinkauf - Bevorzugte Verkehrsmittel 2011 | Statista*. https://de.statista.com/statistik/daten/studie/214883/umfrage/bevorzugte-verkehrsmittel-fuer-den-lebensmitteleinkauf/ Accessed on 07.12.2020.

Statista. (2019). *Anzahl der standardessentiellen Patente für 5G-Fahrzeugapplikationen weltweit 2018 | Statista*. https://de.statista.com/statistik/daten/studie/1035319/umfrage/anzahl-der-standard-essentiellen-patente-fuer-5g-fahrzeuganwendungen-weltweit/ Accessed on 02.12.2020.

Statista. (2020). *Internetnutzer - Anzahl weltweit 2019 | Statista*. https://de.statista.com/statistik/daten/studie/805920/umfrage/anzahl-der-internetnutzer-weltweit/ Accessed on 15.02.2021.

(2018). *Global status report on road safety 2018*. Geneva, Switzerland. World Health Organization.

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

Zhou, H., Xu, W [Wenchao], Chen, J., & Wang, W. (2020). Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. *Proceedings of the IEEE*, *108*(2), 308–323. https://doi.org/10.1109/JPROC.2019.2961937

Declaration about the Thesis

Ich versichere wahrheitsgemäß, die Arbeit selbstständig verfasst, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde sowie die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet zu haben.

Karlsruhe, den 14. April 2021

VORNAME NACHNAME