Cyber Security of Connected and Autonomous Vehicles (CAVs) challenges and avenues for solutions

Schoenmakers, Jan

Cyber Security of Connected and Autonomous Vehicles (CAVs): challenges and avenues for solutions

Jan Schoenmakers

Supervised by

Dr Cristina del Real

Submitted in partial fulfilment of the requirements for the degree of

Executive Master Cyber Security

Institute of Security and Global Affairs

Faculty of Governance and Global Affairs

Leiden University, The Netherlands

The Hague, 2024

Blank page

Abstract: The deployment of Connected and Autonomous Vehicles (CAVs) is increasing. CAVs can offer many benefits related to road safety and environment pollution, to mention just two effects. But CAVs have, due to their heavy reliance on new and innovative technologies supported by software, major cyber security vulnerabilities. In this study we have examined the major cyber security challenges of CAVs and explored the potential solutions to these challenges. Based on a Delphi study of two consecutive rounds, with 20 participants, we identified the three most important security challenges: (1) market dynamics and industry incentives, (2) a missing comprehensive legal framework and (3) technological limitations. To solve these issues government and industry should work on (i) implementing regulation including minimum security requirements, (ii) enforce this regulation; (iii) address safety and security together by a safety-and-security-in-design approach; and (iv) invest in lifecycle management, improve maintenance concepts and replacement, engage in patch management to address vulnerabilities.

Keywords: Connected and Autonomous Vehicles (CAVs), Cyber Security, Regulation, Enforcement, Lifecycle management, Safety-and-Security-by-design.

Acronyms and definitions: list of acronyms and definitions

AI	Artificial Intelligence
CAN	Controller Area Network
CAV	Connected and Autonomous Vehicle
CPS	Cyber Physical Systems
CSMS	Cyber Security Management System
DoS	Denial-of-Service
ECU	Electronic Control Unit
HARA	Hazard Analysis and Risk Assessment
ISO	International Standards Organisation
IT	Information Technology
ITS	Intelligent Transport Systems
OTA	Over-The-Air (updates)
MAAS	Mobility-As-A-Service
NIST	National Institute of Standards and Technology
SAE	Society of Automotive Engineers
TARA	Threat Analysis and Risk Assessment
VANET	Vehicular Ad Hoc Network

Blank page.

Content

Blank page.

1. Introduction

1.1. Connected and Autonomous Vehicles (CAVs)

The "good old" car does not seem to exist anymore. Traditionally, vehicles can be seen as examples of applications of mechanical technology to transport, as vehicles were mostly reliant on physical and mechanical components. Since a few decades electronics and subsequently IT entered massively into the car industry. Current vehicles are the result of a merger between classic mechanical technology and IT. The digitalization of the automotive industry is attracting new players (Tesla, Google, Amazon, Google, etc.) who might finally reshape the whole industry. The traditional world of Original Equipment Manufacturers (OEMs) is converging towards to a world which might finally be dominated by IT companies (Scalas & Giacinto, 2019). Basically, two trends are very important. The first trend is towards more connectivity; where traditional cars although already enriched with electronics are mainly a "closed" system, new CAVs are "open" systems, able to communicate with its environment and other vehicles. CAVs can therefore be considered as implementations of Cyber Physical Systems (CPS) as they are the result of the marriage of physical components and software. The second trend is about autonomous driving. The presence of all kinds of sensors and communication technologies allows CAVs (Thapa and Fernandez: A survey of reference architectures for autonomous cars, 2020) "to differentiate between various types of vehicles, pedestrians, and other obstacles on the road, by analysing the data collected by sensors. Also, AI influences the technology in the vehicles; for example, AI helps the cameras in the vehicle to identify the people in that vehicle, track their eye position and decide whether that person is falling asleep, tired, or distracted. A fully autonomous car is able to perceive, make decisions, and plan". From a hardware driven

industry, the automotive industry is developing into a software driven industry. Software will finally have a dominant position (Burkacky et al., 2018). Although this is applicable to all vehicles, autonomous vehicles rely even more on software as software is capable for critical driving functions with little or none driver assistance. The emergence of CAVs has gained a lot of attention also due to the potential economic (reduction of energy costs, more productive time), social (increased accident prevention and traffic safety) and environmental (lower emissions and air pollution) benefits, paving the way for a smart city (Liu et al., 2020). The facts show that most road incidents are the result of human errors. Another advantage (Burkacky et al., 2018) is the reduction of environmental pollution as the introduction of city shuttles and Mobility-As-A-Service (MAAS) will lead to less vehicles in the streets. The UK government is therefore encouraging the introduction of CAVs (Liu et al., 2020). Also the Dutch association for vehicle owners is very supportive to the entrance of connected vehicles[1]. Central and local governments are generally also positive about the entrance of CAVs as they might bring important advantages (Seuwou et al., 2021) such as reducing pollution and traffic congestion, increasing people safety, reducing noise pollution, improving transfer speed and reducing transfer costs.

On the other hand, due to their large IT dependency CAVs are very vulnerable for cyber-attacks. The high vulnerability is the result of the introduction of all types of communication channels and sensors, each of them being able to collect, store, process or distribute data. Most if not all of these sensors and communication systems have inherent weaknesses which can be exploited. The ubiquitous availability of them in

[1] https://www.anwb.nl/auto/connected-rijden

CAVs indicates that the attack surface is quite large. Cyber-attacks have the capability to make CAVs unavailable, have their operations interrupted, loose control over the vehicle and/or leak (privacy) data. One of the most prominent attacks is the Jeep-Cherokee hack of 2015 which formed a wake-up call for the industry as the researchers were able to connect wirelessly to the backbone of this car. This resulted in a recall program involving more than 1.4 million Fiat Chrysler vehicles (Mulligan and Bamberger, 2016).

One could say that today the issue is not that big since CAVs – especially the most autonomous ones – have not entered massively in the market, which means that there is still time to fix the problem. In our view the sector should not wait too long with solving the issues as according to a report of McKinsey and Company[2] the market size of autonomous driving systems will increase to USD300-400 billion already in 2035. We should however be careful with these forecasts produced by consultancy firms as they might have an incentive to sell their advisory services. In our research we came across highly varying numbers, which should urge us to treat all numbers with

care. It is very likely that the market growth of CAVs will be dependent upon the public views and acceptance of CAVs. And the public acceptance of CAVs, in turn, is highly dependent on the views the public has about the safety and security of CAVs. The public opinion on and public trust in CAVs will be determinative for the acceptance of CAVs. The studies also show that the there is still a lot of work to do in this area as

[2] See: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-drivings-future-convenient-and-connected

the general public has various concerns about CAVs (D. Lee & Hess, 2022; Liu et al., 2020).

There were also dystopic movies such as the Netflix movie ‘You can leave the world behind’ of 2023 containing a scene where, as a result of a cyber-attack, a fleet of Tesla’s is piling up to block a major entrance road to New York. This movies could be a reflection of public worries, amidst of a stream of news articles revealing security weaknesses of CAVs. These weaknesses might be of influence on the public acceptance of CAVs and have also gained attention of national and international regulators due to the public concerns about cyber security of CAVs. It is least clear that the cyber security of CAVs is something to spend attention to ((McLachlan et al., 2022).

At this stage we can conclude that cyber security is a prominent topic when speaking about CAVs, their acceptance and their operations in the field.

1.2. Technologies supporting CAVs

CAVs use a large variety of communication channels such as wireless networks and various sensors to gather road, traffic and other relevant information, also dependent on their stage of autonomy according to the SAE-classification. Fully autonomous cars (SAE stage 5) are much more dependent upon the right information than lower-level vehicles. Another important characteristic of CAVs is the capacity to perform tasks within short and fixed time intervals, as this ability is critical to enable a safe drive.

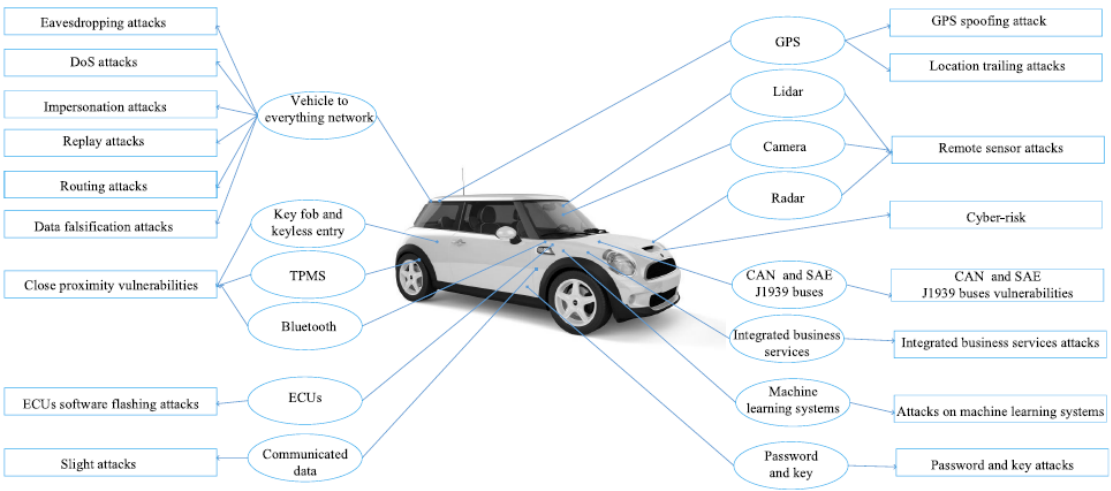
The variety of communication means of CAVs enable them to participate in the so-called Intelligent Transport Networks (ITS) of today. An ITS is a collection of CAVs, infrastructure and communications network which enable a coordinated approach: “By connecting heterogeneous transportation equipment and traffic resources seamlessly, ITS has been a promising traffic management system to satisfy the needs of connecting

vehicles, people, and services. In the smart city era, the requirement is growing dramatically for intelligent and reliable ITS that alleviate traffic congestion, improve traffic rate, and reduce traffic incidents, energy consumption, and environmental pollution" (Deng et al., 2023).

The following kinds of technology are enabling CAVs (Benyahya et al., 2022): (1) in-vehicle sensors, (2) in-vehicle communication-based connectivity solutions mostly wired, based on ECUs, (3) Additional physical ports, (4) Infotainment systems, (5) inter-vehicle communication systems and (6) artificial intelligence software. A detailed overview of the supporting technologies is included in Annex 1.

1.3. Risks in CAVs technologies

The cyber security risks can be categorized in the same way, as there are threats related to sensors, in-vehicle and inter-vehicle communications. The picture gives a good overview of the attack surface of a CAV (Sun et al., 2022):



Source: *Sun et al.* (Sun et al., 2022), © 2022 IEEE; picture included with courtesy of the authors of the article.

There has been a lot of research on vulnerabilities and attack vectors in the past decades. Attacks can be classified following (Khan et al., 2020; Pham & Xiong, 2021; Sun et al., 2022) the types of technology. The first category of attacks relates to *in-vehicle and network attacks*. One variant of this category are remote sensor attacks including LiDAR, RADAR, cameras and other sensors attacks such as tricking the sensor by LiDAR spoofing; where the LiDAR system is misled through the injection of bogus objects into the sensors or RADAR jamming where (Green, 2023)

"a radar jammer transmits signals to a radar's receiver with the intention of suppress its ability to accurately receive its own reflected signal from the target". Also, the GPS can be spoofed (Chapman, 2017) "when someone uses a radio transmitter to send a counterfeit GPS signal to a receiver antenna to counter a legitimate GPS satellite signal". During a location trailing attack privacy can be endangered through relating pseudonymous position samples to specific vehicles. Attacks exploiting close proximity vulnerabilities require vicinity to the targeted CAV for abusing the CAN[3] via function specific ECU[4]s, through the provision of inaccurate inputs to gain access, such as for instance through the Tire Pressure Monitoring System (TPMS) or key fob and keyless entry. In addition, CAN and SAEJ1939 vulnerabilities can by exploited by issuing unauthorized messages or listening to traffic over the CAN, thereby making use of well-

[3] The CAN, or Controller Area Network, is a core bus inside a vehicle, which allows all key systems of the vehicle to communicate with each other. This CAN bus has been introduced in the 80's by firm Robert Bosch and is still having a central function in vehicles.

[4] ECU: Electronic Control Unit, in vehicles various ECUs control specific functions such as the brake system or the motor engine system. All ECUs are connected via the CAN.

known vulnerabilities (no encryption, no authentication) of CAN. ECU software flashing attacks are based upon misusing unpatched software vulnerabilities to gain access to the CAN. A last variant within this category are integrated business services attacks, by first gaining client-level access new attacks can be launched.

The second category of attacks are the *vehicle-to-everything network attacks* which also has multiple attack variants. Denial-of-Service (DoS) attacks are attempts where the attacker is overwhelming the communication channel with messages thereby not allowing legitimate users getting access to the communication channels. Also, the unique identity of a vehicle can be (mis)used by another vehicle, called impersonation attacks. During a replay attack the attacker redistributes messages across a channel to create confusion and wrong interpretation. When an attacker is intervening in the routing process of messages and/or drop messages a routing attack takes place. Just another variant are data falsification attacks where the attacker is transmitting incorrect safety and alert messages. During eavesdropping-attacks the attacker intercepts messages to gain information. The last variant within this category are password and key attacks, where an attacker is trying to crack passwords and entry keys which normally requires substantial investment.

The *remaining (third) category of attacks* is a mixture of various type of attacks such as (i) Infrastructure attacks, where the attacker is not targeting (directly) the CAV but the infrastructure. Note that for their operation CAVs are dependent upon new transportation infrastructure, including road side units, on board units, cloud server, intelligent traffic lights and sensors, traffic management centres etc (Sun et al., 2022); (ii) slight attacks by manipulating data to create hazardous situations and serious safety risks; and (iii) attacks on ML/AI systems (Machine Learning / Artificial Intelligence)

systems where the ML/AI model is impacted by data poisoning attacks, model steal attacks or model inference attacks. ML/AI systems are critical components of primary functions of CAVs and responsible for security-sensitive tasks (Sun et al., 2022).

From what has been discussed it is clear that there is a sheer number of attack targets as a lot of critical components and sensors can be attacked: ECUs, CAN, LiDAR, RADAR, GPS etc. In addition, it is important to identify the various *attack sequences* which can be used (Pham & Xiong, 2021); through which of the many "entry points" will the attacker try to gain access from the outside to the inside (CAN) in order to take over control of the vehicle:

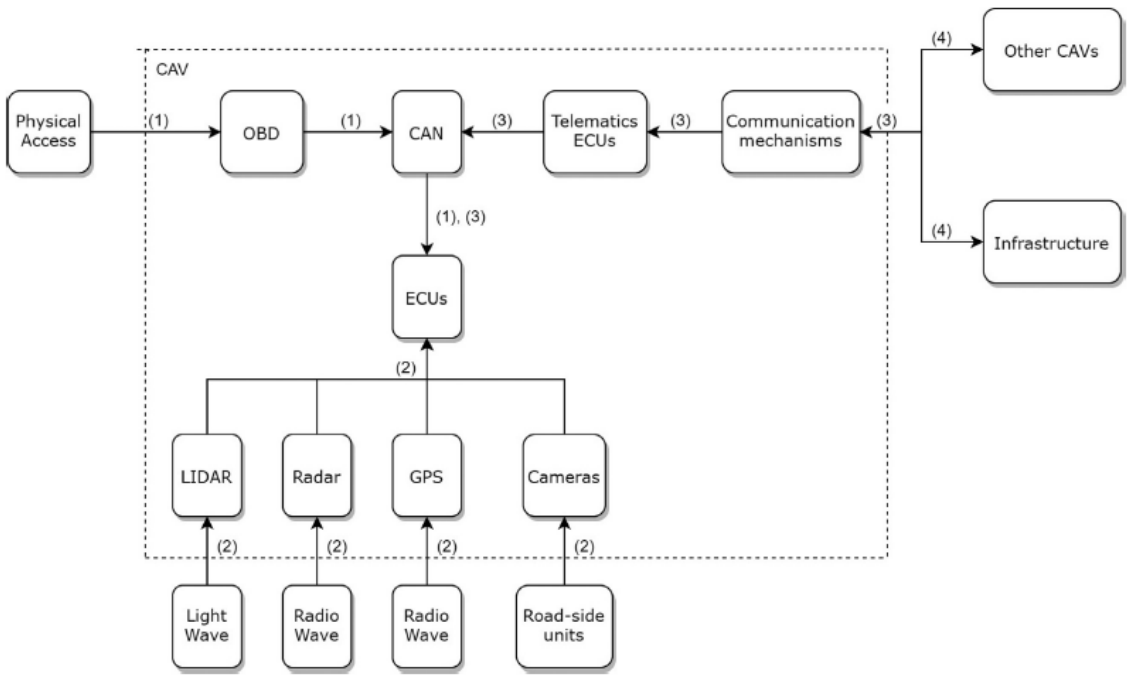


Fig. 5 – Possible attack sequences on the components of CAVs.

Source: *Pham and Xiong*, (Pham & Xiong, 2021)*;* picture included with courtesy of the authors.

In this paper we will not dive further into the various classes of attacks. We refer to the work of various researchers (Pham & Xiong, 2021; Sun et al., 2022). Here, it should

be clear by now that the multitude of communication and sensor technology offers a wide attack surface to attackers, which might want to comprise the CAV for whatever reason.

In the remainder of this paper, we will not differentiate between the various type of attackers (criminals, hacktivists, terrorists, other) also because the number of attacks in the field are quite limited and all attackers will need to use one or more of all identified attack vectors to gain control over the CAV. In the literature three major attack motivations have been listed (Pham & Xiong, 2021): (i) interrupting operations, (ii) gaining control over CAVs and/or (iii) stealing information. Taking into account the big attack surface of CAVs, actions of cyber terrorists actively engaged in attacking CAVs could wreak large havoc. The 2016 Nice truck terrorist attack needed at least one terrorist willing to sacrifice himself. But when terrorists would be able to seize control over all CAVs (not to mention autonomous trucks) of a particular type, the resulting damage for society could be way larger. Although the number of attacks in the field is fairly limited and all research settings where vulnerabilities are exploited are based on controlled settings, this should not give all too much comfort. The low level of real-life attacks might be due to (i) insufficient hackers with the right technical capabilities or (ii) the installed base of CAVs being too limited to allow monetization of a cyber-attack, or a combination of both (Kennedy et al., 2019).

1.4. The current study

Taking into account the issues (challenges) related to cyber security of CAVs as a result of the literature study, which actions and/or measures need to be taken to solve the issues and thereby improve the cyber security of CAVs?

During phase 1 (desk research) two questions will be answered: (1) what are currently the cyber security risks of CAVs? and (2) who are the relevant stakeholders with an interest in (improving the) cyber security of CAVs? The literature study conducted is intended to provide with answers to these two desk research questions. Based on the outcomes of the desk research of phase 1, in phase 2 a Delphi study will be conducted. This study is meant to provide answers on two research questions; (1) which actions and/or measures are needed to overcome the existing issues related to cybersecurity of CAVs? and (2) which stakeholders (automotive industry, legislators/road approval authorities, owners/users, other) should be involved in these actions and/or measures to meet these challenges? The Delphi study will involve the selection of experts identified from literature, representing a few relevant disciplines (industry, academics, government and/or regulation). We will solicit these experts to provide solutions to improve the cyber security of CAVs. To structure the study, we will work with the 3 layers of the cyber security model, which will be introduced in the next sections.

1.5. Definitions and scope

We encountered various slightly different definitions in the literature. For clarity reasons we adopt the definition provided by (Liu et al., 2020). In their taxonomy a "CV is a vehicle that can communicate and exchange information wirelessly with other vehicles, external networks and infrastructure via Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-Everything (V2E) technologies, but that does not necessarily mean that CVs are capable of autonomous driving" (Liu et al., 2020). In this paper an AV is "a vehicle capable of driving themselves without human intervention" (Liu et al., 2020). For AVs, The Society of

Automotive Engineers (SAE) distinguished 6 levels of automation[5] in their international standard J3016 (published in 2016):

SAE level	Meaning
0	No automation
1	Driver assistance
2	Partial automation
3	Conditional automation
4	High automation
5	Full automation

From this overview, mainly AVs on level 4 and 5 can be perceived as true autonomous vehicles. Finally, we use the definition of Nikitas et al. (Nikitas et al., 2020) and define a CAV, the combination of CV and AV, as "any vehicle able to understand its surroundings, move, navigate, and behave responsibly without human input which at the same time has connectivity functions enabling it to be proactive, cooperative, well-informed and coordinated".

CAVs are a rather broad concept. In some views all vehicles which are connected and autonomous to some degree can be part of the definition. Although we accept the broad concept, for the examples in this thesis we will mainly focus on the (retail) user owned CAV and not so much on city shuttles, trucks and other vehicles. Nevertheless, we will use the broad definition in this study as this is the most practical also because the various subcategories have quite some similarities from a cyber security risk perspective; they are all highly dependent upon sensors, communication systems and actuators.

[5] https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.

We will also us take a global perspective. From the literature it will become clear that CAVs are entering the markets in a lot of countries. In some countries very specific conditions are applicable. And there is a huge variety of legislation and standards which has been issued across the globe. In this study we will not focus too much on the country specific circumstances but rather accept the broad variety.

2. Conceptual framework

2.1. Three-layer model of cybersecurity

During our study we use the *3-layer conceptualization model of cyber security* to structure the analysis. The model will help in structuring the discussion when assessing the cyber security threats of CAVs and their solutions which will be discussed later. Furthermore, this will provide us with a framework to check whether the solutions are complete and/or rightly balanced. The model identifies three layers (J. Van Den Berg, 2020). The *first layer is the technical level* which concerns 'pure' IT technology and the security measures in the IT: "IT that enables cyber activities by providing all kinds of underlying supportive services, especially related to world-wide communication" (J. Van Den Berg, 2020). The second level is the *socio-technical level* is about the way humans interact with IT; "cyber activities as being executed by people in an attempt to reach their personal, business, or societal goals. This level considers the activities performed using IT as the key assets, not the IT itself". The third level is the governance layer which contains the layer of rules and regulations (J. Van Den Berg, 2020) that should be put in place to properly organise the two other layers, including their security. This relates, for instance to internet governance next to rules and regulations that influence human behaviour in cyberspace" (J. Van Den Berg, 2020).

2.1.1. Technical cybersecurity challenges of CAVs

For almost all threats described in section 1.3 countermeasures have been defined. We refer to the research paper of Pham and Xiong (Pham & Xiong, 2021) which offers a rich overview of defence techniques. Defence and mitigation techniques are based on the following measures, or combination of them: identification and authorization; redundancy and randomization; (network) segmentation and isolation; cryptography including blockchain for integrity, authorization and authentication; IDS and IPS for detection and response and incident response and recovery. A good overview of the various defence strategies is given in the literature (Dibaei et al., 2019). First, although a lot of solutions seems to be available, this does not mean that all risks have been mitigated effectively; Pham and Xiong (Pham & Xiong, 2021) identified a missing connection between academic research and the implementations done by the industry in this respect. Most of the identified risks and defence measures are based on research. The "real world" of CAVs currently in use might therefore be more risky than necessary.

Second, when overseeing all the research papers there is a material number of remaining issues or challenges. We will discuss most of them here briefly. At the core of the CAV technology there is the CAN, which has critical vulnerabilities that cannot easily be solved. CAN is in the basis a serial bus using a broadcast communication protocol introduced by the firm Robert Bosch in the 1980s. This message-based protocol allows all processors (ECUs) connected to the CAN to submit messages. Although there is some error control, there are no (further) measures implemented for confidentiality (no encryption, no authentication), integrity and availability (Bozdal et al., 2020). Although a few solutions seem promising, for instance a secure communication system of Guardknox (Pham & Xiong, 2021), these issues have not

been solved fully. And there are more technical challenges for CAVs. *Hardware limitations* of IT technology used in CAVs seem to allow only lightweight security technologies. The ECUs in vehicles are mostly embedded systems with low computing power and memory (Scalas & Giacinto, 2019). These components do not allow for various types of encryption (Scalas & Giacinto, 2019). There are r*eal time constraints* as ECUs are working together to realize safety-critical operations. This means that (additional) security measures must not impact these tasks in a negative way (Scalas & Giacinto, 2019). CAV technology is used in *stressful environments* (heat, cold, humidity, vibrations and electromagnetic interference) which puts limits on the impact an ECU might have on the size and weight of the CAV. In addition, the CAN bus topology is for these reasons preferred over a star or ring topology (Scalas & Giacinto, 2019). The issue of *longevity* – CAVs will be for a quit longer period operational than 'normal' workstations – which is posing challenges for maintenance, as the technologies have to be updated for a long period of time. This puts requirements on the hardware in terms of sustainability and the software to be updatable easily (Scalas & Giacinto, 2019).

To complicate things further, the environment including cyber security threats is very *dynamic* (Sun et al., 2022). There is *complexity* due to the sheer amount of technology (sensors, ports, communication channels) in CAVs which all have to operate together. Traditionally, a highly complex system is prone to design or implementation errors. This would require a coherent secure-by-design approach (Liu et al., 2020). The *high level of technological change and innovation* presents the challenge of continuously keeping up with the new types of technology and address vulnerabilities in a swift way (Sun et al., 2022). Another critical issue is the *scope of the technology* considered, as both technology in the CAV *and* infrastructure need to be addressed

together, as isolated solutions might not solve the issues. It is our impression that most of the research literature focuses on the CAV part, not necessarily on the infrastructure part. There are, however, some studies which pay attention to the infrastructure (El-Rewini et al., 2020). To finalize, it should not be forgotten that the introduction of solutions on technical or socio-technical level might bring *new technical security risks*. For instance, the Over-The-Air-update[6] might be vulnerable to man-in-the-middle attacks if not properly designed and executed (Mulligan and Bamberger, 2016).

2.1.2. Socio-technical cybersecurity challenges of CAVs

From the research literature we get the view that there is a strong focus on technical security solutions, more than on the socio-technical level which might need more consideration as research (Liu et al., 2020) revealed that the acceptance of CAVs by the general public is cumbersome. Public acceptance depends on building trust. A range of solutions has been provided at this level. A practical solution are the OTA updates, which are in fact a practical solution to solve technological vulnerabilities which might result in risks for pedestrians. OTA updates are a practical and efficient solution to updating all vehicles remote at the same time to mitigate vulnerabilities (Mulligan and Bamberger, 2016). Other important efforts relate to raising *awareness* at owner/user side. This can be created through campaigns, workshops and advertisements. These activities should lead to building trust among consumers, which is conditional for the consumer acceptance of CAVs (Liu et al., 2020). Related to this, the *education* of CAV users about the cyber security risks of CAVs is also an important investment worthwhile

[6] Over-The-Air update, or OTA-update, is basically an update to an embedded system via a sort of wireless telecommunications network.

taking (Liu et al., 2020) to reduce fear among public and thus to increase acceptance of CAVs. Another study showed that factors such as social influence and the perceived safety are having a significant positive relationship with the *acceptance level of people* for CAVs; where the fear of new technology ("technophobia") is having a negative impact on acceptance levels (Koul & Eydgahi, 2020). In another research setting it was shown that people with more cyber *security knowledge* were better in identifying cyber-attacks on CAVs as they had more situational awareness (Aliebrahimi & Miller, 2023). This research underlines the importance of the human factor. There is US based research showing that a *differentiated approach* might be needed, as demographic variables and political opinions are largely affecting people's concerns related to safety, privacy and security (D. Lee & Hess, 2022).

Nevertheless, also at this level, a wide range of issues or challenges is remaining. It has been illustrated that *awareness and education* of the CAV driver, currently not strongly built, need to be present in order to build *trust* in the new technology of CAVs as the users need to have insight into the risks and dangers of the technology. Once attacked, there are fairly limited resources available to CAV owners to identify or counter the attacks. The CAV owner often does not understand the default configuration or how to best modify this configuration in case of attacks (Kennedy et al., 2019). In a research setting a number of experts which were approached (Liu et al., 2020) believe that education is a key thing to reduce the cyber security risks associated with CAVs. But this might be challenging as cyber security and privacy risks are continuously changing.

The solicited experts in this study claim that there should be legislation from government to enforce a strong education programme as the automotive industry is known for not taking care of education the public on the risks of vehicles (Liu et al.,

2020). Another complication is that *human and psychological diversity asks for a differentiated approach* to improve cyber security. Research further shows that people differ in their ability to identify and respond to cyber security risks (Khan et al., 2020; Linkov et al., 2019). This would plead for an awareness campaign typically focused on the most vulnerable groups (Linkov et al., 2019). Also, humans behave differently when a cyber-attack occurs, where some are able to respond quickly while others face difficulties in multitasking (Khan et al., 2020). In the research cited earlier (Aliebrahimi & Miller, 2023) it was revealed that people with more cyber security knowledge were better in identifying cyber-attacks. However, the *higher situational awareness did not always result in a better response to cyber-attacks*. The research participants with higher situation awareness were not more inclined to take over control of the CAV in cases when this would be required. This could potentially be due to people attributing a (too?) high level of trust to the autonomous capabilities of CAVs (Aliebrahimi & Miller, 2023). Furthermore, the more *transparency* on the CAV and its cyber security, the more the CAV might be exposed to attackers (Liu et al., 2020).

2.1.3. Governance cybersecurity challenges of CAVs

To regulate the 'new' world of CAVs, governments and standard setting institutions have issued a range of standards and regulations related to cyber security. This in contrast to the past, where the automotive industry mainly focused on functional safety[7]. Due to the perceived risks, the attention for cyber security is growing.

[7] ISO 26262. This standard was issued in 2012 and includes recommendations mainly for the functional safety of vehicles. An important element of ISO 26262 is Hazard Analysis and Risk Assessment (HARA)

A very important industry standard (Benyahya et al., 2022; Macher et al., 2020) in this field is *ISO/SAE 21434*. Where ISO 26262 focused on functional safety, this (complementary) guideline focuses mainly on cyber security in interaction with safety. One of the novelties was the introduction of the requirement of having a lifecycle process for cyber security. Instead of Hazard Analysis and Risk Assessment (HARA) as one of the traditional methods applied for achieving functional safety, ISO 21434 is based on Threat Analysis and Risk Assessment (TARA) as a more integrated method. It is important to note that there is a strong involvement from the industry, as the SAE is an industry organization.

A very important international regulation is *United Nations Economic Commission for Europe, Working Party 29 (UNECE-WP.29) regulation R155*. Under this regulation, which will become mandatory for type approval of new vehicles entering the European market starting from July 2022, OEMs can only apply for type approval when the vehicles meet the Cyber Security Management System (CSMS) requirements. The R155 is referencing to ISO 21434, which means that meeting the ISO 21434 requirements is a good starting point for working on compliancy with UNECE R155. Cornerstone of R155 is the requirement to have a risk management approach addressing the entire product lifecycle of a vehicle. The regulation is directed to OEMs which need to comply. They also have a responsibility to implement the requirements across the whole value chain, including all other suppliers. The R155 covers 4 important (UNECE press

release of 24 June 2020[8]) components: "(1) managing vehicle cyber risks; (2) securing vehicles by design to mitigate risks along the value chain; (3) detecting and responding to security incidents across vehicle fleet; and (4) providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "Over-the-Air" (OTA) updates to on-board vehicle software". Noteworthy too are the industry level solutions such as AUTOSAR[9], Harman International[10], Auto-ISAC[11] and the Waymo / Self driving coalition[12]. These solutions can be seen as

---

[8] Source: https://unece.org/sustainable-development/press/un-regulations-cyber security-and-software-updates-pave-way-mass-roll

[9] A 2003 started initiative, a partnership of various key industry players, working on standardization of the software architecture of CAVs. The official website states: "AUTOSAR (AUTomotive Open System ARchitecture) is a global partnership of leading companies in the automotive and software industry to develop and establish the standardized software framework and open E/E system architecture for intelligent mobility", see: https://www.autosar.org/

[10] This Israel based subsidiary of Samsung Electronics is working together with key industry players such as BMW, Audi, Mercedes, Fiat-Chrysler, Toyota, Volkswagen to engage in research of cyber security solutions for CAVs, see: https://car.harman.com/insights/articles/can-hackers-take-control-my-vehicle

[11] Auto-ISAC stands for Automotive Information Sharing and Analysis Center and was formed in 2014 with a focus on cyber security of CAVs. See: https://automotiveisac.com/ This industry organization has published a number of best practice papers

[12] See the website of Waymo: https://waymo.com/

collective efforts of the automotive industry to engage in further research into cyber security risks of CAVs and solutions to these risks.

The list of **remaining issues** on the governance level is rather long. *Market dynamics, business model incentives, tradition and value chain characteristics are leading to the automotive industry (1) not accepting cyber security as a top priority while still focusing on functional safety, (2) not having enough expertise regarding cyber security and/or not sharing it fully; (3) underinvesting in cyber security due to externalities and network effects and (4) not (fully) accepting ownership for cyber security*. Knowledge sharing has become under pressure due to *changes in the structure of the supply chain***.** Where in the past the industry focused on reducing development times to make sure that new cars always have the most recent technology, developing CAVs is a way more expensive and complex task. The dominance of software, technological developments, trends towards more outsourcing, greater importance of cyber security (next to functional safety) and changing customer demands have resulted in a transformation of the automotive industry from a tiered to a network structure (Morris et al., 2020). New suppliers responsible for the complex software systems and the highly integrated hardware systems are taking a leading role. Where traditionally the automotive industry was well-known for its knowledge-sharing, this is changing in the new setting characterized (Morris et al., 2020) by a lack of cyber security knowledge-sharing by participants. One of the underlying issues is that OEMs on top of the chain lack adequate cyber security knowledge according to other suppliers in the chain, which hampers addressing cyber security in the design and development of CAVs (Morris et al., 2020). In addition, there is a lack of trust among participants in the supply chain also resulting in lack of knowledge sharing. The survey also revealed that cyber security is

not a top priority for OEMs as this delays production, increases cost levels and does not contribute to value as perceived by owners (Morris et al., 2020). Another important issue is *ownership and externalities***.** Contrary to traditional cars where OEMs accept the guardian role for safety (safety belts!) this might not be the case for cyber security of CAVs (Kennedy et al., 2019). The transactional nature of the OEM supplier relationships over the supply chain is not beneficial for guardianship which assumes the sharing of risks and responsibilities (Kennedy et al., 2019). "A cooperative approach over the supply chain is essential. Still, effective preventive cyber security solutions might lead to tensions in the relationships between OEMs, suppliers, users and the regulator. In case of inertia, the regulator should step in to improve cyber security" (Kennedy et al., 2019, p. 639). Finally, there is still the risk that the OEM will aim for attaining the minimum level of risk mitigation without being considered reckless. There is an economic externality in play; the OEM will be hesitant to invest in security as he might not experience the negative impact of substandard security. This is a question of social responsibility (Kennedy et al., 2019). The *economics of the supply chain is limiting cooperation* which is needed to improve cyber security. Although cooperation is crucial to achieve safety and security objectives, this is not always achieved[13]. As other researchers point out (Liu et al., 2020) "Nevertheless, building economically successful CPSs has been the priority, since traditionally security and privacy issues can

[13] Main issues (Khan et al., 2020) relate to "(1) cybersecurity is deemed to be a secondary task in most automotive business models and (2) although device manufacturers build components and systems based on the technical requirements and performance criteria of OEMs, they often have to make design choices without OEM input".

be resolved by patching". In addition, there might be typical *business model dynamics* at play where cyber security might not always be a top priority in contrast to vehicle (functional!) safety which traditionally has been a priority. As the margins on CAVs are quite thin in a very competitive market, OEMs will not invest more in cyber security than strictly needed or enforced. In addition, the *network effect* implies that an investment in security will only be perceived by the OEM as valuable if all other value chain players are acting the same way. This might work out paralyzing, where all OEMs are looking at each other. Another related issue is *intellectual property* where the OEMs are having their legitimate trade secrets (OEM intellectual property). Confidentiality, however, does not go along with full transparency which might be needed to increase public acceptance; this might be a difficult balancing act. For reasons of intellectual property, OEMs mostly provide CAVs without the source code. This could make pursuing modifications for security reasons more difficult (Scalas & Giacinto, 2019). Another unsolved issue leading to uncertainty to all stakeholders involved is the *distribution of liability for incidents* since the traditional allocation of liabilities does not work for CAVs. The more autonomous the CAV, the more the liability is expected to shift to OEM as incidents can be considered as matters of product safety or efficacy (Taeihagh & Lim, 2019). Currently, there is no clear legal framework on the distribution of liability between the CAV driver and the parties responsible for the CAV systems: OEMs, suppliers, infrastructure operators, software providers etc. (Taeihagh & Lim, 2019). A few countries are allowing the introduction of CAVs under a traditional scheme of strict liability of the keeper or owner of the vehicle, with some exceptions under very strict circumstances. The massive roll-out of CAVs cannot take place under these schemes. Furthermore, cyber insurance has to deal with limited information as the cyber risks connected to CAVs are very much unknown. The insurance industry is

confronted with enormous challenges here (Channon & Marson, 2021). These uncertainties might hamper the introduction of CAVs in the field. The missing comprehensive legal framework, leading to uncertainty for the industry and a lack of concrete minimum security requirements for CAVs admitted to the road, is probably one of the biggest challenges. The industry (Costantino et al., 2022) has tried to issue standards and guidelines containing principles and practices to improve the cyber security of CAVs. Examples of these industry initiatives include (i) Harman International a collection of OEMs collectively conducting cyber security research (Golden, 2019); (ii) the AUTOSAR consortium issuing security specifications to support the design phase (Costantino et al., 2022) and (iii) Auto-ISAC another industry body with the aim of harmonizing cyber security requirements (Golden, 2019).

The supranational body United Nations Economic Commission for Europe (UNECE) WP.29 has issued an important regulation R155 for cyber security of vehicles. R155 is mandatory for national organizations approving vehicles to their roads (Costantino et al., 2022). R155 can be enforced as the Dutch national authorities for admission of vehicles (RDW) will use the R155 framework to decide about type approval and therefore market access to the Dutch road infrastructure. Almost all European countries have adopted R155[14]. Important to realize is that R155's scope is

[14] The CSMS requirements are still high level, as there is a lot of room for different implementations of the CSMS. Furthermore, as the R155 regulation focuses on processes and not on products, the technical or product related solution or implementation is not regulated (Vellinga, 2023). Although the UNECE R155 can be considered as an important step forward by issuing concrete requirements for the CSMS and all processes over the full lifecycle of CAVs and fosters standardization across the member countries, there is still,

addressing OEMs who should develop adequate Cyber Security Management Systems (CSMS). It has also been argued that type-approval legislation is overstretched in various dimensions as it no longer just contains technical requirements but more principle-based requirements (Charlotte Ducuing, 2019) where most responsibility has been put on the OEM, which, in addition, will be also held responsible for product risks after the product has been introduced to the market (Charlotte Ducuing, 2019). Furthermore, a solid CSMS will without doubt be beneficial for addressing cyber security risks, but this does not guarantee that the CAVs will be fully secure (Vellinga, 2022).

In the literature further critical remarks are made about the risk of R155 becoming a box-ticking exercise, where OEMs will focus on compliancy rather than achieving acceptable cyber security and there is a certain risk that the industry might have a tendency to leave some vulnerabilities undocumented (McLachlan et al., 2022). Major hurdle is that an effective *comprehensive legal framework is missing*, where the existing fragmented legal frameworks (Vellinga, 2022) might either lead to uncertainty for all stakeholders and the legislation does not include specific and concrete security requirements for CAVs (Vellinga, 2022).

When looking at various laws and regulations, we get the impression that the cyber security of CAVs has not been adequately dealt with. First, R155 is issuing requirements regarding the cyber security management processes, not on CAV technical detail level. Second, the new EU Cybersecurity Act does not touch upon this as this act

---

however, a lot of freedom for OEMs and other parties to define their technical solutions addressing cyber security (Vellinga, 2022).

contains an exclusion for motor vehicles covered by the EU 2019/2144 which is about type approval requirements building on UNECE R155. Third, the EU NIS 2 directive only scarcely addresses the issue as there are specific responsibilities issued for operators of critical infrastructure. Nor other acts and standards fully solve the issue. The results in incomplete and fragmented legal requirements (Vellinga, 2022). Research (Liu et al., 2020) revealed that most experts would encourage effective legislation related to enforce a structured design and structured framework which results in (i) software being built in line with international standards, (ii) the installation of accreditation and recertification organizations to provide for a thorough review of the cyber security implementation of the CAV while keeping up with new developments. This will prevent (Liu et al., 2020) in their view the automotive industry to become a market for lemons, where the OEMs compete on features easily recognizable by users but fail to provide for effective cyber security solutions. Upcoming legislation based on the security-by-design principle should lead to the liabilities of all parties involved in the supply chain being clarified at one hand and limiting on the other hand the liabilities as otherwise innovations would be hampered (Liu et al., 2020). The user of the CAV should also accept some responsibility for human errors while operating a CAV (Liu et al., 2020).

To make things even more complex, the integration of ML/AI technology can make it even more difficult to attribute legal liability as normally having control is a prerequisite for legal liability. Specific features of ML/AI are undermining the assumptions of the criminal legal concept of negligence (Giannini & Kwik, 2023). Nevertheless, although a robust legal framework is absent, a lot of initiatives are visible. Only in Europe (Benyahya et al., 2022) there is the EU is sponsored Cooperative Connected and Automated Mobility (CAAM) platform which aim to support

experiments with CAVs on public roads with all connectivity. The European Union Agency for Cybersecurity (ENISA) has published multiple reports on the key challenges and requirements for smart cities and cars. A few industry organizations such as the European Automobile Manufacturers Association (ACEA) have issued key principles for cyber security of CAVs. As a concluding remark, the absence of a strict legal framework could be explained by either legislation which are generally lagging technological developments and also countries being hesitant with issuing restrictive legislation as they strive for dominance in new technologies (Taeihagh & Lim, 2019). To illustrate, the US Department of Transportation issued a publication in 2020 called "Ensuring American Leadership in Automated Vehicle Technologies 4.0".

2.1.4 Overview of the challenges

From this overview it will be clear that there are quite some bottlenecks which should be addressed. Apart from all technological challenges, which cannot be underestimated, there are severe bottlenecks on the governance level, as the many factors of influence on this level (intellectual property, supply chain dynamics, security externalities, legal framework) need further consideration by the relevant stakeholders. As one thing is clear, most of the bottlenecks can only be solved through coordinated efforts by more stakeholders together. Take for instance the economic externality issue; the automotive industry will not solve this. The legislator needs to set a clear legal framework for product liability, both for safety and security aspects, thereby addressing the specificities of the automotive supply chain where components are stemming from a broad variety of players. Another example is the liability for incidents; where insurance companies, automotive industry and legislator need to work together on a differentiated liability framework in line with the 6 SAE levels of automation. To bring together all

stakeholders might not be an easy task as there are many conflicting interests, divergent priorities, and balancing acts prevailing.

There might be additional factors in play which could explain the current situation. First, there is difference between safety science and security studies. Traditionally, safety science focusses on unintentional threats (better called: accidents) and protect humans by preventing the accident or reducing the impact of accidents on or to human beings. Security studies, which is mostly studied in social sciences, focus on the intentions or causes of incidents, with a focus on intentional acts (B. van den Berg et al., 2021). In the automotive industry safety science was traditionally high on the agenda, now the industry also has to spend attention to security studies. The bottlenecks as listed before might be the result of an immature marriage between safety science and security studies. There is work to do in this respect: "An integrated perspective on safety and security, which studies hazardous and harmful events and phenomena in the full breadth of their complexity—including the cause of the event, the target that gets harmed, and whether this harm is direct or indirect—would ultimately lead to a richer understanding of the nature of these events and phenomena and the effects they may have on individuals, collectives, societies, nation-states, and the world at large" (B. van den Berg et al., 2021).

Second, there might be quite different perspectives on risk. While traditionally applied Threat Analysis and Risk Assessments in the automotive industry might indicate that risks are limited, the public could have a different perspective. Typically, experts focus on the likelihood of incidents, where the public focus on the consequences of incidents. If the general public after seeing the movie Leave the world behind on Netflix would believe that CAVs are highly dangerous, it might be questionable whether awareness and education could change this belief. Therefore, in addition to

finding comprehensive solutions covering all layers of the 3-layer model, also safety sciences and security studies have to be integrated and the various perspectives on risk need to be addressed.

2.2 Stakeholders in CAVs cybersecurity

In the preceding sections we have identified the cyber security risks connected to the CAVs, the available solutions and the complications or limitations related to the solutions. We concluded that the many issues can only be solved through concerted actions from many stakeholders together. This has also been underlined in the research literature, where from various angles (Khan et al., 2020; C. Lee, 2017; D. Lee & Hess, 2022; Liu et al., 2020; Morris et al., 2020; Pham & Xiong, 2021; Mulligan and Bamberger, 2016; Taeihagh & Lim, 2019; etc.) it was concluded that a multi stakeholder model is needed to improve cyber security in a more structural and coherent way, giving attention to requirements from all layers of the 3-layer cyber security model. Therefore, it is time to focus on the most important stakeholders regarding the development, production, certification, test, operation, use and governance of the CAVs. In our view, regarding CAVs the variety of stakeholders is larger than for traditional vehicles, due to the connectivity with other vehicles, the infrastructure, the cloud and the broader package of services[15] such as operating in Intelligent Transport Systems.

Relevant key stakeholders in our view, based upon an overview of the research literature, are (i) the automotive industry: OEMs and other parties in the supply chain;

[15] CAVs can be operated as a fleet of vehicles which would offer new functionality to owners and/or operators.

(ii) government, legislator and national (type approval/road admission) authorities; (iii) owners and users of CAVs; (iv) other traffic participants such as pedestrians; (v) standardisation bodies such as SAE and ISO, which are issuing policies; (vi) infrastructure operators such as cities operating a VANET of city shuttles or Operators of ITSs; (vii) insurance companies, which are insuring vehicles and traveling.

It should be mentioned that other classifications have been identified in the research literature. Regardless which list of stakeholders one would like to use, it is clear that there are quite a few important stakeholders which should have a say in solving the existing challenges. Some authors (Khan et al., 2023) argue that is essential to develop a Cyber Security Regulatory Framework (CRF) for CAVs to solve the existing technological, legal and social challenges. This CRF should cover important aspects such as privacy, liability, ethical considerations, and cyber security aspects (Khan et al., 2023). In the creation of this CRF, government should have a critical role. Government has a multidimensional role as the entrance of CAVs will impact the infrastructure set-up, layout of cities, legal and liability arrangements, road safety, protection of the environment (less pollution) and last but not least also taxation. Therefore, government's role is multidimensional (Khan et al., 2023). In the research literature 4 distinct stakeholders, each with basic roles, rights and needs has been distinguished (Khan et al., 2023). First, government which is responsible for providing road safety; enabling country and city development; protecting the environment against pollution; protecting consumers / owners; providing a clear and balanced legal framework that deals with liabilities: implementing a CRF based upon research findings and solve issues relate to negative externalities and knowledge asymmetries. Second, CAV owners and drivers being able to use CAVs in a safe and secure way: having legal certainty about liability in case of incidents; having their privacy protected; be able to

build knowledge of CAVs. Third, OEMs/automotive industry which is responsible for producing safe and secure CAVs based on clarity about the minimum cyber security standards that are applicable to them and the other parties in the value chain; including clarity about related topics such as OTAs/patches, intellectual property, and the right to repair. Fourth and last, insurers which are offering insurance services for all types of CAVs, based on a clear legal framework which brings clarity on legal liabilities of the involved parties in case of an incident (Khan et al., 2023).

3. Methodology

The goal of our study was to assess the assess the most severe cyber security issues related to CAVs and the ways to solve them. For this study we will gather expert opinions on the severity, potential solutions and stakeholders involved in the five of the most pressing cyber security challenges of Connected and Autonomous Vehicles (CAVs). It will be explored whether a consensus opinion amongst the participating experts can be found.

3.1. The Delphi method - overview

The Delphi study was used by RAND corporation in the wake of the second world war for making predictions on which technologies would impact mostly modern warfare. Because other research methods were not rendering the desired results this new Delphi study format was developed (Dalkey & Helmer, 1963). In essence a Delphi survey is a structured, iterative, qualitative survey focusing on measuring consensus among a number of experts who are participating on an anonymized basis in the survey (Dalkey & Helmer, 1963; von der Gracht, 2012). First, a Delphi study is a structured qualitative approach to gather expert opinions on a few selected topics. Goal is to reach

consensus by collecting the opinions of these experts on a complex topic on which there is insufficient evidence available.

The first round contains a set of open questions, where the next rounds contain mainly contain closed questions which should be rated by the panel of experts. Second, as already mentioned the Delphi study is an iterative approach consisting of a few rounds led by a facilitator. After each round the facilitator analyses the results, for identification of common themes, which will then form the basis of the questions for the new round. The analysis will be shared as controlled feedback (von der Gracht, 2012) with the participants, which will enable them to review their opinions and views, also based upon the contributions of other experts.

Statistical techniques will be applied to check whether or not consensus have been achieved on one or more of the research questions (von der Gracht, 2012). Although it is also very clear that many different approaches for measuring consensus can be found in practice (von der Gracht, 2012), the Inter Quartile Range is according to Von der Gracht "generally accepted as an objective and rigorous way for determining consensus" (von der Gracht, 2012, p. 1532). Third, there is isolation between the contributions from the participants, as it is very important to ascertain anonymity across the experts. Goal is to collect their open answers, without being steered or influenced by other participants' opinions. The participants therefore will remain anonymous to each other, where only the facilitator will have access to all participants data. Groupthink, hastily conceived opinions and dominance by one or more experts can be prevented by this approach (Dalkey & Helmer, 1963). Fourth, before entering into the panel, the participant has to give (informed) consent to participate in the study.

3.2. The Delphi method - implementation

This study is an operationalisation of the Delphi technique. The Delphi method was appealing as there are quite a few challenges related to cyber security of CAVs, with a lot of research findings but without consensus on the (relative) importance of the various issues and challenges, and also on the ways to solve these issues. For this study a number of experts have been selected which have demonstrated expertise in the field of cyber security of CAVs. After selection of the subject matter experts we obtained informed consent from all the participants to our Delphi study. During each round the participants were requested to review the online consent form which is part of the survey and to explicitly give consent to participate in the survey.

3.3. Participants

Initially around 150 experts were selected, based upon their expertise in, knowledge about and influence on the field of study, ranging from academic publications on cyber security aspects of CAVs, government officials responsible for regulation of CAVs and/or admission of CAVs to public roads, to (technical) experts working on cyber security in the automotive value chain, consultants advising the sector on these topics and the insurance sector. For this study participants were recruited from all continents, although the number of Netherlands based participants is far higher.

More in detail: from the literature review performed, we selected 60 academic researchers on this topic, which all received an invitation. Having (co-)published a scientific article on cyber security of CAVs was used as major selection criterion here. By searching on the internet for cyber security experts working in the automotive industry, we selected management or other staff members holding a relevant position with responsibility for cyber security of CAVs and/or being a recognized expert in this

field. The last category includes speakers on a congress or seminar on this topic. In total we selected about 45 industry representants. By searching for government related publications and websites we identified about 12 government contacts, mainly Netherlands based. In addition, about 5 representants from well-known research institutes were selected.

3.4. First round questionnaire

A literature review formed the basis for the first round with the identification of five of the most challenging cyber security challenges of CAVs related to: (1) Market dynamics and industry incentives, with subfactors (1a) Not accepting cyber security as a top priority while still focusing on functional safety, (1b) Not having enough expertise regarding cybersecurity and/or not sharing it fully, (1c) Underinvesting in cyber security and/or (1d) not fully accepting ownership for cyber security; (2) Comprehensive legal framework, (3) technical limitations, with subfactors (3a) Vulnerabilities related to existing (legacy) technologies, (3b) Constraints in the technologies used, (3c) Longevity of CAVs in the field and/or (3d) Complexity of all technologies being used together; (4) Ambiguity in legal liability and (5) Awareness and education.

For each of these challenges the respondent was requested to (i) Assess its current severity; which means to indicate to what extent the challenge is a problem for achieving cyber security of CAVs on a 5-point ordinal scale in the range between '1' (no effect on cyber security) and '5' (critical effect; cyber security is no longer possible); (ii) Suggest at least three potential measures to solve the issues and (iii) List which stakeholders should be involved in the solutions. For challenges (1) and (3) the severity rating was requested on a more granular level, that of the key contributing factors of these challenges.

In addition, the participants were asked to rate the relative importance of each of the five challenges. Finally, they were also given the opportunity to make additional suggestions.

3.5. Second round questionnaire

The second round basically was composed of three parts: (i) For the challenges where no consensus on their importance for achieving cyber security of CAVs was achieved during round 1, the respondents were asked again to what extent this challenges is problematic for achieving cyber security of CAVs; (ii) Based upon a clustering of all suggestions made during the first round, the participants were asked to rank the importance of the suggestions for each of the five challenges on a five point ordinal rating scale from '1' (not important at all) to '5' (essential); and (iii) To indicate for the stakeholders identified during the 1st round, the importance of their contribution (no role, a contributing or a leading role) in addressing each of the five challenges.

3.6. Data collection and data analysis

Before uploading the questions for the first round to the Qualtrics application we produced an invitation template and an information sheet containing all relevant information of this master thesis research study. After approval by the supervisor, the materials were uploaded to Qualtrics, under the University of Leiden licence. The first relevant question of the online survey in Qualtrics was about informed consent. The participants had to respond positively to this question before they can participate in the study.

On February 23rd 2024, after opening the online survey in Qualtrics, more than 130 emails were sent to the selected individuals. We tried to personalize the invitation

as much as possible. Because we did not know the selected individuals in person, this was to a certain extent a challenge. The invitation was sent from our university email account, with the information sheet containing general information about the online survey as attachment. In the invitation email there was a link to the online survey in Qualtrics.

During the first week when the survey was active only a few responses were collected. On March 1st 2024 a reminder was sent to all invited participants for participation into the survey. This reminder did not result in a major increase of participants. Finally, this approach resulted in 7 experts which participated in the first round of the study. We considered the number of participants at this stage as too low, especially because there is the known risk that some of the participants in the first round of a Delphi study do not participate in further iterations. Therefore, a revised approach was needed as continuing with the initial approach would not result in the required number of participants. Therefore, in consultation with the supervisor, a more network oriented approach was selected. The new approach was based upon the approaching our network, using a snowballing approach, to ask relevant contacts in our network to introduce the survey to the sought relevant experts in their network, with a clear description of the necessary professional role or expertise for qualifying as a participant. This approach proved to be much more successful. A lot of effort has been spent in approaching the network comprising friends, relatives, neighbours, relatives and other people in the network. Social media, especially Linkedin, were used as a selection tool to find relevant subject matter experts. The revised approach finally resulted in having 28 experts participating in the first round of the Delphi study. The majority of the selected experts is based in the Netherlands, the home country of the researcher.

During round 1 of the survey relevant information concerning the participants was gathered: (i) Gender; (ii) Number of years of professional expertise in the cyber security field; (iii) The highest level of education obtained; (iv) the sector where the participant is working in; (v) Whether or not the participant is working in a management position; and the (vi) the size of the organisation where the professional is working. Round 2 participants were basically all the people which were participating in round 1. Of the 28 participants of round 1, 8 participants did not make it for whatever reason to participate in the second round.

Data collection took place in Qualtrics. After closing the first round of the survey the results were exported to SPSS for further analysis. Descriptive statistics including frequency distributions, mean and variances and interquartile distances were calculated with the SPSS package. In addition, all other (text-based) suggestions and comments were gathered in a specific Excel working file; to analyse the answers to identify common themes and to cluster the suggestions accordingly. After finalisation of the first round, all participants were informed about the outcomes (pdf-file; as an attachment) and then invited to voluntarily participate in the second round of the survey. For this goal a second survey in Qualtrics has been set up. Again, the second survey was anonymously distributed to all remaining 28 participants by a link in the invitation email. Also the responses of the second round were analysed with SPSS with descriptive statistics.

3.8 Ethical considerations

All approached participants did not have any private or business relation with the organiser of the survey. The participants have been fully informed on the set-up and the goals of the survey to ensure strict transparency. The participants were approached from

the researcher's university email account, and only by this email account, which is not used for other purposes. The on-line survey started with request for consent. If a participant did not give consent, the survey would no longer be available to this participant. The contact information of the thesis supervisor has been included in the information sheet and the survey, to give the participants the opportunity to discuss potential issues or tensions in case they feel uncomfortable with the survey or the way the survey is conducted. The email addresses of the participants are only available in the email account of the university, which will be closed once the thesis has been finalised. Upon finalisation of the thesis all working documentation, including the email account will be deleted.

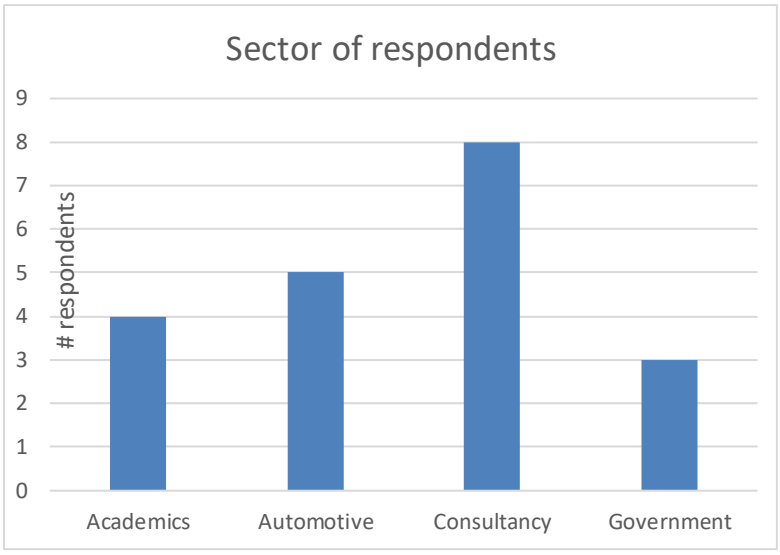
4 Results

The goal of the survey was to consider five important challenges and to explore whether each of these challenges is problematic for achieving cyber security of CAVs. In addition, it was explored which solutions would be valuable in solving the issues.

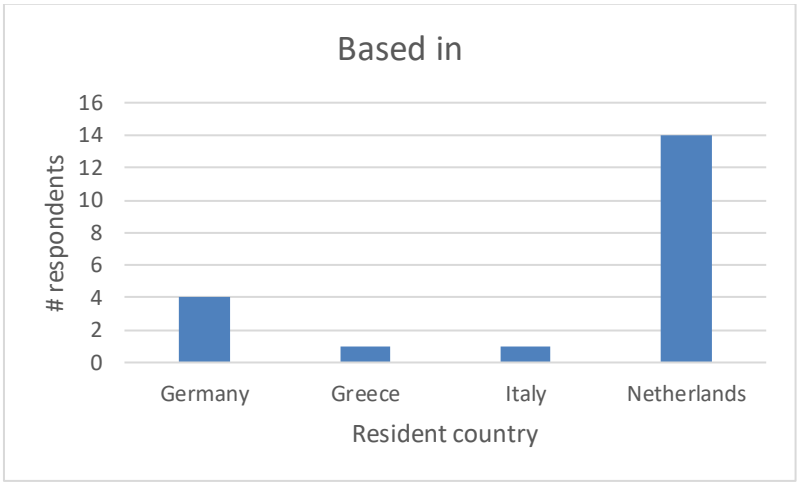
4.1 Description of participants

As mentioned before, a total number of about 150 participants was initially invited to participate in the survey which started on February 23rd, 2024. Finally, after additional invitations 28 eligible respondents participated in the first round which was finished on March 25th. Initially, all 28 respondents were invited to participate in the second round. As there was some attrition, finally 20 respondents concluded the second round which was finished on April 26th, 2024.

A further breakdown of the participants by background is provided below.



Another breakdown can be made of the participants regarding the country where they are professionally active.



As the majority of respondents is based in the Netherlands, there could be a representativeness issue. On the other hand, we do not have indications that the strong Netherlands overrepresentation would distort the results due to Netherlands specifics issues or topics.

4.2 Outcomes of the first round

During Round 1 the participants were asked to consider each of the five challenges, to indicate to what extent this challenge is problematic for achieving cyber security of

CAVs and to suggest a few measures to address the respective challenge. For a few challenges, participants were also asked to indicate which of the listed factors are contributing the most to this challenge. Finally, the participants were asked to rank the five challenges from least important to most important.

The responses and ratings indicate that out of the total number of five challenges, three challenges are considered as the most severe ones by the respondents: 'Market dynamics and industry incentives' (challenge 1); closely followed by 'Technological limitations' (challenge 3); and at a small distance the 'Comprehensive legal framework' (challenge 2). The other 2 challenges generally score lower in their importance according to you. This suggests that the priorities should be on solving the first three cyber security challenges according to the respondents.

Ranking of the challenges	**Importance**						**N**
	1	**2**	**3**	**4**	**5**	**Mean**	
Challenge 1 - Market dynamics and industry incentives	9	7	8	3	1	2,29	28
Challenge 2 - Comprehensive legal framework	7	9	4	5	3	2,57	28
Challenge 3 - Technological	10	6	5	6	1	2,36	28
Challenge 4 - Legal liability	2	5	5	8	8	3,54	28
Challenge 5 - Awareness and education	0	1	6	6	15	4,25	28

Challenge 1, market dynamics and industry incentives, has been ranked by the respondents as the most important one under all the described challenges.

Challenge 1: market dynamics and industry incentives. **Overview responses (n=28)**	**1- Effect not noticable, No effect on cyber security**	**2 - Minor effect**	**3- Moderate effect**	**4 - Major effect**	**5 - Critical effect, cyber security not possible**	**Total**	**Mean**	**IQR**
Not accepting cyber security as a top priority	1	3	7	14	3	28	3,54	1,00

while still focusing on functional safety - 1a								
Not having enough expertise regarding cyber security and/or not sharing it fully - 1b	0	3	3	12	10	28	4,04	1,00
Underinvesting in cyber security - 1c	1	4	8	9	6	28	3,54	1,00
Not (fully) accepting ownership for cyber security - 1d	1	4	4	13	6	28	3,68	1,00

Regarding challenge 1 the participants rate “not having enough expertise regarding cybersecurity and/or not sharing it fully” (1b), immediately followed by “not (fully) accepting ownership for cybersecurity” (1d) as having the most important effects on cybersecurity. It has to be said however that although these two factors scored highest, the differences to the scores of both remaining factors is not that high. This means that the other two factors, “not accepting cyber security as a top priority while still focusing on functional safety” (1a) and “Underinvesting in cyber security” (1c) should not be abandoned too soon.

The statistical analysis showed that for challenge 1 there is consensus under the participants (as the Inter Quartile Range or IQR, a generally accepted measure for the spread of a distribution, is not higher than 1). Therefore, no further iterations are necessary. Related to this challenge a huge number of recommendations has been made by the participants. For our study we clustered the recommendations to common themes. The most important theme-wise recommendations were: (i) Increase the awareness in automotive industry; invest in training and education programs of

engineers and other levels (architect, software suppliers etc); (ii) Create platforms and/or expertise centres like Auto-ISAC for knowledge /best practices sharing among industry, software suppliers, cybersecurity experts, and government. Foster transparency on incidents like the airline industry is doing; (iii) Implement regulatory measures or industry standards, including minimum requirements (baselines) for the industry and let the industry be certified for meeting the regulatory requirements; (iv) Work on enforcement of the cybersecurity regulations and standards; make the industry liable for deviations; (v) Integrate both security and safety requirements in the design phase; (vi) Establish standardized security assessments and external security reviews by specialized (certification) agencies eventually combined with market surveillance by authorities; and (vii) Create and/or enforce transparency on cyber security risks, this should be part of the regular disclosure of the industry.

Some other responses include: (viii) Work on enforcement of the regulation; (ix) Integrate cyber security in the design phase, (x) Engage in thorough testing and certification, (xi) Invest in cyber security knowledge at C-level in the automotive industry and (xii) Thrive for more innovation and investments in cyber security.

According to the participants (mainly) the automotive industry and (also) government are the most relevant stakeholders for challenge 1. A few times certification bodies, standardization organisations (ISO) and approval/admission authorities are also mentioned as relevant stakeholders.

Challenge 2, the comprehensive legal framework, has been ranked by the respondents as the third most relevant challenge, very close to the most important two challenges. This means that this challenge is definitely a relevant challenge to consider for this study.

Challenge 2: Comprehensive legal framework Overview responses (n=28)	1- Effect not noticable, No effect on cyber security	2 - Minor effect	3- Moderate effect	4 - Major effect	5 - Critical effect, cyber security not possible	Total	Mean	IQR
A missing comprehensive framework	2	2	3	13	8	28	3,82	1,75

The statistical analysis showed that for challenge 2 there has not been reached consensus under the participants (IQR = 1,75). Therefore, this question had to be repeated in the second round. The issued recommendations were broadly categorized into mainly four types of actions: (i) Work on a more comprehensive, standardized, harmonized legal framework including AI legislation; (ii) Not issuing new regulation, as there is already a lot available, time should be taken to implement the legislation and build experience; (iii) Work on collaboration in the industry by setting minimum standards and issuing benchmarks, create expertise centers in the industry, engage together in a structured dialogue with government on legislation and work on a collective liability scheme; and (iv) Issue new regulation also incorporating among others AI and remote update schemes.

Although less often mentioned, there were very interesting suggestions on: (v) Solving the balancing act between issuing regulation specific enough to be executable and measurable while also allowing for adaptation and change, being not overly technology specific. A related suggestion was that regulations should not be based upon detailed measures but on security objectives on a higher level; (vi) Invest in training and education in the automotive industry but also public awareness campaigns to educate customers on the importance of cyber security in CAVs; (vii) Enforcing the existing

legislation; (viii) Improve the cyber security algorithms, and infrastructure; (ix) Doing thorough evaluation and certifications; and (x) Introduce digital crash tests.

In contrary to challenge 1, now participants rate (mainly) government together with the automotive industry as the most relevant stakeholders for challenge 2. In a few instances also other stakeholders as mentioned as relevant.

Challenge 3, technological limitations, was ranked as 2nd important challenge, close after the first challenge. From the listed factors "complexity of all technologies being used together" and immediately thereafter "vulnerabilities relating to existing (legacy) technologies" were considered as mostly contributing to this challenge. But the differences with the rankings of the other factors remained small, which suggests that all factors mentioned under the technological related challenges need attention.

Challenge 3: Technological limitations **Overview responses (n=28)**	**1 - Effect not noticable, No effect on cyber security**	**2 - Minor effect**	**3- Moderate effect**	**4 - Major effect**	**5 - Critical effect, cyber security not possible**	**Total**	**Mean**	**IQR**
Vulnerabilities relating to existing (legacy) technologies - 3a	2	2	7	12	5	28	3,57	1,00
Constraints in the technology used - 3b	2	2	11	11	2	28	3,32	1,00
Longevity of CAVs in the field - 3c	2	4	6	13	3	28	3,39	1,00
Complexities of all technologies being used together - 3d	1	2	4	16	5	28	3,79	0,75

The statistical analysis showed that for challenge 3 there is consensus under the participants (IQR <= 1). Therefore, no further iterations are necessary. Participants recommendations could be broadly clustered into mainly four themes: (i) Invest in

lifecycle management, improve maintenance concepts and replacement, addressing vulnerabilities in legacy systems including patch management, doing periodical check-ups on security and over the air upgrades; (ii) Work on standardization and using modular concepts, try to reduce complexity, potentially including working with open-source solutions and/or reusable building blocks (HBOM/SBOM); (iii) Cooperation in the automotive value chain to improve cyber security by investing in expertise sharing, defining uniform solutions and/or through learning from other industries (such as incident sharing in airline industries); and (iv) Issuing legislation to create level playing field, for getting access to critical security modules, putting limitations on outdated technologies and/or to reduce complexity.

Other, less frequent, given recommendations relate to: (v) Improve integration testing, validation and certification, define a uniform and clear verification and testing process, establish test and experiment areas; (vi) Build a security architecture; invest in security by design for CAVs; (vii) Isolate entertainment functions from critical operating functions; and (viii) Work on awareness and education both in the automotive industry as well as for the drivers. For challenge 3, the most relevant stakeholders are first the automotive sector and also to a certain amount government mentioned by the participants.

Challenge 4, ambiguity in legal liability, has been relatively ranked by the participants as less important (place 4 under the 5 challenges) in comparison with challenges 1, 2 and 3. Furthermore, from participants' responses on the importance of this challenge for cyber security of CAVs no consensus is visible, as some respondents considered this topic as not important for realizing cyber security of CAVs while other respondents adhere to a contrarian view.

Challenge 4: Ambiguity in legal liability Overview responses (n=28)	1 - Effect not noticable, No effect on cyber security	2 - Minor effect	3- Moderate effect	4 - Major effect	5 - Critical effect, cyber security not possible	Total	Mean	IQR
Ambiguity in legal liability	6	4	5	8	5	28	3,07	2,00

The statistical analysis showed that for challenge 4 there has not been reached consensus under the participants (IQR = 2,00). Therefore, another iteration was necessary on this topic in the second round. In the recommendations there was also a large variety of suggestions visible. Two key themes most indicated were: (i) Establishment of clear legislation dealing with liability issues (most often mentioned) and (ii) Engage in a collaborative discussion with OEMs, government and users to address the liability aspect. Other suggestions made by participants: (iii) The liability should be put on the OEM side as the car driver cannot be held responsible for the consequences of cyber-attacks; (iv) Car drivers should always be held responsible; (v) Wait until jurisprudence will bring clarity in the liability issues; (vi) Work on the right insurance schemes for cyber security of CAVs, potentially accompanied by a collective guarantee fund for cases where the liability is difficult to assign; (vii) Work on awareness of the driver and train the CAV driver to take over control when needed; (viii) Improving / harmonizing traffic liability regimes on a risk basis rather than on negligence basis; and (ix) Stimulate cross border standardization regarding legislation and liability.

Challenge 5, awareness and education challenges, has been ranked by the participants as the least important, that is place 5 under the 5 challenges. Note that the

scope of this challenge is very specific, it is about the awareness and education of the CAV driver/owner (not in the automotive industry or elsewhere!).

Challenge 5: Awareness and education Overview responses (n=28)	1 - Effect not noticable, No effect on cyber security	2 - Minor effect	3- Moderate effect	4 - Major effect	5 - Critical effect, cyber security not possible	Total	Mean	IQR
Awareness and education	5	11	5	5	2	28	2,57	1,75

The statistical analysis showed that no consensus had been achieved for challenge 5 under the participants, as the IQR is above 1. Therefore, this question has to be repeated in the second round.

Under the suggestions from participants related to this challenge a few common themes were identified: (i) Invest in specific (mandatory) training of drivers, potentially added by virtual training facilities, additional requirements for drivers' licence; (ii) Improve the Human Machine Interface (HMI) to enable timely anticipations and corrections by the driver, requiring visibility of deviance in the cockpit, introducing a kill switch, additional monitoring systems, establish intuitive user interfaces and/or fail-safe systems in case of incidents. Standardization of this HMI is of key importance; (iii) Organize awareness campaigns, educate the drivers, OEMs and other stakeholders; and (iv) Safety and security should be built in features, transparent for the drivers, which should not be burdened with all the details of this.

There were also a few *other recommendations* provided by participants, which were not related to the 5 challenges. The analysis of this category revealed that some common themes were coming back: (1) Invest in awareness for cyber security risks at

both OEMs and consumers. Some interesting suggestions which were not mentioned before include (2) Do not be over optimistic on the prevention of incidents; there will always be breaches, therefore it is important to invest in timely detection, response and recovery and (3) Road infrastructure can be a limiting factor, there are also lots of differences across Europe. Therefore, harmonization is needed in this respect.

Regarding the *stakeholders involved*, the first round revealed a quite rich list of stakeholders, of which two stakeholders mentioned each time very prominently: (i) the automotive supply chain including software suppliers, tech companies and sector institutions and (2) government, as legislator and type approval authority. To a lesser extent certification agencies, standardization bureaus (ISO), academia, consulting and auditing bodies, insurance firms and other bodies were mentioned. Respondents made it also very well clear, that for most of the challenges, with an exemption for the comprehensive legal framework, it should be the automotive value chain which has a key responsibility for finding solutions. The full list of stakeholders, combined with all the suggestions indicating that a collaborative approach is needed involving various stakeholders to deal with the 5 challenges. This cannot be solved by individual parties themselves. A bit surprising outcome was that CAV drivers or representative associations of drivers were rarely mentioned as a relevant stakeholder. The reason for this is unknown. In the second round of the Delphi study the participants will be asked which stakeholders should have a leading or contributing role when dealing with the five challenges.

4.3 Outcomes of the second round

During Round 2 the respondents were asked to basically address 3 questions (1) For the challenges for which during the 1st round no consensus was achieved, the

respondents were asked again to indicate to what extent this challenge is problematic for achieving cyber security of CAVs; (2) To rank the suggestions / recommendations given for each challenge during the first round in order of importance and (3) To indicate for the stakeholders identified during the 1st round, to which extent they should have (no role, a contributing or leading) role in addressing each of the 5 cyber security challenges for CAVs.

Regarding challenges 2, 4 and 5 for which no consensus was achieved during the first round, the respondents were asked again to what extent each of these 3 challenges would be problematic for achieving cyber security of CAVs. For *Challenge 2, Comprehensive legal framework*, which was ranked in the 1st round by the respondents as the third most relevant challenge, very close to the most important two challenges, during the second round consensus has been achieved.

Challenge 2: Comprehensive legal framework **Overview responses (n=20)**	**1 - Effect not noticable, No effect on cyber security**	**2 - Minor effect**	**3- Moderate effect**	**4 - Major effect**	**5 - Critical effect, cyber security not possible**	**Misssing**	**Total**	**Mean**	**IQR**
A missing comprehensive framework	1	1	4	11	2	1	20	3,63	1,00

Although the mean of the scores during the second round (3,63) is – although slightly lower - quite close (3,82) to the mean of the first round, now the IQR (1,0) indicates that consensus has been achieved. No further questions are necessary in this respect. Consensus could unfortunately not be achieved for *challenge 4, ambiguity in legal liabilities*, as the dispersion of the answers remained too big (IQR =1,75):

Challenge 4: Ambiguity in legal liability Overview responses (n=20)	1 - Effect not noticable, No effect on cyber security	2 - Minor effect	3- Moderate effect	4 - Major effect	5 - Critical effect, cyber security not possible		Total	Mean	IQR
Ambiguity in legal liability	0	5	7	7	1	0	20	3,20	1,75

Also for *challenge 5, Awareness and education*, no consensus could be achieved during the second round, as the IQR remained above 1:

Challenge 5: Awareness and education Overview responses (n=20)	1- Effect not noticable, No effect on cyber security	2 - Minor effect	3- Moderate effect	4 - Major effect	5 - Critical effect, cyber security not possible		Total	Mean	IQR
Awareness and education	3	5	6	3	3	0	20	2,90	2,00

From the scores it is clear now that consensus have been achieved for challenge 2 during the second round. During the first round, already consensus has been achieved for challenges 1 and 3. Challenges 4 and 5 are still a bit problematic, as after round 2 still no consensus has been achieved. When assessed in the light of the scoring during round 1 of the relative importance of each of the five challenges, the not reaching of consensus for challenges 4 and 5 do not seem problematic.

Ranking the challenges Overview responses (n=28)	1 - Most important	2	3	4	5 - Least important	Total		Mean
Challenge 1 - market dynamics and industry incentives	9	7	8	3	1	28		2,29

Challenge 2 - comprehensive legal framework	7	9	4	5	3	28		2,57
Challenge 3 - technological	10	6	5	6	1	28		2,36
Challenge 4 - legal liability	2	5	5	8	8	28		3,54
Challenge 5 - awareness and education	0	1	6	6	15	28		4,25

The participant responses indicated clearly that challenges 1, 2 and 3 are considered as the most important. Therefore, the priority should be on solving the first three cyber security challenges according to the respondents. At this stage we conclude that consensus has been achieved among participants on challenges 1, 2 and 3, but not for challenges 4 and 5, which are also the less relevant ones.

The *second part of round 2* focused on asking participants to rank the suggestions, clustered by themes, which were identified during the first round. *Challenge 1, Market dynamics and industry related incentives*, has been ranked by the respondents as the most important one among all the described challenges.

Challenge 1: Market dynamics and industry incentives. **Overview responses (n=20)**	**1 - Not important at all**	**2 - Low impor-tance**	**3-Moderate impor-tance**	**4 - High importance**	**5 - Essential**	**Missing**	**Total**	**Mean**	**IQR**
M1: Create awareness in the automotive industry …	0	2	6	7	5	0	20	3,75	1,75
M2: Create platforms and/or expertise centers …	0	4	1	13	2	0	20	3,65	0,75
M3: Implement regulatory standards …	0	0	2	6	12	0	20	**4,50**	1,00
M4: Work on enforcement	0	1	3	8	8	0	20	**4,15**	1,00
M5: Integrate both safety and security requirements …	0	0	4	5	11	0	20	**4,35**	1,00
M6: Establish standardized security assessments ….	0	1	4	9	6	0	20	4,00	1,75

M7: Create and/or enforce transparency on cyber security risks…	0	1	4	8	7	0	20	4,05	1,75
Total	0	9	24	56	51	0	140		

The respondents ranked three measures for challenge 1 as most important by the respondents which are, in descending importance: (1) M3: Implement regulatory measures or industry standards, including minimum requirements (baselines) for the industry and let the industry be certified for meeting the regulatory requirements; (2) M5: Integrate both security and safety requirements in the design phase; and (3) M4: Work on enforcement of the cybersecurity regulations and standards; make the industry liable for deviations. The IQR for these three measures indicate that there is consensus among the participants in the sample about the importance of these measures to solve challenge 1. As indicated by their means, the other measures are also considered as important by the respondents, although it has to be noticed that according to the IQRs not always consensus was achieved here: (4) M7: Create and/or enforce transparency on cyber security risks, this should be part of the regular disclosure of the industry; (5) M6: Establish standardized security assessments and external security reviews by specialized (certification) agencies eventually combined with market surveillance by authorities; (6) M1: Increase the awareness in automotive industry; invest in training and education programs of engineers and other levels (architect, software suppliers etc.); and (7) M2: Create platforms and/or expertise centers like Auto-ISAC for knowledge /best practices sharing among industry, software suppliers, cybersecurity experts, and government. Foster transparency on incidents like the airline industry is doing. Taking into account that generally the participants consider all these measures as of high relevance, we would recommend that all 7 measures will be adopted by the relevant stakeholders to

improve cyber security of CAVs, where measures M3, M5 and M4 should be short term priority.

Note that *challenge 2, Comprehensive legal framework*, has been ranked by the respondents as the third important, at close distance of challenges 1 and 3. The results of the ranking by the participants of the solutions for this challenge are depicted below.

Challenge 2: Comprehensive legal framework Overview responses (n=20)	1 - Not important at all	2 - Low importance	3- Moderate impor-tance	4 - High importance	5 - Essential	Missing	Total	Mean	IQR
M1: Work on a more comprehensive, standardized, harmonized framework …	0	2	6	7	5	0	20	**3,75**	1,75
M2: Not issuing new regulation …	2	4	4	9	1	0	20	3,15	2,00
M3: Work on collaboration in the industry…	0	1	6	6	7	0	20	**3,95**	2,00
M4: Issue new regulation …	0	4	6	7	3	0	20	3,45	1,00
M5: Solve the balancing act …	0	3	5	7	4	1	20	3,63	1,00
M6: Invest in training and education ….	0	2	7	7	4	0	20	3,65	1,00
M7: Enforcing the existing legislation	0	0	2	8	10	0	20	**4,40**	1,00
M8: Improve the cyber security algorithms and infrastructure	0	3	10	3	4	0	20	3,40	1,00
M9: Doing thorough evaluation and certifications	0	2	7	5	6	0	20	**3,75**	2,00
M10: Introduce digital crash tests	2	2	4	9	3	0	20	3,45	1,00
Total	4	23	57	68	47	1	200		

From the scoring it becomes clear that four measures are ranked as most important by the respondents in order of descending importance: (1) M7: Enforcing the existing legislation; (2) M3: Work on collaboration in the industry by setting minimum standards and issuing benchmarks, create expertise centers in the industry, engage

together in a structured dialogue with government on legislation and work on a collective liability scheme; (3) M1: Work on a more comprehensive, standardized, harmonized legal framework including AI legislation; and (4) M9: Doing thorough evaluation and certifications. Only for M7, considered as the highest relevant measure among respondents, the respondents achieved consensus on the importance, which is between highly important and essential. For the other measures, although generally considered as highly relevant, there was no consensus as indicated by IQR scores larger than 1. This also indicates that the focus for the short term should be on enforcement of the current regulation. There are two other measures considered close to highly relevant, and interestingly enough, although they rank a bit lower in importance, there is consensus among experts on the importance: (5) M6: Invest in training and education in the automotive industry but also public awareness campaigns to educate customers on the importance of cyber security in CAVs, (6) M5: Solving the balancing act between issuing regulation specific enough to be executable and measurable while also allowing for adaptation and change, being not overly technology specific. A related suggestion was that regulations should not be based upon detailed measures but on security objectives on a higher level. The remaining measures score closer to moderate importance and are therefore not considered further.

Challenge 3, technological limitations was considered by the respondents as the second important one under all the described challenges. There was also consensus that solving this challenge was of high importance for improving cyber security of CAVs. The respondents were asked to rate the importance of the themes from round 1:

Challenge 3: Technological limitations. Overview responses (n=20)	1 - Not important at all	2 - Low importance	3- Moderately important	4 - High importance	5 - Essential	Missing	Total	Mean	IQR
M1: Invest in lifecycle management …	1	1	2	9	7	0	20	**4,00**	1,00
M2: Work on standardization and use modular concepts …	0	4	1	13	2	0	20	3,55	1,00
M3: Cooperation in the automotive industry …	0	1	8	4	7	0	20	3,85	2,00
M4: Issuing legislation to create level playing field	0	5	4	8	3	0	20	3,45	1,75
M5: Improve integration testing, validation and certification …	0	2	5	10	3	0	20	3,70	1,00
M6: Build a security architecture ….	0	1	4	10	5	0	20	**3,95**	1,50
M7: Isolate entertainment functions…	1	2	1	9	7	0	20	**3,95**	1,00
M8: Work on awareness and education	0	1	8	9	2	0	20	3,60	1,00
Total	2	17	33	72	36	0	160		

The respondents ranked three measures as most important in order of descending importance: (1) M1: Invest in lifecycle management, improve maintenance concepts and replacement, addressing vulnerabilities in legacy systems including patch management, doing periodical check-ups on security and over the air upgrades; (2) M7: Isolate entertainment functions from critical operating functions; and (3) M6: Build a security architecture; invest in security by design for CAVs. The IQR for the first two measures indicates that there is consensus among the participants in the sample about the importance of (taking) these measures. This is not the case for M6, where there is no consensus achieved. As indicated by their means, the other measures are also considered as important by the respondents, although no consensus was achieved for M3: (4) M3: Cooperation in the automotive value chain to improve cyber security by

investing in expertise sharing, defining uniform solutions and/or through learning from other industries (such as incident sharing in airline industries); (5) M5: Improve integration testing, validation and certification, define a uniform and clear verification and testing process, establish test and experiment areas; (6) M8: Work on awareness and education both in the automotive industry as well as for the drivers; and (7) M2: Work on standardization and using modular concepts, try to reduce complexity, potentially including working with open-source solutions and/or reusable building blocks (HBOM/SBOM). Taking into account that generally the participants consider all measures as of high relevance, we would recommend that all 7 measures will be adopted by the relevant stakeholders to improve cyber security of CAVs, where measures M1 and M7 should be given priority as these are considered as the most important by most of the respondents.

The outcomes for challenges 4 and 5 will be discussed more briefly, as these challenges are both considered by participants as less relevant than the other challenges and the lack of consensus about the relevance of these challenges for achieving cyber security of CAVs. Hereunder the results of the rating by respondents of the measures to solve *challenge 4, Ambiguity in legal liability* are shown.

Challenge 4: Ambiguity in legal liability **Overview responses (n=20)**	**1 - Not important at all**	**2 - Low importance**	**3- Moderately important**	**4 - High importance**	**5 - Essential**	**Missing**	**Total**	**Mean**	**IQR**
M1: Establishment of clear legislation …	1	1	2	8	8	0	20	**4,05**	1,00
M2: Engage in collaborative discussion with OEMs …	2	1	7	6	4	0	20	3,45	1,00
M3: The liability should be put on the OEM side…	3	1	5	4	7	0	20	3,55	1,00
M4: Car drivers should always be held responsible …	5	5	4	4	2	0	20	2,65	2,75

M5: No action needed now …	11	5	3	0	1	0	20	1,75	1,00
M6: Work on right insurance scheme	0	4	4	9	3	0	20	3,55	1,00
M7: Work on awareness and education	1	2	2	6	9	0	20	**4,00**	1,75
M8: Improving / harmonising traffic liability schemes	2	4	5	5	4	0	20	3,25	2,00
M9: Stimulate cross-border standardisation	1	0	6	5	7	1	20	**3,89**	2,00
Total	26	23	38	47	45	1	180		

Three measures are ranked as most important by the respondents in order of descending importance: (1) M1: Establishment of clear legislation dealing with liability issues (most often mentioned); (2) M7: Work on awareness of the driver and train the CAV driver to take over control when needed; and (3) M9: Stimulate cross border standardization regarding legislation and liability. Note that for three of these measures no consensus has been reached across participants on the relative importance of the measures.

For *challenge 5, Awareness and education*, the respondents ranked the measures as stated below.

Challenge 5: Awareness and education **Overview responses (n=20)**	**1 - Not important at all**	**2 - Low importance**	**3- Moderately important**	**4 - High importance**	**5 - Essential**	**Missing**	**Total**	**Mean**	**IQR**
M1: Invest in specific (mandatory) training of drivers …	2	2	7	5	4	0	20	3,35	1,00
M2: Improve the Human Machine Interface …	0	0	5	10	5	0	20	**4,00**	1,50
M3: Organise awareness campaigns ….	1	1	10	7	1	0	20	3,30	1,00
M4: Safety and security should be built in features…	1	1	2	10	6	0	20	3,95	1,00
Total	4	4	24	32	16	0	80		

Two measures have been scored as most important in order of descending importance: (1) M2: Improve the Human Machine Interface (HMI) to enable timely anticipations and corrections by the driver, requiring visibility of deviance in the cockpit, introducing a kill switch, additional monitoring systems, establish intuitive user interfaces and/or fail-safe systems in case of incidents. Standardization of this HMI is of key importance; (2) M4: Safety and security should be built in features, transparent for the drivers, which should not be burdened with all the details of this. Here again the respondents did not achieve (full) consensus for M2, although they did for M4. M2 and M4 are prioritized above investing in (additional) training for CAV users and/or working on awareness and education. This seems that participants give preference to improving the HMI and make safety and security as built-in features transparent to CAV users.

Last topic for round 2 included asking respondents to rank the *importance of contributions by each of the stakeholders* for solving the respective challenges. During the first round, respondents have been asked to specify the stakeholders which should be involved in the solutions to each of the described challenges. Based upon the results of the 1st round, the respondents were asked during the 2nd round to clarify the importance of the contribution per stakeholder to each of the 5 challenges. There were basically three choices: (i) '0' meaning no role for the stakeholder in solving this challenge; or (ii) '1'meaning a relevant contribution for the stakeholder to the challenge or (iii) '2' there is a leading role for the stakeholder for solving the challenge. The table below gives an overview of the results.

Stakeholders involvement: 0 - no involvement necessary 1 - contributing role 2 - leading role Overview responses (n=20)	Automotive value chain	Govern-ment	Acade-mia	CS experts and consul-tants	Standar-disation bodies	Consu-mers	Insu-rance compa-nies	Testing and Certi-fication labs
Challenge 1: Industry dynamics and market incentives	**1x0** **4x1** **15X2**	6x0 10x1 4X2	11x0 8x1 1X2	8x0 10x1 2X2	9x0 8x1 3X2	10x0 9x1 1X2	12x0 6x1 2X2	9x0 8x1 3X2
Challenge 2: Comprehensive legal framework	5x0 13x1 2X2	**1x0** **4x1** **15X2**	7x0 9x1 4X2	4x0 11x1 5X2	4x0 11x1 5X2	9x0 10x1 1X2	9x0 8x1 3X2	6x0 12x1 2X2
Challenge 3: Technological limitations	**1x0** **6x1** **13X2**	10x0 7x1 3X2	5x0 10x1 5X2	1x0 14x1 5X2	5x0 10x1 5X2	16x0 3x1 1X2	15x0 5x1 0X2	5x0 8x1 7X2
Challenge 4: Ambiguity in legal liability	5x0 13x1 2X2	**1x0** **5x1** **14X2**	4x0 11x1 5X2	9x0 7x1 4X2	8x0 9x1 3X2	6x0 11x1 3X2	6x0 9x1 5X2	8x0 9x1 3X2
Challenge 5: Awareness and education	6x0 7x1 7X2	4x0 9x1 7X2	3x0 11x1 6X2	5x0 11x1 4X2	10x0 10x1 0X2	3x0 12x1 5X2	7x0 9x1 4X2	13x0 7x1 0X2
Total	0	0	0	0	0	0	0	0

The respondents indicate clearly that the automotive industry and/or government should have the leading roles in solving most of the challenges. The outcomes show that the instructions might not have been clear enough, as it was mentioned in the instruction that for each challenge there could be only one stakeholder having a leading role. The respondents interpreted the instructions slightly differently and often suggest that for specific challenge there can be more stakeholders having a leading role. Therefore, we interpreted the score '2' no longer as the single party having the leading role for solving this challenge, but as having a very relevant role in solving the challenge, which role is at least more important than for roles where the respondents scored a '1'.

For *challenge 1 Market dynamics and industry incentives*; respondents indicate that the automotive industry is the most important contributor to solving this issue. Other, although less important, stakeholders are government; cyber security experts and consultants; standardization bodies and testing and certification labs. There seems to be

quite some logic behind this score, which indicates a leading role for the industry with contributions from other stakeholders. On the other hand, in literature it was argued that the industry cannot solve it themselves, as the incentives and/or externalities are working in another direction. In addition, two of the three most relevant ranked measures (M3: "Implement regulatory measures or industry standards, including minimum requirements for the industry and let the industry be certified for meeting the regulatory requirements", and M4 "work on enforcement") are indicating a leading role for government instead of the automotive industry. The results are contradictory in this respect. Some sort of explanation can be found in respondents suggesting a very relevant (co-leading) role for the other stakeholders, which can be seen as a confirmation that other parties are needed to solve this challenge.

For *challenge 2 Comprehensive legal framework,* government is widely seen as the leading contributor to achieving cyber security, with less important roles for most of the other stakeholders. This is quite clear, without needing additional explanations. The scores are also in line with the ranking of the measures /recommendations.

The outcomes for *challenge 3 Technological limitations* indicate a clear leading role for the automotive industry in solving the technological limitations. The contributing stakeholders do not come as a surprise: academia, cyber security experts and consultants, standardization bodies and testing and certification labs. The leading role for the industry is confirmed by the three most important ranked measures by respondents (M1, M7 and M6). Remarkable, but not surprising, is that the contributing role of the government is considered as very limited by the stakeholders.

For *challenge 4, ambiguity in legal liability*, it might not be a large surprise that the participants consider government as the stakeholder which should have the leading

role. Contributing roles are perceived for the automotive industry; academia; insurance companies and consumers.

Typical enough, for *challenge 5 Awareness and education*, a lot of contributing stakeholders are recognized, without one of them being considered as having the leading role. Taking all challenges together, the automotive industry and government are considered to have the leading role in solving the challenges.

4.3 Summary of outcomes

During round 2 more clarity has been achieved. First for *challenge 2 Comprehensive legal framework* consensus has been achieved during round 2. This means that for the 3 challenges which have been rated as the most important by the respondents, consensus has been achieved. For the remaining two challenges (4 and 5) no consensus could be achieved. Also taken into account that these two challenges were ranked as less important, which is confirmed by the lower severity score, it is clear that these two challenges are less important in the view of the respondents. No further work will be done on these challenges.

For *challenge 1 Market dynamics and industry related incentives* three measures have been rated as highly important to essential (scores are in range 4,15 to 4,50) were '4' means highly important and '5' essential. In addition, the respondents reached consensus on the importance of these three measures. These three key measures are: (1) Implement regulatory measures or industry standards, including minimum requirements (baselines) for the industry and let the industry be certified for meeting the regulatory requirements); (2) Integrate both security and safety requirements in the design phase; and (3) Work on enforcement of the cybersecurity regulations and standards; make the

industry liable for deviations. Therefore, we conclude that no further work needs to be done for challenge 1.

For *challenge 2 Comprehensive legal framework* one measure was scored between highly important and essential: enforcement of the existing legislation. And there was consensus among experts on the importance of this measure. Most other measures score in the range from 3,40-3,95 where '3' stands for 'moderate importance' and '4' for 'highly important'. The conclusion is that only for one measure, e.g. enforcing the existing legislation, consensus could be achieved. The suggestion to work on a more comprehensive, standardised and harmonised legal framework scored close to 'highly important', but unfortunately no consensus could be reached among participants on the importance of this measure.

The respondents rated three measures related to *challenge 3 Technological limitations* as most important: (1) invest in lifecycle management, improve maintenance concepts and replacement, addressing vulnerabilities in legacy systems including patch management, doing periodical check-ups on security and over-the-air upgrades; (2) isolate the entertainment functions from the critical operating functions; and (3) build a security architecture, invest in security by design for CAVs. For the first two measures consensus has been achieved, not for the last one. Therefore, we conclude that this challenge can best be addressed by focusing on the first two measures.

Regarding *the relevant stakeholders* in solving the five challenges the respondents have indicated clearly that the automotive industry should have a leading role in solving challenges 1 ("Market dynamics and industry incentives") and 3 ("Technological limitations") where government is perceived as having a leading role in solving challenges 2 ("Comprehensive legal framework") and 4 ("Ambiguity in legal liability").

For challenge 5 no clarity was brought about which stakeholder should have a leading role. It was also clear that for most challenges a couple of stakeholders were identified which should have a contributing role.

5 Discussion and implications

In this chapter we will present an evaluation of the results of the study, also in the light of the outcomes of the literature study of chapters 1 and 2. Furthermore, the implications and recommendations based on the study are noted with suggestions for further work.

5.1 Discussion

First, we will discuss the *relative importance of the various challenges*. The participants indicated that challenges 1 ('Market dynamics and industry incentives'), 2 ('Comprehensive legal framework') and 3 ('Technological limitations') are the most important challenges to solve. And, which is also relevant, the respondents reached consensus on that these challenges are considered to have a significant and/or major effect on cyber security of CAVs. This was not the case for challenges 4 ('Ambiguity in legal liability') and 5 ('Awareness and education'), these challenges were considered by the respondents as less important than the other challenges. Both challenges are expected to have a moderate effect on cyber security of CAVs although no consensus was achieved on this. In the research literature the focus has been on identifying and exploring cyber security risks of CAVs and charting the potential solutions, not so much on ranking the severity of the various cyber security problems. Previous research did not reveal a distinct order in the relative importance of challenges. This did not come as a total surprise as various academic disciplines are each focusing on a selected field of

activity. It remains therefore unclear why challenges 4 and 5 are considered less relevant by participants. Possible explanations might be that (i) challenge 4 is very specific and is a topic of interest for a very specific discipline of academic researchers; (ii) less research has been done on challenge 5 as the CAVs are still a relative new phenomenon and not that many CAVs are in the field yet; and/or (iii) the experts which did participate in the panel are more involved in challenges 1, 2 and 3. More research is needed to get clarity here.

Second, we will evaluate the solutions to the most importantly rated challenges themselves. In our view, the solutions to the three major challenges are closely related. The presented solutions to the three challenges can be aggregated to four key measures as shown below:

	Description of measures
A	Implement regulatory measures or industry standards, including minimum requirements, let the industry be certified for meeting the requirements
B	Adopting a safety-and-security-by-design approach based on a security architecture, including separation of critical from non-critical functions
C	Enforce the cyber security regulations and standards, punish misconduct
D	Invest in lifecycle management, improve maintenance concepts and replacement, address vulnerabilities with patch management

The first measure A which is about implementing regulatory measures or industry standards, including minimum requirements is in line with current research which indicates that the industry will not accept by themselves their guardian role for cyber security (Kennedy et al., 2019). This solution does also fit with other previous research (Mulligan & Bamberger, 2016, p. 27) which made clear that cyber security as

public good will be underproduced by the market, “ensuring that the automotive industry develops adequately secure systems requires intervention to overcome positive and negative externalities that lead rational entities to underinvest”. Under these circumstances the introduction of binding regulations makes very well sense. Previous research (Costantino et al., 2022; Vellinga, 2022) highlighted that the fragmented legal frameworks do not include coherent, specific and concrete cyber security requirements for CAVs. UNECE R155 is setting requirements on a reasonable high level for the Cyber Security Management System (CSMS) of CAVs, which are by nature more principle-based (Charlotte Ducuing, 2021). Even having a solid CSMS (Charlotte Ducuing, 2021; Vellinga, 2022), as required by UNECE R155 regulation which is binding for type approval in European countries, does not guarantee that the technical implementations in CAVs will achieve full cyber security. Just implementing regulatory measures and industry standards such as UNECE R155 and R156 will therefore not be enough as this gives too much leeway to the industry to define their cyber security solutions, at the risk that both adequate and non-adequate industry implementations might get product-approval (Costantino et al., 2022).

Here the other part of the proposed measure, introduce minimum requirements could be relevant. This could solve the before mentioned issues. This is confirmed by other researchers (Liu et al., 2020) who underline the importance of legal readiness; that is legislation should be established before the massive deployment of CAVs and related infrastructure. In the same research (Liu et al., 2020) the importance of creating a framework in which software is developed in line with international standards and the industry be accredited and certified to these standards. Then the relevant question remains which minimum requirements for cyber security of CAVs need to be implemented. This question has not been answered yet and needs further consideration.

The survey revealed furthermore that, although building a more comprehensive, standardised and consistent legal framework was rated as close to highly important, no consensus was achieved across experts on the importance of this measure. This outcome is not fully in line with the research literature which indicates (Vellinga, 2022) that a comprehensive legal framework is missing.

The third measure (C), work on enforcement and make the industry liable for security deviations might be the essential complement to solve this. This is in line with research done by (Liu et al., 2020) that enforcement will prevent the automotive industry to become a market for lemons failing to provide for effective cyber security solutions. Previous research (Liu et al., 2020) revealed that legislation should strike a balance between a heavily controlled industry and allowing innovation by giving some leeway, where the gap could be closed by insurance. This is another topic, including the role of insurance, which deserves further attention. Other researchers (Taeihagh & Lim, 2019, p. 120) discovered that "the release of cyber security principles reflect the government's intentions to gradually shape AV [Autonomous Vehicles] developments alongside technological progression before making any hasty policy decisions". Another researcher (C. Lee, 2017) arrived at the same conclusion, new robust legislation has to strike a balance between encouraging innovation and protecting customers.

Overseeing existing research, we can conclude that the proposed measures A and C are fully consistent with the existing body of knowledge. These measures have potential to solve the remaining issues on governance level stemming from previous research and described in section 2.1.3.: (1) not accepting cyber security as a top priority while still focusing on functional safety, (2) not having enough expertise

regarding cyber security and/or not sharing it fully; (3) underinvesting in cyber security due to externalities and network effects and (4) not (fully) accepting ownership for cyber security. As concluded by another researcher (Kennedy et al., 2019); the challenges related to market dynamics and industry incentives might lead the industry to think that cyber security for CAVs is someone else's responsibility, a clear intervention from the regulator is needed.

Measure B, integrating security and safety requirements in the design phase, also seems largely consistent with existing research. (Lee, 2017, p. 49) stated that "regulation should aim for a 'preventive medicine' approach by having manufacturers proactively protect a vehicle's onboard system and create mechanism for systems to self-diagnose problems". In this respect, segregation of entertainment functions from critical operating functions should be realised. Other researchers (Khan et al., 2020) are coming to a similar conclusion, the CAV entertainment functions should be segregated from the critical driver functions.

Considering the complexity of the CAV technologies, existing research (Liu et al., 2020) indicates that a higher degree of complexity can result in more errors in the design and development phase of CAVs, which calls for a security-by-design approach. Also from other research (Mulligan & Bamberger, 2016) it was revealed that security should not be an afterthought, and security as a public good should be considered with other important values in the design phase. This research (Mulligan & Bamberger, 2016) contained a case study on electronic voting systems, where important values (privacy, security, usability) were not considered in the design phase. This was the root cause for the failure of the electronic voting systems. Furthermore, measure B could be an answer to issues identified in previous research showing that the automotive industry

is focusing on functional safety and do not consider cyber security as a top priority (Liu et al., 2020), and rather rely on software patches to deal with cyber security weaknesses. This integration is furthermore in line with the second component of the UNECE R155 regulation: securing vehicles by design to mitigate risks across the value chain.

Existing research (Morris et al., 2020) highlighted a lack of cyber security knowledge at OEM level in combination with a lack of knowledge-sharing in the entire chain due to both a lack of trust and/or a high level of competition. This implies that the implementation of measure B should go alongside with measures A and C related to introducing and enforcing legislation. Upcoming stringent legislation might provide a clear incentive for the industry to invest in cyber security and the related expertise. The survey resulted in no clear consensus for other measures related to challenge 2 ('Comprehensive legal framework'). This might not be a major drawback in the current state of play still before the mass deployment of CAVs) and also considering that consensus has been achieved on implementing and enforcing legislation. For now, it might be practical to first implement the proposed measures, build experience, monitor the effects in the field and then take further steps based upon a further assessment.

The last measure, measure D on implementing life-cycle management, improve maintenance concepts and replacement, address vulnerabilities with patch management including OTA-updates, is consistent with existing research. The lifecycle management solution, combined with security and safety by design, could address the issues of hardware limitations, real time constraints, stressful environments, and high level of technological change and innovation. By doing Over-The-Air updates in combination with updating and replacing of important components of CAVs the mentioned issues could be solved. As stated before, the issue of CAV complexity could be solved by

adopting a safety-and-security-by-design approach. Remaining design or implementation errors or other vulnerabilities can be addressed with updates and replacements. Measure D could be considered as an important complement to Measure B; the adoption of the safety-and-security-by-design approach can be very well combined with a modular maintenance concept which is at the basis of the lifecycle approach.

The respondents indicated clearly which *stakeholders should have a leading role or contribute to solving the solution* for each of the challenges. For challenges 1 ('Industry dynamics and market incentives') and 3 ('Technological limitations') the automotive industry should have a leading role, where for challenges 2 ('Comprehensive legal framework') or 4 ('Ambiguity in legal liability') government should have a leading role. As discussed before, in research literature (Golden, n.d.; Kennedy et al., 2019; Khan et al., 2020; Liu et al., 2020; Mulligan & Bamberger, 2016) it is clearly indicated that the automotive industry cannot solve challenge 1 themselves, due to the nature of the issues. The market structure, incentives and externalities do suggest that other parties need to have a major role here. Therefore, it seems contradictory that respondents deem that the automotive industry should have a leading role in solving the first challenge. This contradictory result cannot be fully explained, although there might be a few mitigating factors: (1) For challenge 1, the respondents indicate that other stakeholders such as government, cyber security experts, standardisation bodies and testing and certification labs should make a contribution as well; and (2) By addressing challenge 2 ('Comprehensive legal framework') the automotive industry will be confronted with enforcement of legislation, which will give an incentive to accept ownership of cyber security and thus lead to the industry giving priority to cyber security. So, the challenges are not fully independent themselves. Nor

are the solutions, as we discovered that the solutions to each of the three major challenges are closely related. In essence four measures will address all three key challenges. This might be the key to the solution; by working on these 4 measures all together, as an integrated package, it should be possible to provide solutions to the identified challenges.

5.2 Implications

The study conducted offers a bigger understanding of the main cyber security challenges of CAVs and the solutions to solve them. Implementing regulatory measures or industry standards, including minimum requirements for cyber security, in combination with enforcement, that is keeping the industry liable for misconduct, seems to be a key solution to the perceived challenges. Other important measures to solve the key issues for cyber security of CAVs are adopting a safety-and-security-by-design approach, and implement lifecycle management, improve maintenance concepts and replacement, do patch management including OTA-updates to CAVs. The survey also revealed, as the proposed solutions are closely related and may address often more than one challenge, that it is of key importance to adopt and implement the suggested measures together as one coherent package. This requires a coherent approach where the main stakeholders are working together.

5.3 Limitations and future research

There are various limitations which should be noted. First, the current level of deployment of CAVs is still limited and most of the identified cyber security weaknesses were identified and explored in research settings. Second, the survey did not check whether the respondents had a comparable knowledge and understanding of the current cyber security challenges, whether from a legal, socio-technical or technical

perspective. Furthermore, the final survey participants where mainly NL-based, where a more international perspective could offer additional insights.

One important area for further research could be the respective order of importance of the cyber security challenges. It is not fully clear now why the legal liability issue (challenge 4) and education and awareness of CAV drivers (challenge 5) have been rated as of medium or even low importance. Is this a realistic view based upon deep knowledge by the respondent or the result of underestimation of the relevance of these topics? This should be further investigated.

In addition, further research is needed on the specification of the minimum cyber security requirements for CAVs, which could form the basis for accreditation and certification. This can be quite a challenge due to the big variety of technology, the complexity of the technology and the innovations and dynamics in the sector. Another topic for further research is how to strike a balance between implementing strict regulation and allowing flexibility to leave room for innovations, also in connection with the way how insurance could fill this gap.

6 Conclusions.

This study focused on the key cyber security challenges for CAVs and the avenues for solutions. Goal was to explore the actions and/or measures which should be taken by relevant stakeholders to improve the cyber security of CAVs. During the desk research phase, we identified five key cyber security challenges for CAVs based on an analysis of existing research literature. From the Delphi study conducted it was clear that challenges related to ‘market dynamics and industry incentives’ (challenge 1), ‘comprehensive legal framework’ (challenge 2) and ‘technological limitations’ (challenge 3) are considered as the most relevant challenges with a (potential) large

impact on the cyber security of CAVs. The participants in the Delphi study reached consensus on the importance of implementing the following solutions (i) implementing regulations including minimum security requirements, (ii) enforcing these regulations and (iii) adopting a security-by-design approach; and (iv) implement life-cycle management, including modular maintenance and patch management. Interesting enough, most of these solutions address more than one challenge and should be therefore implemented together as a package. Key stakeholders to accomplish the desired solutions are government and the automotive industry. The findings are in line with existing research. One of the biggest challenges will be to establish a comprehensive legal framework, including specific minimum cyber security requirements, most desirable on a global basis, which also allows for future innovation. This can be quite a balancing act. But this could be a very worthwhile step to take, before the mass deployment of CAVs. To update one of Arnold Schwarzenegger's famous quotes out of Terminator 3, instead of articulating that 'we need a new vehicle' we should say 'we need a safe and secure CAV' which meets the minimum cyber security requirements.

7 Bibliography

Aliebrahimi, S., & Miller, E. E. (2023). Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles. Source: Transportation Research Part F: Traffic Psychology and Behaviour, 96, 82–91. https://doi.org/10.1016/j.trf.2023.06.010

Benyahya, M., Collen, A., Kechagia, S., & Nijdam, N. A. (2022). Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. Source: Computers and Security, 122. https://doi.org/10.1016/j.cose.2022.102904

Bozdal, M., Samie, M., Aslam, S., & Jennions, I. (2020). Evaluation of can bus security challenges. In: Sensors (Switzerland) (Vol. 20, Issue 8). MDPI AG. https://doi.org/10.3390/s20082364

Burkacky, O., Deichmann, J., Doll, G., & Knochenhauer, C. (2018). Rethinking car software and electronics architecture, McKinsey publication.

Channon, M., & Marson, J. (2021). THE liability for cybersecurity breaches of connected and autonomous vehicles. Source: Computer Law and Security Review, 43. https://doi.org/10.1016/j.clsr.2021.105628

Chapman, A. (2017). GPS spoofing. Tufts Senior Project Handbook.

Charlotte Ducuing. (2021). Towards an obligation to secure CAVs in design. Source: Security and Law, Chapter 8, Cambridge University Press.

Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434. Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022, 340–347. https://doi.org/10.1109/EuroSPW55150.2022.00041

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the Delphi Method to the Use of Experts. Source: Management Science (Vol. 9, Issue 3). https://www.jstor.org/stable/2627117

Deng, X., Wang, L., Gui, J., Jiang, P., Chen, X., Zeng, F., & Wan, S. (2023). A review of 6G autonomous intelligent transportation systems: Mechanisms, applications and challenges. Source: Journal of Systems Architecture (Vol. 142). Elsevier B.V. https://doi.org/10.1016/j.sysarc.2023.102929

Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., Zhang, Y., Deng, Y., Wen, S., Zhang, J., Xiang, Y., & Yu, S. (2019). An Overview of Attacks and Defences on Intelligent Connected Vehicles. http://arxiv.org/abs/1907.07455

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. In: Vehicular Communications (Vol. 23). Elsevier Inc. https://doi.org/10.1016/j.vehcom.2019.100214

Giannini, A., & Kwik, J. (2023). Negligence Failures and Negligence Fixes. A Comparative Analysis of Criminal Regulation of AI and Autonomous Vehicles. In Criminal Law Forum, 34(1), 43–85. https://doi.org/10.1007/s10609-023-09451-1

Golden, J. (2017). The darkening storm of cyberterrorism: international policy for adaptation for automotive cybersecurity. https://nakedsecurity.sophos.com/2017/08/07/congress-looks-to-take-the-whe

Green, P. (2023). An overview to electronic attack and the jamming classifications. Skyradar Blog.

Kennedy, J., Holt, T., & Cheng, B. (2019). Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. Source: Journal of Crime and Justice, 42(5), 632–645. https://doi.org/10.1080/0735648X.2019.1692425

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Source: Accident Analysis and Prevention, 148. https://doi.org/10.1016/j.aap.2020.105837

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Warren, M. (2023). Cybersecurity regulatory challenges for connected and automated vehicles – State-of-the-art and future directions. Source: Transport Policy. https://doi.org/10.1016/j.tranpol.2023.09.001

Koul, S., & Eydgahi, A. (2020). The impact of social influence, technophobia, and perceived safety on autonomous vehicle technology adoption. In: Periodica Polytechnica Transportation Engineering, 48(2), 133–142. https://doi.org/10.3311/PPtr.11332

Lee, C. (2017). Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars' (2017) 69(1) Federal Communications

Law Journal 25 MLA 9th ed. Lee, Chasel. In Federal Communications Law Journal (Vol. 69, Issue 1). https://heinonline.org/HOL/License

Lee, D., & Hess, D. J. (2022). Public concerns and connected and automated vehicles: safety, privacy, and data security. In Humanities and Social Sciences Communications, 9(1). https://doi.org/10.1057/s41599-022-01110-x

Linkov, V., Zámecník, P., Havlícková, D., & Pai, C. W. (2019). Human factors in the cybersecurity of autonomous vehicles: Trends in current research. In Frontiers in Psychology (Vol. 10, Issue MAY). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2019.00995

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. In Transportation Research Part F: Traffic Psychology and Behaviour, 75, 66–86. https://doi.org/10.1016/j.trf.2020.09.019

Macher, G., Schmittner, C., Veledar, O., & Brenner, E. (2020). ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12235 LNCS, 123–135. https://doi.org/10.1007/978-3-030-55583-2_9

McLachlan, S., Schafer, B., Dube, K., Kyrimi, E., & Fenton, N. (2022). Tempting the Fate of the furious: cyber security and autonomous cars. In International Review of Law, Computers and Technology, 36(2), 181–201. https://doi.org/10.1080/13600869.2022.2060466

Morris, D., Madzudzo, G., & Garcia-Perez, A. (2020). Cybersecurity threats in the auto industry: Tensions in the knowledge environment. In Technological Forecasting and Social Change, 157. https://doi.org/10.1016/j.techfore.2020.120102

Mulligan, D., & Bamberger, K. (2016). Public Values, Private Infrastructure and the Internet of Things. Journal of Law & Public Regulation.

Nikitas, A., Michalakopoulou, K., Njoya, E. T., & Karampatzakis, D. (2020). Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility era. Sustainability (Switzerland), 12(7), 1–19. https://doi.org/10.3390/su12072789

Pham, M., & Xiong, K. (2021). A survey on security attacks and defense techniques for connected and autonomous vehicles. In Computers and Security (Vol. 109). Elsevier Ltd. https://doi.org/10.1016/j.cose.2021.102269

Scalas, M., & Giacinto, G. (2019). Automotive Cybersecurity: Foundations for Next-Generation Vehicles. http://arxiv.org/abs/1910.01037

Schwarz, C., Gaspar, J., Miller, T., & Yousefian, R. (2019). The detection of drowsiness using a driver monitoring system. In Traffic Injury Prevention, 20(sup1), S157–S161. https://doi.org/10.1080/15389588.2019.1622005

Seuwou, P., Banissi, E., & Ubakanma, G. (n.d.). The Future of Mobility with Connected and Autonomous Vehicles in Smart Cities. www.trucks.com

Sun, X., Yu, F. R., & Zhang, P. (2022). A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). In IEEE Transactions on Intelligent Transportation Systems, 23(7), 6240–6259. https://doi.org/10.1109/TITS.2021.3085297

Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. In Transport Reviews, 39(1), 103–128. https://doi.org/10.1080/01441647.2018.1494640

Thapa and Fernandez: A survey of reference architectures for autonomous cars (2020) Proceedings of the 27th Conference on Pattern Languages of Programs. The Hillside Group.

B. Van den Berg, Prins, R., & Kuipers, S. (2021). Assessing Contemporary Crises: Aligning Safety Science and Security Studies. In Oxford Research Encyclopedia of Politics. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1733

Van Den Berg, J. (n.d.). A Basic Set of Mental Models for Understanding and Dealing with the CyberSecurity Challenges of Today. https://www.jinfowar.com/journal/volume-19-issue-1/basic-set-mental-models-understanding-dealing-

Vellinga, N. E. (2022). Connected and vulnerable: cybersecurity in vehicles. In International Review of Law, Computers and Technology, 36(2), 161–180. https://doi.org/10.1080/13600869.2022.2060472

von der Gracht, H. A. (2012). Consensus measurement in Delphi studies. Review and implications for future quality assurance. In Technological Forecasting and Social Change, 79(8), 1525–1536. https://doi.org/10.1016/j.techfore.2012.04.013

Appendix 1 : Technologies supporting CAVs

Basically, there following kinds of technology are enabling CAVs (Benyahya et al., 2022):

(1) In-vehicle sensors:

a) (Differential) Global Positioning System (GPS): able to locate the geographical position of CAVs making use of satellite technology.
b) Light Detection and Ranging (LiDAR, Light Detection And Ranging of Laser Imaging Detection): for measuring the distance to another object laser is used, where the LiDAR laser calculates the distance to another object by measuring the time interval between the CAV issuing the laser and the time of receiving the reflection.
c) Radio Detection and Ranging (RADAR): In contrast with LiDAR now electromagnetic waves are issued and the distance to another object is measured by the elapsed time between issuance and receiving the reflection.
d) Acoustic (ultrasonic) sensors, cameras: It is expected that CAVs of the future will have acoustic sensors to be able to hear external noises.
e) Tyre Pressure Monitoring Systems (TPMS): The pressure monitoring sensors within each tire are monitoring and reporting the specific pressure levels in real time.
f) Odometric systems: The odometric sensor is estimating the change in position over time of a vehicle based on data from its own sensors.

(2) In-vehicle connectivity-based solutions (mostly wired), based on ECUs, where ECU communications can be serviced by

a) CAN (Controller Area Network): the backbone communication circuit of vehicle, connecting all microprocessors and ECUs of a vehicle, each capable of controlling a specific function. The CAN-bus serial protocol has been invented in the 1980s by the company Robert Bosch.
b) Local Interconnect Network (LIN), a sort of master-slave protocol by which various devices can communicate with each other over a serial bus network.
c) Media-Oriented System Transport (MOST): a specific network topology by which in-vehicle media systems can communicate with each other.
d) FlexRay: the FlexRay communications bus is a deterministic, fault-tolerant and high-speed bus system developed in conjunction with automobile manufacturers

and leading suppliers. FlexRay delivers the error tolerance and time-determinism performance requirements for x-by-wire applications16

e) Ethernet messaging services: ethernet network for communications between in-vehicle devices

(3) Additional physical ports such as

a) On-Board Diagnostic System (OBD-II): specific port to which a person can connect to extract diagnostic information related to the vehicle's specific functions. Malfunctions or problems can be revealed
b) USB-ports: a USB-port connection to enable connected external devices to a vehicle
c) electronic charging ports: ports for charging external devices

(4) Infotainment systems: systems within a vehicle with the ability to provide information and entertainment services

(5) Inter-vehicle communications systems to provide for V2V, V2I, V2N or V2E (mostly wireless)

a) Channels: Radio (AM, FM, DAB, RFID), Bluetooth, Cellular (4G/5G), bidirectional communication (IEEE 802.11p or Wifi), Dedicated Short Range Communication (DSRC), Wireless Access in Vehicular Environments (WAVE) and in some cases IoT networks (IEEE 802.15.4, ZigBee). Wireless communications enable creating VANETs (Vehicular Ad-hoc Networks): they all have the ability to connect the CAV with its environment
b) V2V, mainly DSRC17 and Wifi

---

[16] https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/flexray-automotive-communication-bus-overview.html

[17] Techtarget: "is a wireless communication technology designed to allow automobiles in the intelligent transportation system (ITS) to communicate with other automobiles or infrastructure technology". https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/flexray-automotive-communication-bus-overview.html

d) V2I, with data exchange between On Board Unit (OBU) and Road Side Unit (RSU): these are the building blocks of VANETs the OBU and RSU communicate among each other on a wireless channel
e) V2E, including Vehicle-to-Cloud (V2C) and Vehicle-to-Pedestrian (V2P)

(6) Artificial Intelligence software which can assist in interpreting vast amounts of data gathered by the CAV systems.