Stakeholders' Trust in Automated Driving

Master of Science (Tech) Thesis
University of Turku
Department of Computing
Communication and Cyber Security Engineering
2023
Jesse Järvi

Supervisors:
Antti Hakkala
Seppo Virtanen

UNIVERSITY OF TURKU Department of Computing

Jesse Järvi: Stakeholders' Trust in Automated Driving

Master of Science (Tech) Thesis, 61 p.
Communication and Cyber Security Engineering
October 2023

As automated driving continues to evolve, trust plays a pivotal role in its adoption and acceptance in society. This thesis aims to explore different stakeholders' trust in automated driving systems by examining factors that influence said trust. A questionnaire was developed in order to gather recent data on trust in automated driving systems and it was used to analyze factors that influence trust in automated driving. The questionnaire was also used to identify possible methods that could improve trust.

The questionnaire in this thesis also identifies which types of stakeholders would trust automated driving, for example by examining familiarity. Furthermore, the study addresses the issue of vulnerable road users reasons for distrust in automated driving. Identifying these issues in such fields as ethics, legislation, or safety can lead to enhancement of development strategies, which in turn would enhance stakeholders' trust in automated driving.

This thesis provides valuable insights into the relationship between trust, technology adoption, and user apprehensions on automated driving, with a goal of improving the development considerations in the rapidly evolving transportation technology.

Keywords: trust, automated driving, cybersecurity, trust factors, technology adoption

Contents

1 Introduction **1**

1.1 Research problem 1

1.2 Research objectives 2

1.3 Structure of the thesis 3

2 Trust **5**

2.1 Defining Trust 5

2.1.1 Different elements of trust 6

2.1.2 Repairing trust 8

2.2 Societal pressures 8

2.2.1 Institutions 9

2.2.2 Morals 9

2.2.3 Security 9

2.2.4 Reputation 10

2.3 Trust in IoT 10

2.3.1 Technology acceptance model 12

2.3.2 GDPR 13

3 Automated driving **15**

3.1 Automation 15

3.1.1 Levels of automation 16

3.2 Safety first! . . . 18
3.2.1 Safety . . . 18
3.2.2 Security . . . 21
3.3 Communication technology . . . 28
3.3.1 External communications . . . 29
3.3.2 Internal communications . . . 29
3.4 Issues in automated driving . . . 31
3.4.1 Cybersecurity . . . 31
3.4.2 Technology . . . 34
3.4.3 Legislation . . . 35
3.4.4 Ethical . . . 37

4 Trust in automated driving -questionnaire 39
4.1 Methodology . . . 39
4.1.1 Research design and rationale . . . 39
4.1.2 Development and data collection . . . 40
4.1.3 Data analysis . . . 42

5 Discussion 50
5.1 Interpretation of results . . . 50
5.2 Implications and research questions . . . 54
5.2.1 How do different stakeholders trust automated driving? . . . 54
5.2.2 What are some of the key trust issues related to automated driving? . . . 55
5.2.3 How to increase the trust of different stakeholders in automated driving? . . . 55
5.2.4 Possible difficulties with implementing trust increasing methods in automated driving? . . . 56

5.3 Limitations and future research 57

6 Conclusion **59**

Lähdeluettelo **62**

List of Figures

3.1 SAE levels visualized. Adapted from [16] 16

3.2 Defence in Depth model vizualised. Adapted from [17] 26

3.3 CAN bus depicted. Adapted from [34] 30

3.4 Attack surface of a vehicle. Adapted from [33] 32

4.1 Answers to the 1st question: How do you find the safety of traffic at the moment in your hometown 43

4.2 Answers to the 2nd question: You receive information that automated vehicles are being tested in your neighbourhood, how would you feel? 43

4.3 Answers to the 3rd question: Automated vehicles are safe. 44

4.4 Answers to the 4th question: Automated vehicles as part of regular traffic increases the feeling of safety. 45

4.5 Answers to the 5th question: Automated vehicles improve traffic safety in extraordinary driving circumstances. 45

4.6 Answers to the 6th question: Advantages of automated driving. Choose 3. 47

4.7 Answers to the 7th question: Disadvantages of automated driving. Choose 3 48

4.8 Answers to the 8th question: What would make you trust automated driving more? Choose 3 49

List of acronyms

ATM Automatic Teller Machine

CAN Controller Area Network

ECU Electrical Control Units

GDPR General Data Protection Regulation

ICT Information and Communication Technology

IDS Intrusion Detection System

IoT Internet of Things

IT Information Technology

LIDAR Light Detection and Ranging

OBU Onboard Unit

SAE Society of Automotive Engineers

SDL Secure Development Lifecycle

SOTIF Safety of intended functionality

TAM Technical Adoption Model

UTAUT Unified Theory of Acceptance and Use of Technology

V2X Vehicle to X communication

VANET Vehicular Ad Hoc Network

1 Introduction

Automated driving has been a relevant topic for controversies and research in recent years. Recent advancements in the fields of Artificial Intelligence and Machine Learning have laid the groundwork for automated driving to thrive. The potential with automated driving is immense, and it would allow for example possibly improved environmental effects from traffic, improve comfort while driving, and improved safety in traffic. Operating through sensing their environments from different sources, automated vehicles could make traffic far more efficient and safe. However, successfully integrating automated driving does not only depend on their technical capabilities, but also on the fundamental human factor of trust.

Trust plays a very crucial role in the acceptance and adoption of new technologies. Overall technology adaptation becomes far more difficult if there is no trust in the technology's ability to make correct decisions and respond appropriately and various scenarios as an example. As vehicles equipped with automated systems begin to share the road with human-driven vehicles, understanding how trust is formed, maintained, and potentially eroded in this dynamic environment becomes extremely important.

1.1 Research problem

Trust is something that doesn't just happen for no reason and without trust, technology adaptation becomes nearly impossible and could possibly hinder the devel-

opment of automated vehicles further. In order to avoid this, steps must be taken to improve stakeholders' trust in automated driving.

There are many different factors that influence trust in automated driving. As an example, as automated driving is still a developing technology, legal considerations and unfamiliarity with technology are a prevalent problem in forming trust in automated driving. Legal issues already surrounding privacy and new technologies in general are not improving trust in automated driving. Legislation and different standards are important for the safety and security of the users, as well as the performance consistency of the product. Legislation and unfamiliarity surrounding new technologies are just a few of the problems in creating and upholding trust in automated driving.

Trust is something that one build over a long period of time. Long-term adaptation of technology involves a strong trust relationship that needs plenty of positive interactions, while keeping the anomalies of vehicle behavior to a minimum.

Developing automated vehicles requires plenty of resources. However, more often than not when implementing new technologies as complicated as automated vehicles, it is not an easy process. Resources can run out, there may not be enough resources to be allocated to certain fields, or there aren't available experts to deal with certain issues, and new issues may arise.

1.2 Research objectives

Based on the problems mentioned in 1.1, research objectives and methods used are formed as follows:

- O1: How do different stakeholders view automated driving?

  A questionnaire will be used as the primary research method.

- O2: What are the reasons behind some of the key trust issues related to automated driving?

  A questionnaire and literature review will be used as research methods.

- O3: How to increase the trust of different stakeholders in automated driving?

  A questionnaire and literature review will be used as research methods.

- O4: Are there possible difficulties with implementing trust increasing methods in automated driving?

  A questionnaire and literature review will be used as research methods.

1.3 Structure of the thesis

The thesis is structured so that this chapter introduces the problem, background, and motivation. The next chapter 2 defines, and examines trust. Different forms of trust are explained, and relevant aspects in the scope of this thesis are covered. Trust in different technologies and technology adaptation are also covered in this chapter.

In the third chapter 3, automated driving is discussed. Technical backgrounds on automated driving are provided, and also technologies and communication tools used in automated driving are introduced. Potential threat landscape in automated vehicles is introduced, a few relevant cyber-attacks are discussed in more detail.

In the fourth chapter 4 the thesis advances to discussing the actual research conducted to in making this thesis. A questionnaire was conducted, background and rationale are covered, as well as results are shortly presented in this chapter.

In the fifth chapter 5 we discuss the results of the questionnaire in more detail, we also compare our results with previously conducted research on the subject. Future directions and conclusions are provided in this chapter, as well as limitations for the

study.

And finally we reach the conclusion 6, which entails the results of this thesis in a brief summary. The level of fulfilment of the research objectives are also included in this chapter.

2 Trust

The concept of trust is the foundation of this thesis. Trust is what drives us to decisions and cooperation with different entities. This chapter aims to define trust in a sense that is relevant to the thesis, and explore some factors that affect trust, define different elements related to trust, and describe what trust means when it comes to an IoT environment. In chapter 2.1. a relevant definition and background of trust is presented, as well as the more negative versions of trust, such as distrust are introduced and defined. Forced trust as a concept in addition to trust repair are also covered in this subchapter. In chapter 2.2 the social pressures that enforce trust in different entities are defined and introduced. Chapter 2.3 covers trust in IoT environment and introduces a few challenges related to trust in IoT, as well as a technology acceptance model is introduced.

2.1 Defining Trust

Trust can be defined a bit differently depending on the source, but the idea remains similar: you expect something or someone to behave in a certain way expecting a desired result of the interaction, or you place confidence in them. Trust is often viewed differently across different fields, such is IoT for example. Trust is something that society needs in order to function in the state that it has developed to. People need to be able to trust different actors daily, be it a plumber or an ATM. This is simply because if there is no trust in for example any service provided, the world

wouldn't have developed the way it has. [1] [2] [3]

Merriam webster defines trust as: "Assured reliance on the character, ability, strength, or truth of someone or something; one in which confidence is placed." [2]

As previously stated, trust is essential in societies in order for them to function, and with globalisation and the emergence of the Internet, societies and the number of actors one has interactions with has increased many times over. This means that trust is more and more placed in security measures over the Internet for example, rather than having to verify everything and everyone yourself. Other pressures can also be put in place to predict certain behaviours enforcing trust. However sometimes people defect, meaning that we do not behave in the expected manner in society's eyes for example. Defector is known as the entity doing the defecting. Defecting sounds bad at first, as defection can be as simple as stealing food, or inflicting a massive cyberattack on a hospital's information systems. Defection could however also be viewed as the necessary step in order to create change in a broken system. Justifying defection is in the eye of the beholder. Often when we defect, we believe we are morally in the right, which justifies the defection in our eyes. Defection can sometimes have a more negative impact on reputation, which could lead to different actors not trusting the defector. These elements of trust can be defined as mistrust, distrust or untrust. [1] [3]

2.1.1 Different elements of trust

In addition to trust, Marsh and Dibben have defined three other, more negative, aspects of trust, which are distrust, untrust and mistrust. What if the interactions between the trustor and trustee are involuntary? [4]

Mistrust is a form of a trust encounter where a trustee has not delivered the expected result of the trustor, so the trust the trustor has placed on the trustee has been misplaced, and there for referred to as mistrust. [4]

Mistrust can then turn to untrust. Untrust can also be a result of someone's reputation. When a trustee is untrusted, it is a measure of how little they are trusted. It basically means that the trustor has little faith that the trustee is actually going to act in the expected sense. Untrust can be turned to trust by having positive interaction that increase the trust between the trustor and the trustee, or by implementing common rules or other pressures to work together on a certain dilemma. The line between trust and untrust is referred to as the cooperation threshold. Distrust means that the trustor believes that the trustee will actively work against or sabotage the expected goal for the interaction. This level of negative trust is harder to turn to trust or untrust. That does not mean that distrust would not be important in certain situations. It helps to be paranoid by default in some cases, it is useful to spot out actors that are not working in your favour or for the common good and place expected distrust on their action until proven wrong. [5] [4]

Then there is also the concept of forced trust, because not every situation is about voluntarily trusting another actor. Forced trust is introduced in situations where a user is basically forced to trust an entity, or an information system for example, in order to complete transactions or tasks. The user in these cases has no right of choice to trust, but is forced to trust the entity. In the paper by Hakkala et. Al. the examples on forced trust and its implications are for example viewed through critical governmental information systems. The model then presented includes different types of trust between different actors in the information system. This then enforces that not every single entity and user can be trusted, so some form of forced trust is necessary for the system to remain functional. [6]

2.1.2 Repairing trust

As we previously discussed the effects and classifications for mistrust, untrust and distrust, there is also a way to negate some of their effects. Repairing trust can be a long process, or it can be unachievable given the circumstances of the severity of distrust or mistrust. All in all, repairing ones trust in someone else, or ones reputation, takes time because the trust broken needs to be slowly rebuilt. There are alternative methods to trusting in order to complete transactions among trustees, such as establishing evaluation procedures that can be agreed upon or creating an agreed upon set of rules for the transaction.[1] [7]

2.2 Societal pressures

Societal pressures are basically put in place to enforce societies' interests and norms, while attempting to minimize defection regarding personal interest. Defection in this case is defined similarly to Bruce Schneiders Liars and outliers, and it's basically something not operating under group norms, for example if the group norm is to not steal food, then a defector is someone who does steal food. Motivations for defection can vary as people have complicated motives for doing things, especially when defecting. You could be stealing food to feed your starving infant for example. It is then a matter of the morals of others to decide whether you are right to steal food or not. Societal pressure are put into place to minimize defection, and they do it in a variety of different ways. You could for example increase the difficulty of defecting, reduce the benefits of defecting or increase the benefits of not defecting. Different kinds of societal pressures work on different sizes of groups and societies and these societal pressures are institutional pressures, moral pressures, reputational pressures, and security related pressures. [1]

2.2.1 Institutions

Institutional pressures work best in larger communities and societies. Institutional pressure means that you have an agreed upon set of rules or laws that most people follow, and defection, if caught, leads to a relevant punishment. This is done in order to induce cooperation among people that may or may not know each other in anyway, but the still belong to a certain group, so they would have to follow similar general rules. Institutional pressures help us predict a certain level of behaviour so that we can trust people around us. Speed limits and laws in a society can be viewed as an example of institutional pressures. [1]

2.2.2 Morals

Moral pressures work best in small communities, where most people know each other. Morals are basically the voice telling you that something you are thinking about doing is wrong, not because it has been made difficult or the punishment is severe, but because you believe it to be wrong. People also hate feeling guilty, so morals prevent you from defecting if you believe it to be for a wrong reason. [1]

2.2.3 Security

Security systems work for groups of all sizes, security is not necessarily size related. Security systems are ways of making defection more difficult than it already is, they work as preventors, or they can work after defection as well as different security mechanisms. Security can be a burglar alarm also, which is an example of a security system that is used to prevent, alarm during, and notify after defection. [1]

2.2.4 Reputation

Reputational pressure works best in small to medium sized societies. The better we know people, the better we know their reputation. Reputation is a tool we can use to determine from other people's experiences and their past behaviours if they are trustworthy. If you choose to defect, your reputation among people that know you, will be affected. [1]

2.3 Trust in IoT

Trust in IoT, as previously mentioned, is fairly similar, but also differs a bit as to what it actually entails in itself in comparison to the previous definitions of trust. When it comes to IoT and ICT, trust can be viewed as threefold according to Aldowah et. Al. These three interactions related to trust are user-to-machine, machine-to-machine, and machine-to-user, and this thesis is mostly focused on the trust relationship between a user and a machine. When considering the different interactions within the IoT scope, as well as comparing the scope of IoT with ICT and autonomous driving, we can discover that machine-to-machine communication is the first difficulty, as well as the question that 'what makes a user trust an IoT device?', which is most relevant for this thesis. [8]

Trust is a sum of various things when it comes to an IoT device and its user. Information security plays a rather large role in trust when it comes to IoT and ICT. The three pillars of information security are often a good place to start building trust. These pillars are Integrity, availability, and confidentiality. What they stand for in IoT means that your data should be available to you within a reasonable amount of time, integrity means that data is accurately presented, and it is not altered by unauthorized people and this includes hardware for IoT, and lastly confidentiality means that measures are taken to make sure that unauthorised access attempts

are prevented. Information and cyber security in IoT and especially in automated vehicles is discussed more in later chapters. [9]

Trust comes from a place of a perception that "we are safe", which here includes that information and data about us is properly handled and securely transferred and stored. This also then extends the trust of the IoT device to the IoT network and infrastructure. The network is consisted of different nodes, which could be prone to attack, even if the device wouldn't be. Also, trusting an IoT device means that a user is required to lose some control because the device makes decision in the user's place. [9]

How the IoT device, network or manufacturer handles different kinds of threats and issues is also one of the indicators that trust can be built. As users become knowledgeable or have more experience with the products and their security features, the trust level increases. Users have a need for assurance that they are safe and that the organisations behind the device can provide a necessary amount privacy protection and security is key for trust. [9]

The above-mentioned things may not be too easy to achieve as they might sound on paper. IoT devices are a bit different from the average computer systems, and the network structure can also be built differently, as more connections may be needed. Different difficulties with IoT devices often include for example their complexity as they might have sensors that interact with the real world. Also, IoT has three key issues on hardware limitations: storage capacity, computation power, and energy consumption. These issues are hard to solve in IoT and often require not the ideal solutions to be presented as the used communication technologies for example may not be ideal in speed, but what they lack in speed they make up for in being low in energy consumption for example. So basically, one has to make some sacrifices in order to create viable and cost-effective security and communication methods for many different IoT devices. Some other issues that may arise in IoT include but

are not limited to scalability, infrastructure, lack of laws and regulations and for example identity management. All of the above can have an impact on the building of trust with an IoT device, service or an organisation even. [9] [8]

2.3.1 Technology acceptance model

When it comes to understanding the adoption or acceptance patterns for new technology, it is essential to understand how those patterns are formed to develop technologies further. As this thesis aims to explore the trust in the stakeholders on automated driving, understanding the acceptance of technology is important regarding every single stakeholder. There are relevant models that exist already, the ones this thesis covers are: Technical Adoption Model and Unified Theory of Acceptance and Use of Technology. [10] [11]

The Technical Adoption Model (TAM) has been widely used in different technology adoption studies and it is fairly simplistic. TAM is built around two constructs, which are perceived usefulness and perceived ease of use. What these constructs mean is that the adoption of technology is based on the potential user's perception of the products usefulness in order to do their job, and that the product is easy to use or "free of effort". The perceived usefulness weighing a bit more than perceived ease of use. The Unified Theory of Acceptance and Use of Technology (UTAUT) has however rather overthrown TAM as the leading model for adoption in the fast-changing IT environment. UTAUT is meant to serve as a more comprehensive model compared to the simplicity of TAM. UTAUT has four constructs, which are performance expectancy, effort expectancy, social influence and facilitating conditions. Facilitating conditions means the perception of existing infrastructure supporting the use of the new system. [10] [11]

An example use case for the UTAUT can be found in the research of Koivumäki et. al. in The perceptions towards mobile services: an empirical analysis of the

role of use facilitators. In this study, the perception towards new mobile services was tested using the UTAUT model, and especially the facilitating conditions were concentrated on in the study. What they found was that the time spent using the services did not have an impact on perceptions, so first impressions last according to this case study. Familiarity with the devices however did have an impact, as well as user skills. [10] [11] [12]

2.3.2 GDPR

Then there of course are the issues of privacy, which was already briefly mentioned. Privacy is a thing that people value, so it is important to have support for people's privacy in an IoT product. The way to achieve this is by addressing the previously mentioned lack of laws and regulations. The GDPR is a good example of things moving forward in the EU area, needless to say no rule or regulation is perfect on their own, but the GDPR has become rather an important regulation when it comes to privacy and data protection. [13]

GDPR or "General Data Protection Regulation" was created in 2018 to unify EU's data protection and privacy laws and regulations into one single entity or guideline. The purpose of the GDPR is to ensure the integrity, confidentiality, availability, safety and security of the data of EU citizens, as well as ensuring their privacy. An example of these regulation would be that you have the right to request and know what data an organisation is handling of you, or ask that your personal information be deleted. The organisations have a set of guidelines and requirements which they have to follow and fill in order to be compliant with the GDPR. An example of these would be that an organisation has to be able to present and produce clear information about their data collecting. The GDPR is enforced with penalties, which are mostly large fines dependent on a lot of factors, such as severity, scale, continuity and size of the organisation basically. The largest fine received for

breaking the regulations of the GDPR was issued to Amazon in the amount of 746 million Euros. GDPR is definitely a step in the right direction when it comes to data protection and processing, but still, plenty of issue arise fairly often. But as previously stated, the GDPR is just for EU citizens, and when it comes to IoT, there are several different privacy related issues to be handled still. One being data collected from sensors, such as images or other things that can have information that a person could be identified from. Also, the storing of this data is a huge question as well. This is relevant to know for this thesis, because these issues for example include automated vehicles as well as connected ones. [13]

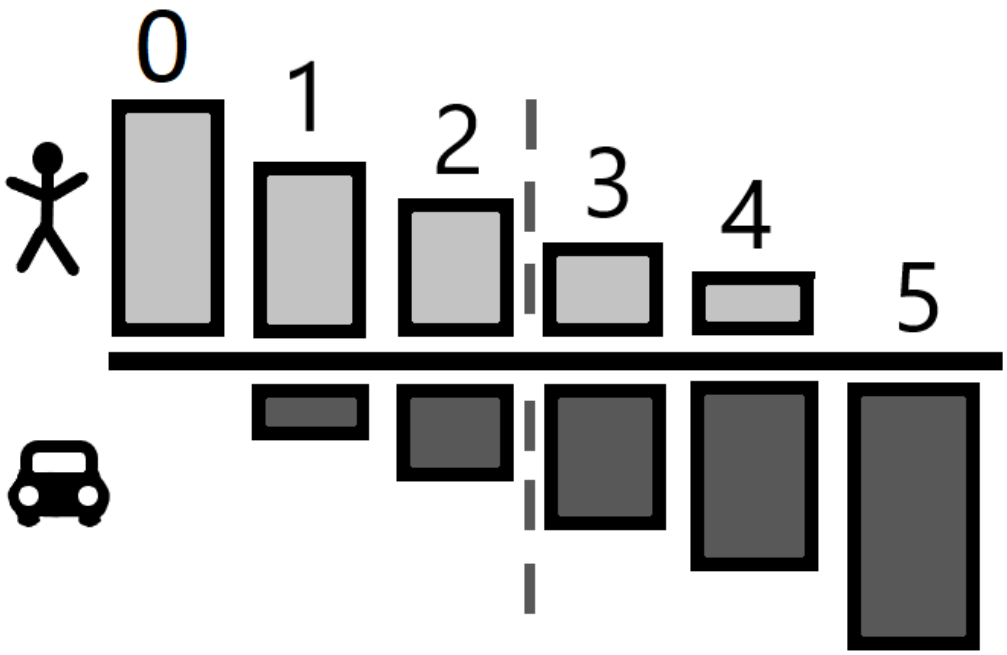
Transient data is something that can be difficult to handle in compliance with the GDPR, because the GDPR's scope extends to all data that can be used to directly or indirectly identify an individual regardless of how long the data is retained. Transient data is meant to be stored temporarily and deleted shortly afterwards. Sensors collect data and thjis daat can either be transient, or it can be stored for longer periods of time in the automated vehicle's memory. In order for the collection of sensory data to be compliant with the GDPR, some steps have to be taken. Some solutions for these issues include minimizing the amount of collected data to only what is strictly needed, automated deletion of transient data after it is no longer needed, masking sensitive information as it is received before storing, such as faces, and to incorporate privacy design principles within the systems. [14] [15]

3 Automated driving

Automated driving is an emerging technology that has been a topic of research and controversy over some years now. It is a technology that enables vehicles to drive without or with minor human intervention. It ahs great potential, as it has many benefits if implemented correctly into society. However, automated driving has many challenges in the form of legislation, cyber-security, ethics and technology. Technology adaptation is also a very relevant challenge, one that this thesis aims to address. The following chapters will provide an overview on different fields of automated driving, such as defining automation, relevant technologies and most prominent challenges.

3.1 Automation

Automation means the act of minimizing human interaction with anything. This is done by utilising new technologies and having computers and machines function without human interaction. Vehicular automation can be defined multiple different ways, and vehicles can have distinct levels of automation in its features to be considered automated. The Society of Automotive Engineers or SAE has created a standard for categorizing different levels of automation in vehicles. [16]



h

Figure 3.1: SAE levels visualized. Adapted from [16]

3.1.1 Levels of automation

The different levels of driving automation that SAE has defined in their standard are the following:

- Level 0: No driving assistance This level includes no automation of features. These features are very limited, and they only provide warnings and momentary assistance when driving. For example, blind spot warnings, lane departure warnings and automatic emergency braking are the only automation assistance features this level entails.

- level 1: Driver assistance Some driver assistance is provided and they only function one at a time. Keeping the driver still very relevant, but some more assistance is provided. These features are used in steering or brake/acceleration support, but not at the same time. Steering support can be used in lane centering, brake/acceleration support can be used in adaptive cruise control.

- level 2: Partial driving automation Level 2 is fairly similar to level 1, but instead of the automated features providing one of, for example, adaptive cruise control or lane centering, the vehicle can do both at the same time. This makes the vehicle a bit more automated than the level before.

- level 3: Conditional automated driving Level 3 is the first larger leap into fully automated driving. This level includes features that can control the vehicle under certain conditions, and only after these conditions are met, will these features take control of the vehicle. The feature can shift over the responsibility of driving to the driver if not all conditions are met. These kinds of features include traffic jam drive.

- level 4: High driving automation When we reach high driving automation, the features no longer require the driver to take action. However, this level still does require some conditions to be met before the features can start driving. Driver can still take action if the driver wants, and if there is a steering wheel installed. This is a type of automation that that can be utilised in local driverless taxies for example. Features do not work in every possible condition, but the features do not require the driver to take action.

- Level 5: Full automated driving Level 5 is again, similar to level 4, with the exception of the features being expected to be able to drive the vehicle under all conditions, and it can drive everywhere. Again, the features do not require the driver to take action, and most likely no steering wheel is installed as the vehicle is supposed to be fully capable of driving.

These levels of automation can be grouped into two (2) categories, which are basically the ones where the human drives, and the ones where the features do most of the driving. Levels 0-2 are driver support features, and the driver is still responsible for the vehicle at all times. The driver supervises every action, and the driver is the one driving. Levels 3-5 include automated driving features. When these features are engaged, the driver is not in control of the vehicle, and is not driving

it. The driver may still take action, or may be required to take action in some cases and conditions until the final level of automation. [16]

3.2 Safety first!

As automated driving is becoming one of the most prevalent new technologies which aims to improve transportation significantly, safety and security become much more important the closer we get to fully automated driving. The main difference between safety and security is that safety includes different features that are meant to keep you and other road users safe from environmental hazards and variables, and accidents, whereas security is there to protect the driver and the vehicle from deliberate cyber-attacks and attempts at theft for example. Safety and security need to be designed early on in development, and different principles have to be addressed. In the previous chapter 3.1.1 was mentioned that a driver would have to take control of the vehicle if the vehicle's systems alerted the driver a certain way. This is an example feature that has to be done in a safe way and that the vehicles operator also has to have awareness in these situations, also the driver-initiated handover should be done with minimal risk. Also, as an example of the principles of automated driving include, but are not limited to dealing with degradation, passive safety, such as seating position or crash scenarios, and behaviour in traffic. How should safety and security concretely be considered and how is it provided? [16] [17] [18] [19] [20]

3.2.1 Safety

Creating safety overall is not too easy, but it can be done. Take airplanes for example. They are flying death traps if you wish to look at them that way, but they are much safer to travel in today's world than cars are. Why is that? One reason is that the measures taken to ensure a safe travel and landing are so over-the-top that

little to nothing severe can go wrong. Of course, there is always something that can go wrong, but you are still less likely to die flying than driving. Safety is ensured by having a set of standards for safety, professionals flying the planes, control towers to take care of incoming and departing traffic at airports, new technologies are tested and trained properly before applying them in a real-world scenario, and so on. This type of over-the-top thinking regarding safety in automated driving could be a good thing. The part about safety being difficult to apply all the way is that sometimes too much safety hurts system availability so much that it is not efficient and is less likely to be used due to the decreased customer satisfaction and feeling of safety. However, one does not want their safety systems to be lacking in a critical sense. [17] [19] [21] [22]

Safety of intended functionality

As previously mentioned, standards are something that can have a huge impact on the safety of vehicles, and more importantly, they are frameworks on which to build on different safety measures for example, and they are there to ensure a certain, universal, level of safety. The ISO-21448 or SOTIF (Safety of intended functionality) is a standard developed for the purpose of providing a framework for measures in order to ensure safety of the intended functionality. This basically means that the standard offers guidance on different methods on minimizing hazardous behaviour of the vehicle when encountering different risks in different scenarios. The aim is also to help identify as many safety hazards as possible and to reduce risks implemented in different phases. The mentioned phases include for example ways of verification and validation of algorithms and other functionalities, technical reviews on them, operation phase, which includes field testing and simulation testing, and field monitoring different SOTIF incidents. Since the cause of hazardous incidents can be originated from the vehicles own system misbehaviours or from external

factors, SOTIF and other safety and security standards can be applied to automated vehicle safety. [23]

Safety in sensory technology

Algorithms and sensors are things that automated driving is heavily reliant on. Sensors provide the necessary data in order for the algorithms to perform in a certain way. The previously mentioned SOTIF applies here as well. Changing weather conditions can prove to be difficult when it comes to automated driving, as it has an element of risk and variability that can impact sensory detection of objects for example or impact the driving functionalities of the algorithms by not having enough data to work with due to bad weather. [24] [25] [26]

There are different kinds of sensors used in automated driving. Since one single sensor type is not capable of providing enough reliable information especially under not ideal weather conditions, automated vehicles have a few different types of sensors embedded in them. Some of these sensors are more affected by bad weather conditions than other. Camera is a sensory technique that is highly sensitive to weather conditions. Cameras are affected by sunlight, rain and fog for example. Cameras also have limited precision from range, but they do provide visible cues effectively in proper conditions. Another example of a sensor that is impacted by weather conditions is LIDAR. LIDAR is another technology that autonomous vehicles can utilise in mapping their surroundings. LIDAR is not as easily affected by weather conditions as cameras are, but it does have some sensitivity to weather conditions, such as rain and fog. Then there are other sensors that are not so reliant on weather that are utilised in automated driving. Radar technology being one of them. It is precise and used for detecting moving objects within a relevant range and has high resistance to weather conditions changing. These types of sensors are referred to as "environment perception sensors". [24] [25] [26]

There are also plenty of other sensory systems in vehicles that are used in localization, tracking the vehicles states and for example in monitoring different events and failures. It becomes crucial that these sensors provide information via the proper pathways to the relevant receivers. [24] [25] [26]

Life cycle

Safety is crucial part of automated driving, and as the vehicle gain more mileage, and different parts begin to deteriorate, safety still needs to be a priority. Sensors can be used to detect performance and wear and tear to some extent at least, in order to keep the vehicle as safe as possible. The fact that vehicles often can have a rather long-life span, can create some challenges when it comes to safety and security especially. One needs to replace or upgrade parts and software during the vehicles lifespan, there for it is important that these parts are replaceable, and that they are compatible with the vehicles other systems that are in place. It would also be considerable that a certified and trusted professional would do these system updates, upgrades, or part replacements. This is simply because otherwise they could create certain security issues, and therefore safety issues. For example updating your vehicles systems in a not-so trusted establishment could result in computer viruses or spyware being uploaded into the systems, which could result in the vehicle not functioning properly and therefore not being safe. [17] [19]

3.2.2 Security

Security is something that entails plenty of aspects in its definition. Security often means that you have some protective features from different types of dangers, be it physical or in this case, cyber-physical. Vehicles need to be protected from dangers as they are high in value, and because human life is also very valuable. A vehicles' systems can be complicated, and plenty of fail-safes and different protective features

are often instilled in them to firstly prevent the loss of life in traffic, and also preserve the vehicle. The fact that the vehicles systems and connectivity is increasing and when it comes to automated driving, it is definitely the case, means that the area of possible points of weakness in the system increases. The systems in a vehicle are also reliant on other system, so the infrastructure and other systems need to be secure in order to function and form trust in automated driving. This does mean that the number of threats increases as communication systems become more complicated, which poses a challenge for the security engineering of cyber-physical systems. [19]

Cybersecurity

Cyber security in automated vehicles can be very complicated and different components and systems needs to be secure in order for the whole vehicle to be secure. An example of the categorization of different point of attacks in vehicles can be as follows: 1. Automotive control system This includes the vehicles electrical control units ECU and in-vehicle networks, which is mostly built around the CAN-bus, which will be covered in more detail in section 2.3. 2. Autonomous driving system components These components include the previously mentioned sensors, and mobile applications. 3. V2X communication Vehicular ad hoc network (VANET) and infotainment. This section includes ways that the vehicle communicates with the outside world to other vehicles or infrastructure. These will also be covered in section 3.3 in more detail.[27]

All of these differently categorized points of attack have increased presence in vehicular systems, and an autonomous vehicle is reliant on most of these technologies in order to function properly, so there has to be methods in order to protect vehicles as a whole package, and technologies need to be chosen with not only effectiveness but also security in mind. How is cyber security effectively built in autonomous vehicles and what kind of security systems need to be in place? [27]

Cybersecurity can be implemented in several different areas and different ways in vehicles by utilizing different types of protocols and systems. For example, from an architectural standpoint we can design different frameworks that work in automated driving. V2X communication systems are an example of a complicated system that would require planning on an architectural level. Also, CAN-bus and VANET security is something that needs to done in an architectural manner in order to gain understanding about the structure of the system. Architecture models are the foundation in defence against cyber threats and threat modelling. [27] [19] [28]

Different components in a normal computer network can be protected with methods and systems such as IDSs Intrusion Detection System, encryption methods, firewalls, access control methods and verification methods. These methods and systems can also be applied to autonomous vehicles' inner networks over the CAN-bus for example and to the communication between V2X. [29]

Intrusion detection systems are basically software or devices used to detect malicious activity or policy violations in a network by monitoring the networks activity. Intrusion detection systems are a reactive method of cyber-security, as they monitor when a threat is detected, and notify the necessary parties of this anomaly. There are a couple of versions if intrusion detection, and a couple of examples are NIDS Network Intrusion Detection System and HIDS Host Intrusion Detection System. NIDS monitors a network with certain policies, and HIDS is used on a single device at one time to monitor the traffic of a device. These systems often react to known attack patterns and they are used to prevent such scenarios from escalating. IDSs can be utilized and should be utilized in automated driving, as for example, the CAN-bus can be very vulnerable, and there are different variations of system introduced especially for the CAN-bus. These methods vary from focusing on anomality detection to language-based IDS in automotive embedded networks. [29] [30]

Encryption methods are a preventive method of cyber-security. Encryption

methods are used in different computer systems quite extensively with different variations of asymmetric and symmetric cryptography. The point is to encode the data that is stored or transported, so that only the intended receiver can read it, even if the data reaches the wrong parties because of an attack. Cryptography can sometimes be a bit much on an IoT system, so more lightweight encryption options have also been developed. A widely used encryption algorithm is known as the AES (Advanced Encryption Standard), which utilizes symmetric key encryption. Data transported with in the CAN-bus or VANET can also be encrypted. This was not the case too long ago, as the CAN-bus was considered moderately safe and encryption was deemed useless. An example of an incident will be provided later, and different encryption methods that can be used in automated vehicles include AES. [31]

Firewalls are basically systems that control and monitor network traffic based on a set of pre-described rules. Firewalls are an essential part of network security in most smaller and larger systems, and applications. Firewalls are a threat preventive method of security, but the rules and functions of firewalls can be changed by reacting to new types of threats. Firewalls work well with IDS and are often paired up. Firewalls are used in vehicles to block unauthorized requests from external factors. Firewalls are being used to secure communication channels in automated vehicles by monitoring and controlling traffic that is incoming and outgoing. [28]

Access control is a method of security that enables only authorized users to access a system's data and resources. Access control methods include the likes of username and password combination, or for example biometric identifiers such as fingerprints or voice. A key can also be defined as access control for example. But when it comes to some of these methods, they all have their strengths and weaknesses. People can forget their password, they can sometimes be guessed by outsiders, or a key can be stolen. These methods however do make the vehicle more secure when properly

managed and implemented. Username and password combination are a fairly basic example of how one could implement access control in a vehicles information systems. [28]

The field of cyber security also requires standards in automated driving. As previously explained, standards are a way to ensure that certain systems and services are to some extent working in an expected manner and they provide a sufficient amount of security for example. ISO/SAE CD 21434: cybersecurity engineering is a standard that is explicitly aimed at road vehicles. More this and other standards in chapter 3.2.2. [32] [27]

Standards

There are already existing different standards for cyber-security. Some of them are aimed at automated driving, and some of them are aimed at cyber security as a whole, but they can be adopted in automated driving in regard to safety and cyber-security. Defence in depth, secure development lifecycle and ISO/SAE CD 21434: Road vehicle - cyber-security engineering are examples of some of the standards that are utilized in automated driving. [32] [17]

Defence in depth is a strategy that utilizes multiple different methods of security that can described as layers of security. This is done in order to prevent access to valuable data and to prevent attacks, as well as minimize the damage an attack could do to vehicle by providing additional layered security to different components of a vehicle for example. If a part of the vehicles defence systems fails, the vehicles integrity as a whole should not be compromised and this is where Defence in depth comes in. As previously mentioned, there are many methods of security, some of them protect the data, and then moving up layers, some of the methods are used to protect the network for example. As vehicles do not operate by themselves as they are supported by infrastructure, these security methods need to be applied to those

h

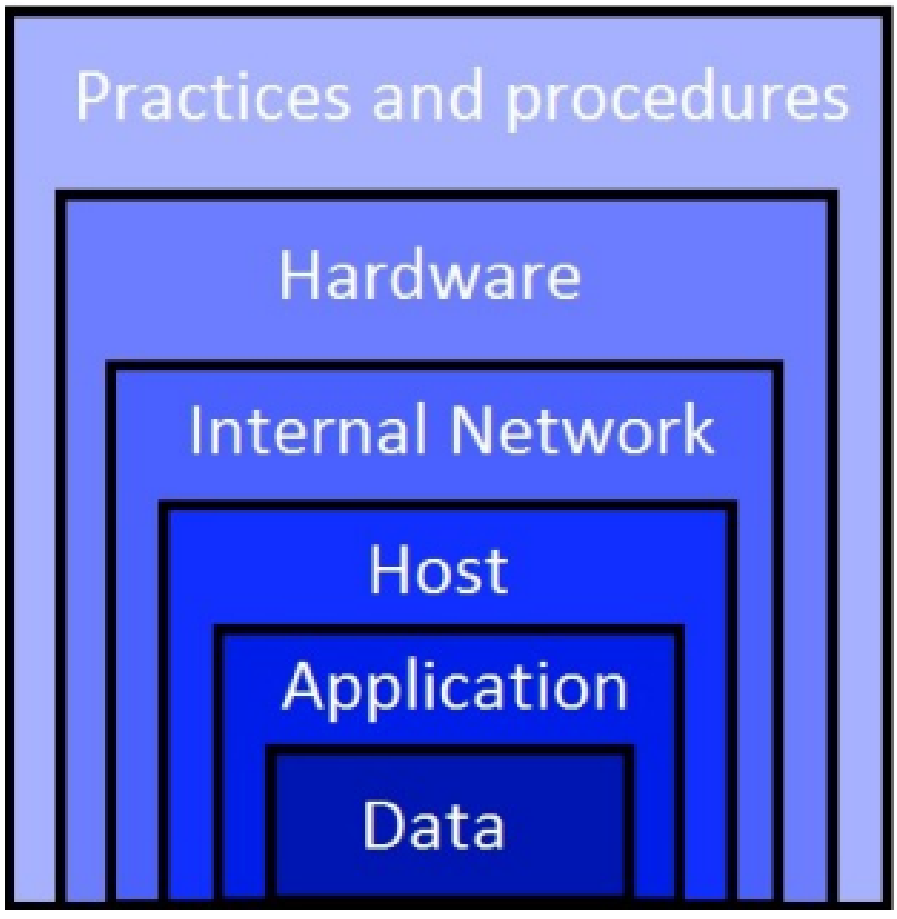


Figure 3.2: Defence in Depth model vizualised. Adapted from [17]

as well, because an automated vehicle should be able to trust the data it receives from different infrastructures.[32] [17]

Secure development lifecycle (SDL) is another type of method used to ensure that development of applications and functionalities of the entirety are conducted securely early on. SDL practices are diverse and can be used to prevent attacks and fix vulnerabilities before they become an issue. SDLs can be divided into 3 categories, which are the preliminaries, development and finally sustainment. The preliminaries include training within the developing organisations in order to achieve a certain level of knowledge of the development and relevant issues and best practices, as well as guidelines, procedures and policies are made to ensure the development itself has a steady foundation. The development phase includes all the aspects that are related to software engineering. These include the likes of defining the security requirements, threat modelling, code review and penetration testing. And finally, there is the sustainment of the product. Incident response and keeping up to date software are examples of ensuring product continuity after release. All these 3 areas of secure development lifecycle are required in building security. Of course, resources are not infinite within most organisations, and some risk trade-offs probably have to be made and some issues are of a higher priority than others. Risk assessments are used in order to decide what is of the highest priority and what is not. [32] [17]

ISO/SAE CD 21434 is a standard that specifically is aimed at the cybersecurity engineering of road vehicles. Its aim is to ensure the consideration of cybersecurity in road vehicles, adapting to new technology and evolving attack methods. As other ISO standards, this standard also offers guidelines in order for organisations to “define cybersecurity policies and processes, manage cybersecurity risk and foster a cybersecurity culture”. The scope also includes engineering requirements that enforce cybersecurity risk management regarding for example development, maintenance and decommissioning of different electronic systems in road vehicles. [32]

[17]

Physical security

Automated vehicles are a prime example of cyber-physical systems that are placed in vulnerable positions in the world. This is why a physical level of security is also required in order to prevent attacks and malicious intentions to the vehicle or its owner. Physical security in cyber-physical systems is used to prevent data from being in the wrong hands by for example storing data in a safe environment behind a locked door or having a hardware security module as an added layer of physical security. Security engineering offers us plenty of solutions for physical threats, with vehicles as well. [33]

Storing a vehicle in a safe location helps the vehicle be secure and protected, but the most obvious first levels of physical security are a car alarm and a car lock. Criminals can already breach both of these methods fairly easily, even with electronic key systems by relaying the signal from the key for example. But non-the-less, physical security also evolves as time goes on, and physical security methods often act as a deterrent to ever even try to attack a vehicle in this case. They are also put in place to make stealing or breaking into a vehicle much more difficult, and to protect the cyber-systems on a physical level as well. [33]

3.3 Communication technology

Firstly, the amount of communication technologies within connected vehicles, let alone autonomous ones, is quite insane. This is due to the fact that a vehicle needs to acquire data from many different sources, and it may also be needed to provide data to some actors within the traffic systems. Internet of Vehicles, as it is referred to as, covers a variety of different interactions an autonomous vehicle has. These interactions are reliant on OBUs (onboard units), RSUs (roadside units) and

vulnerable road users. Different sensors and actuators are responsible for providing and collecting the data from each other or from the environment in order to assist automated driving. [34] [35] [36]

3.3.1 External communications

Examples of different communication needs that an autonomous vehicle has are V2I (Vehicle-to-Infrastructure), V2V (Vehicle-to-Vehicle), V2P (Vehicle-to-Pedestrian) and V2U (Vehicle-to-User). Vehicle-to-Infrastructure is a wireless communication exchange between the traffic infrastructure, such as road or weather condition alerts, and traffic control information. Vehicle-to-Vehicle communication is communication that happens between vehicles about their speed, distance, and overall position among vehicles. Vehicle-to-Pedestrian communication is communication between vehicles and vulnerable road users about safety related services. And finally, Vehicle-to-User communication is between the current user and the vehicle about driving situations in detail, such as location for example. The last communication exchange can be wired or wireless. [34] [35] [36]

What makes external communication so important is the fact that driving and autonomous driving is very dynamic when it comes to sensory data, so the communication of data in and out of the vehicle needs to be accurate, efficient, and reliable, also, uncompromised. External tools are used for safety reasons, but they do raise some privacy and security concerns, which will be discussed in chapter 3.4 more in detail. [34] [35] [36]

3.3.2 Internal communications

The internal communication of vehicles is mostly conducted by utilising a network called CAN (Controller Area Network). It is a rather simple system, where different electronic control units (ECUs) are transmitting data amongst themselves in a net-

h

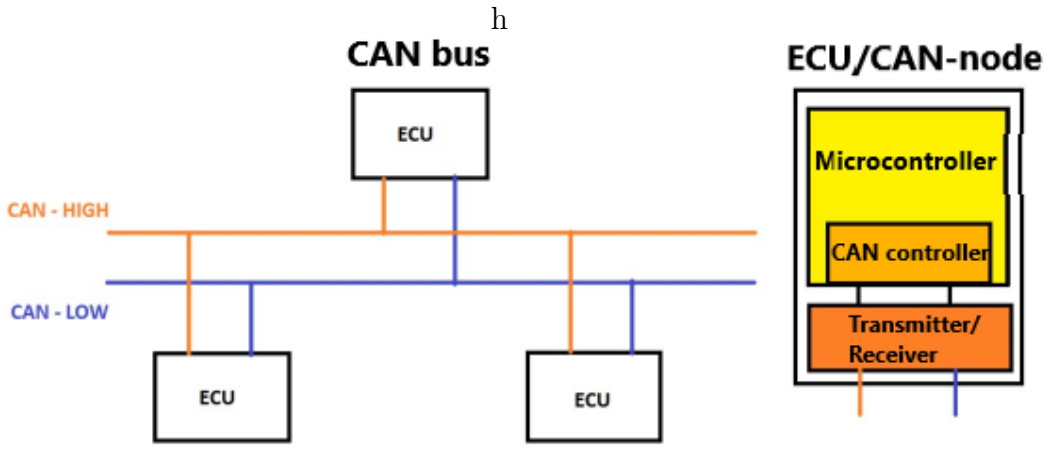


Figure 3.3: CAN bus depicted. Adapted from [34]

work being interconnected, rather that each ECU having a separate communication channel for data transfer. The reason CAN bus is so popular in vehicles is that it is fairly simple and cost-effective way to create a bus that allows communication between different ECUs of the vehicle. It is also scalable and adaptable, which makes it even more desirable. [34] [35]

The way CAN bus works is that the ECU in the node decides the message that will be transported, the CAN-controller then stores the message and forwards it to the transmitter-receiver, which then sends the data into the network, transferring it into a transportable form, and utilizing the different levels of the CAN bus. When receiving, the transmitter-receiver is checking the bus for messages dedicated to this specific ECU, it then transfers the message to a readable form for the CAN-controller, which then stores the message for the micro-controller to be retrieved when necessary. The different levels of the CAN bus have different voltages. This allows for the communication within the bus to not be disturbed by outside disturbances. [34] [35]

CAN bus does have its weaknesses when it comes to security. When devising a

communication method that allows for the communication of every ECU together in one bus, the problems are bound to happen. Data security within the bus, with an evaluation of current threats, can be questionable at times. More on the threats and challenges related to the CAN bus in Chapter 3.4.

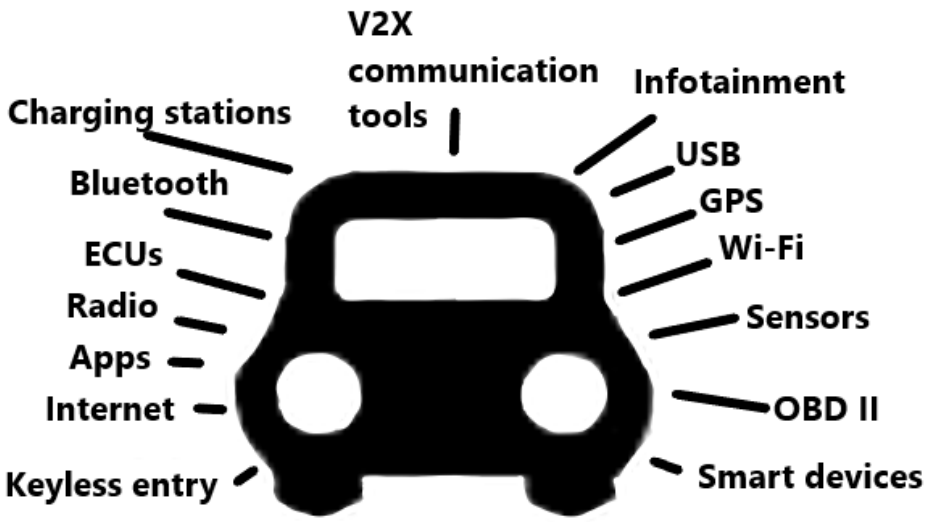
3.4 Issues in automated driving

Automated driving is a rapidly developing technology, and it has great potential to improve transportation. However, there are plenty of issues and challenges when it comes to automated driving. Some of these challenges are also relevant in the trust and adaptation of completely automated driving. They are also spread around many different fields, such as legislation, ethical issues, technology usage and cyber security.

3.4.1 Cybersecurity

Cybersecurity is the act of protecting systems and networks from malicious actors. Attacks from malicious may disrupt the systems, disclose unauthorized information or otherwise damage the system for example. Some of the most relevant threats that automated vehicle's systems' may encounter are described in this chapter. [37] [28] [37]

Remote hijacking means the act of gaining unauthorized access to a vehicle's systems and take over the controls of critical functions such as acceleration, braking and steering. This can lead to accidents or enable malicious activities. A great example of remote hijacking a vehicle was presented by C. Miller and C. Valasek in 2015. In their experiment, they managed to stop a road vehicle in traffic, and also control other vital driving elements remotely. They identified a vulnerability in the vehicle's infotainment system, granting them access to the internal communication



h

Figure 3.4: Attack surface of a vehicle. Adapted from [33]

bus of the vehicle, allowing them to remotely hijack basically any road vehicle of the same model. The discovery of the vulnerability caused a mass product recall of the vehicle. In this particular case, the vehicle was not highly automated, but a vulnerability still managed to cause significant potential harm. [38]

Malware and ransomware attacks in automated vehicles can also prove to be a major threat, because the vehicles rely heavily on software, and if these systems are compromised by malware or ransomware, it can disrupt vehicle operations, compromise passenger safety, or hold the vehicle's functionality hostage until a ransom is paid. [27]

Because autonomous vehicles also rely on sensors providing the systems information, Sensor spoofing can also be a relevant attack. In a sensor spoofing attack, an attacker aims to manipulate sensor data provided by LiDAR, cameras, and radars, affecting the way the vehicles perceive their surroundings. This can result in the vehicle making incorrect decisions, such as failing to detect obstacles or misinterpreting road signs. [27] [24] [25]

Data privacy is something that will affect many different areas of automated ve-

hicles challenges, for example legislation, but data privacy breaches are also a severe threat with high risk when it comes to automated driving data. Automated vehicles collect vast amounts of data, and store data relevant to the users, such as location, personal information and driver behaviour. If this data is not adequately protected, hackers can gain access to sensitive information, leading to privacy violations or identity theft. [27] [39] [37]

Communication channel attacks are also relevant in autonomous vehicles. Autonomous vehicles rely on wireless communication technologies for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, as well as others mentioned in chapter 3.3. Attackers can attempt to intercept or tamper with these communication channels, leading to disruption in communication, false messages, or unauthorized access to vehicle networks. [34] [35]

Supply chain vulnerabilities are also considerable when contemplating threats to a vehicle's information security implementation. The complex supply chains involved in manufacturing autonomous vehicles can introduce cybersecurity risks. If any component or software in the supply chain is compromised, it can lead to vulnerabilities in the vehicle's security and compromise its overall safety. Also, Different manufacturers need to communicate their cybersecurity protocols and needs for different products and vehicle components. This can lead to different issues regarding different components manufacturers also. [19] [17]

Lack of cyber-security awareness, or social engineering, is something that attackers actively try to use to their advantage. Social engineering can conventionally be done in the form of phishing emails, but social engineering is also a problem in automated vehicles. If users or operators are not adequately educated about potential threats or fail to follow security best practices, they may unknowingly expose the vehicle's systems to vulnerabilities. As an example, a user could potentially insert a compromised disc into the system or download an application that has malicious

software component, compromising the system to attacks and privacy violations. [40]

3.4.2 Technology

Technological challenges with sensors, safety and the algorithms used in decision making, as well as other different parts of the vehicle are introduced briefly in this section. Firstly, thorough demonstrations that considering SAE levels 3-5 of automation the vehicle can operate safely. It can also be affected by driver interaction, as levels 3 and 4 may still require driver interaction, but the driver might not be as alert as usually with less automation. Vehicle control take over should also be indicated clearly, so that the driver notices the requirement even if they are not focused on driving while the vehicle has full control. The transition should also be made smooth, so that it is safe for all parties. [18] [17]

Sensors need to be able to provide reliable data for the vehicle. This coupled with difficult road conditions, or high speeds can affect the decision making of the vehicle's systems. If sensors are unable to provide reliable and accurate data for the vehicle to help it have situational awareness, they are ineffective. There can be difficulties in utilising multiple different sources of information, especially if sensors and other sources of information have conflicting data. [24] [25]

CAN Bus is mostly responsible for the communication between different ECUs in a vehicle. Making it reliable, safe and secure would be a top priority. However, the CAN Bus offers a wide attack surface for potential attackers in the forms of physical attack opportunities (OBD port, Multimedia) as well as remote attack opportunities Bluetooth, cellular, Wi-Fi, GPS..., meaning that security features need to be implemented. Considering the fact that an automated vehicle needs fast communication in order to make decisions, these security features; verifications and authentications can't be too heavy on the systems processors as they could slow

down the vehicle response times. Machine learning is probably the biggest part of automated vehicles that requires testing and validation in order to be implemented and trusted. Transparency in its decision making is a relevant component in creating trust in machine learning. These algorithms are also susceptible to different attacks. As the importance of data grows, the possible risks and effects of data corruption, manipulation and cyber attacks in general are amplified. Unpredictability is another possible issue that needs to be addressed for the safety of passengers and other road users. [34] [35] [36]

3.4.3 Legislation

Issues regarding legislation in automated driving can prove to be very difficult. Especially now that a manufacturer or service provider could be more easily held responsible for car accidents, and legislation regarding traffic is different in different countries. Currently however, unless a new framework is presented, manufacturers and providers have significant freedom in deciding how to manage their liability in accident situations. [40] [41] [42]

The relationship between privacy and legislation is also quite difficult to determine, as privacy is another aspect that may affect liability and effects of accident causes. Automated vehicles gather plenty of information that could prove to be useful in determining causation and liability, but sometimes at the cost of privacy. Operational functions, speed, position and other factors can be detected by using data. These factors could determine liability if for example the vehicle is not entirely automated, and the driver was properly and timely warned to take over the vehicles controls but refused to do so. Or in the case that the vehicle is fully automated, and what needs to be determined is that is another road user is at fault. This could be determined from the operation of the automated vehicle. [37] [39] [42] [41]

Then there are the cases where the vehicle has a design defects, or manufacturing

defects. A design defect means that in this case, the vehicle is manufactured correctly according to the design and instructions, but it means that the defect is in the designs. This can mean everything from designing the functioning logic for the vehicle, or designing how a seatbelt is supposed to function. A manufacturing defect means that the vehicle is not manufactured as it was designed, and that there is a faulty part somewhere. [42] [41]

Design defects are somewhat common in vehicles, as mechanical defects, but are not too easy to detect, and they require a certain amount of proof before potential issues can be proven to be defects. Design defects can be issued from not meeting customer expectations, as in something is not functioning the way that most consumers would expect, or they can be issued from there being a more reliable and feasible solution that can be provided. Testing and simulations can be used to mitigate the chances of there being many design defects. Vehicles and especially automated vehicles are complicated entities, so it makes design defects all the more probable. [42] [41]

Manufacturing defects are rather straight forward as previously stated, there has occurred an error in the production line and the product has now become faulty even if the design is all right. Quality control and minimization of variables during the production process are ways to prevent these types of issues. How ever, when it comes to automated driving, the software is supposed to learn from previous experiences, which means that the software is not same when driving and leaving the factory. This again is another liability difficulty. [42] [41]

Cybersecurity is another issue that is heavily included in legislation issues. Cybersecurity problems in automated vehicles are a liability and as previously presented, they can prove to be a huge dilemma in other ways as well in the form of hacking and theft. However, still, developing cybersecurity is mostly up to the manufacturer to implement following certain guidelines. There are no specific re-

quirements presented to manufacturers, but general security features need to be implemented in order to be certified for example. There are certain sets of governing entities that enforce the implementation of cybersecurity measures, and several different standards that can help manufacturers implement cybersecurity methods, but it is not easy. One of the most prominent issues with legislation regarding cybersecurity in automated driving is that in how much detail should legislation address cybersecurity threats and requirements. [42] [41] [28]

3.4.4 Ethical

There are also plenty of ethical issues regarding automated driving. These issues can be combined with for example some security related issues such as privacy, as it is also an ethical concern in the field of automated driving and computing in general. Ethical categories include issues such as job displacement, social inequality, previously mentioned privacy, liability and safety. [43] [44]

Safety is a very important ethical issue. It is important to make the vehicle safe for its users and other road users. Safety is an issues that extends beyond the vehicle itself. Relevant safety over the vehicles software and hardware that operate the vehicle is also important, because these are the parts responsible for the vehicles activities on the road that affect other road users' safety. Then there are some moral dilemmas included in safety. Such as how should the vehicle react to surprising situations and complicated decisions. If the vehicle is faced with the decision of hitting a pedestrian, a wall or dodge into oncoming traffic, how should it be taught to react. [43] [44] [17]

Liability can be connected with legislation issues. The fact remains that car accident responsibility is still an issues that is up for debate. It is not easy to decide if the driver, manufacturer or software developer for example are responsible for car accidents. Even currently accident responsibility can be difficult to determine, but

it is still manageable due to the fact that human drivers make mistakes. You can blame a vehicles programming, but who will your car insurance provider feel about that. [43] [44] [42] [41]

Privacy is also an ethical issue, because we have systems that improve the safety and security of passengers as well as other road users, but sometimes a safety-privacy trade-off is necessary, and determining the acceptable line for the trade-off needs to be considered. Currently road users can move in traffic without an electronic trace if they so choose, but automated driving affects this in a negative way. As an example, a vehicle can detect information about its passengers and people around the vehicle, which can sometimes be considered as intrusive of privacy, in addition to other communication methods that the vehicle uses and needs, as they are introduced in chapter 3.3. Job displacement is also an issue to consider. It is important because many people work as professional drivers, such as taxi or bus drivers for example. The automation of these jobs will most likely lead to unemployment or at least require some type of solution about the situation. However, the automation of these jobs and the improvements of automation of traffic might bring different jobs, or at least motivate the workforce to work further away from home and the need for engineering jobs might increase in the automotive industry. The impact that automated driving might have on employment is uncertain. [43] [44] [39] [37]

Automated driving might also bring social inequality. This is because it will most likely not be cheap at first, and not everyone will be able to afford such a travel method. Also, automated travel could be significantly improved for those who can afford it, creating social inequality. Some sensors can also be affected by a pedestrian's colour of skin, making it more dangerous to be a pedestrian in traffic for different skin toned people. Automated driving could also impact localization of shops and firms creating newly desirable areas and possible making other areas undesirable. [43] [44]

4 Trust in automated driving -questionnaire

An analysis of trust in automated driving from a road user's perspective was done in the form of a questionnaire in this thesis. Other stakeholders in automated driving, such as society, infrastructure, and vehicles themselves were not considered in this study due to increased difficulty in the measurements of trust on a certain scale. The following chapters explain the reasoning and validation behind the chosen research methods, an insight is offered into the questions in the questionnaire, and an overview of the results from the questionnaire is presented.

4.1 Methodology

4.1.1 Research design and rationale

Research design methods for this thesis include a literature review and a survey on trust related to automated driving. Research questions can be examined through both, and a survey on trust related to automated driving is a good way to determine the current state of trust in automated vehicles. Literature review section is meant to explain the reasoning behind this questionnaire, as well as define trust, and automated driving for the thesis. What we can then gather from the survey and previous research, is used to draw conclusion and offer suggestions on increasing trust

in automated driving. Implications include contributing to a better understanding on the current state of trust in automated driving, and technology related to it. The research findings could then aid in fostering public trust and acceptance, which is crucial in successfully integrating new technologies. Rationale for this research is heavily focused on the previously mentioned importance of trust in successfully integrating new technologies, and by generating a survey, we can then measure trust currently, and identify possible issues that are affecting the formation of trust in a more negative way. Also, to see if there is a correlation of trust in automated driving between different categories of education or previous experience with automated vehicles. A certainty trough is also briefly considered in the analysis of this questionnaire. A certainty trough [45] based on Donald MacKenzie's conception can be described so that people who have a slight understanding of a subject often tend to have more confidence in it than actual professionals and people more educated on the subject. This is because the actual professional is expected to be more educated on the dangers, risks and difficulties involved. How ever, the group who has little to no understanding on the subject is still expected to be the least confident in it. [46] [47] [48] [10] [45]

4.1.2 Development and data collection

The questionnaire was developed under the premise of answering the research questions by coming up with recently collected data and answers to relevant questions. The questions asked in the questionnaire were developed by assessing the research questions and asking questions that would provide answers to them, while also keeping the questionnaire fairly short and easily answered in order to get answers altogether. Another aspect that affected the development of questions was previous research with similar intentions and research goals. These studies being [47] and [48]. The questionnaire was receiving answers for about 3 weeks and was developed

in Finnish, as most students this survey received spoke Finnish, and most people understand the terminology better in their native language. [47] [48]

Methods used in ensuring the validity of the questionnaire were the previously mentioned studies that helped form the questionnaire questions of this thesis. Also, the questions formed so that they should provide answers to research topic and questions. Anonymity in the questionnaire was also implemented to encourage more honest answers and reduce social bias when answering. Anonymity also hoped to increase participation as it protects your identity when answering these questions and they are not linked back to a certain person. Anonymity does have a few drawbacks which include lack of verification and a lack of potential follow up question. Neutral answers were removed from the questionnaire, because this would force a slight tilt to either side of the spectrum of answers, even if the participant had a neutral feeling towards the question. At first the questionnaire was in the point of view of every possible entity related to automated driving, but ultimately after recommendations, a more simplistic approach was taken, and the questionnaire was delivered with a singular and relatable point of view of a person in traffic with automated vehicles.

The questionnaire was mostly answered by and targeted to young university students, as they were easily reachable through the channels that were provided. The summer holidays may have impacted the number of answers received for this survey, and the total number of responds to this questionnaire was 53. The students were mostly reached through popular university communication channels for fields of study, which included Discord, which by far provided the most answers. Answers were from a couple of different Universities and the questionnaire was also posted on a University of Turku bulletin board on Intranet. Other than university students were also reached through some Discord channels for example, and the respondents were given the option to select their education background, results of which will be discussed in the section 4.1.3.

4.1.3 Data analysis

The data will be analysed by using three different comparisons. Firstly, the whole group, secondly, we will compare the answers between those who said they are not familiar with automated driving, or have only shallow knowledge on the subject, and those who said they are somewhat familiar or very familiar with automated driving. Lastly, we will examine if education background impacts answers by comparing those that have or are attending a master's degree equivalent or above, to those that said their education background is a bachelor's degree or below. We are going to assign capital letter abbreviations to the select groups in order to be clearer when presenting the results. Those that selected that they are rather unfamiliar with automated driving will be referred to as "unfamiliar" and they take up 48 of responders. Their counterparts, those that are somewhat familiar with automated driving, will be referred to as "familiar", who take up 52 of participants. Those that belong in the group of bachelors and below will be referred to us "bachelor's" with 66 of participants, masters and above will be referred to as "master's" with 34 of participants. These classes were assigned to determine if there is a correlation between knowledge on automated driving and perceiving its threats more than its possibilities. A certainty trough is also applicable, but due to a somewhat low number of answers and a low amount of actual experts contacted, we can only compare people with little to no knowledge to people with some knowledge on automated driving, and see how their perspectives differ from one another. Educational groups were also assigned for the reason of determining if education levels have a correlation in technology adaptation. Data analysis question by question:

1. "Millaiseksi koet liikenneturvallisuuden kotikaupungissasi tällä hetkellä" (How do you find the safety of traffic at the moment in your hometown) The question was asked on a scale from 1 (not good) to 4 (very good).

This question shows no relevant variation between our selected comparison cate-

	n	Minimum	Maximum	Average	Median
Unfamiliar	26	2,0	4,0	3,2	3,0
Familiar	27	2,0	4,0	3,1	3,0
Everyone	53	2,0	4,0	3,1	3,0
Bachelor's	33	2,0	4,0	3,2	3,0
Master's	20	2,0	4,0	3,0	3,0

h

Figure 4.1: Answers to the 1st question: How do you find the safety of traffic at the moment in your hometown

	n	Minimum	Maximum	Average	Median
Unfamiliar	26	1,0	4,0	2,8	3,0
Familiar	27	2,0	4,0	3,3	3,5
Everyone	53	1,0	4,0	3,1	3,0
Bachelor's	33	1,0	4,0	3,1	3,0
Master's	20	1,0	4,0	3,0	3,0

h

Figure 4.2: Answers to the 2nd question: You receive information that automated vehicles are being tested in your neighbourhood, how would you feel?

gories, as the results vary from averages of 3,0 to 3,2. Those that were in the groups of "unfamiliar" and "bachelors" answered an average of 3,2. All groups average was 3,1, and "familiar" and "master's" groups answered 3,1 and 3,0 respectively. However, this question is an important baseline that we will then compare the results received from the reactions to automated driving in traffic.

2. "Saat tiedon, että asuinalueellasi testataan täysin itseajavia ajoneuvoja liikenteessä, miten reagoit?" (You receive information that automated vehicles are being tested in your neighbourhood, how would you feel?). The question was asked on a scale from 1 (not good) to 4 (very good).

This is already a question with some varying results between groups. The "unfamiliar" have responded with a value of 2,8 which is close to neutral (2,5). Whereas "familiar" have responded with a 3,3, so mostly positive feelings towards testing

	n	Minimum	Maximum	Average	Median
Unfamiliar	26	2,0	4,0	2,5	2,0
Familiar	27	1,0	4,0	3,0	3,0
Everyone	53	1,0	4,0	2,7	3,0
Bachelor's	33	2,0	4,0	2,7	3,0
Master's	20	1,0	4,0	2,7	3,0

h

Figure 4.3: Answers to the 3rd question: Automated vehicles are safe.

automated vehicles in a populated neighbourhood. The “bachelor’s” and “master’s” have a very similar 3,1 and 3,0 averages, so overall positive results.

3. “Autonomiset ajoneuvot ovat turvallisia.” (Automated vehicles are safe.) The question was asked on a scale from 1 (disagree) to 4 (agree)

Differences can again be seen in familiarity rather than general education level groups. The consensus appears to be a bit lower than before with a 2,7 average, which is close to neutral, but just slightly agree. With the entire average going down, the first neutral average among groups has been achieved among “unfamiliar” with a 2,5 average and their counter parts have answered a 3,0, which still resembles previous answers.

4. ”Autonomisten ajoneuvojen oleminen osana liikennettä lisää turvallisuuden tunnetta jalankulkijana.” (Automated vehicles as part of regular traffic increases the feeling of safety.) The question was asked on a scale from 1 (disagree) to 4 (agree).

This question again has the downward trend in answers, with an overall average of 2,5, which is neutral. Slightly disagreeing are “unfamiliar” and “Bachelor’s” while slightly agreeing are “familiar” and “Master’s”.

5. ”Autonominen ajaminen parantaa ajoturvallisuutta liikenteessä poikkeuksellisissa ajo-olosuhteissa.” (Automated vehicles improve traffic safety in extraordinary driving circumstances.) The question was asked on a scale from 1 (disagree) to 4

	n	Minimum	Maximum	Average	Median
Unfamiliar	26	1,0	4,0	2,2	2,0
Familiar	27	1,0	4,0	2,7	3,0
Everyone	53	1,0	4,0	2,5	2,0
Bachelor's	33	1,0	4,0	2,4	2,0
Master's	20	1,0	4,0	2,6	3,0

h

Figure 4.4: Answers to the 4th question: Automated vehicles as part of regular traffic increases the feeling of safety.

	n	Minimum	Maximum	Average	Median
Unfamiliar	26	1,0	4,0	2,2	2,0
Familiar	27	1,0	4,0	2,6	2,5
Everyone	53	1,0	4,0	2,4	2,0
Bachelor's	33	1,0	4,0	2,3	2,0
Master's	20	1,0	4,0	2,6	2,0

h

Figure 4.5: Answers to the 5th question: Automated vehicles improve traffic safety in extraordinary driving circumstances.

(agree).

Very similar answer patterns in this question also. Overall average slightly disagreeing, while “Unfamiliar” and “Bachelor’s” groups are slightly disagreeing yet again, and “Familiar” and “Master’s” groups are slightly agreeing, yet again.

6. ”Autonomisen ajamisen edut. Valitse 3 sinulle tärkeintä.” (Advantages of automated driving. Choose 3.) In the section “Others” another suggestion was made, it was the automation of fright deliveries, which was seen as a good thing. In general, there is not too much variety between our selected categories as to what is an important advantage that automated driving offers road users. The clear top 3 among all groups are ‘Removing incapacitated drivers from traffic’, minimizing human error, and comfort in traffic. Possible improvements in environmental emissions

and general traffic safety were not seen as a top priority.

7. ”Autonomisen ajamisen haitat. Valitse 3 sinulle tärkeintä.” (Disadvantages of automated driving. Choose 3) Another answer was provided, it being the potential of falling objects from a vehicle in front of our automated vehicle. This question can be categorised in the behaviour of different scenarios, but still a valid thought overall. Again a fairly similar graph among all participants about the top 3 disadvantages of automated driving. Top 3 concerns generally being ‘Manufacturing or design errors causing malfunction’, Vehicles behaviour in different unexpected scenarios’, and a tie between ‘information safety and security’ and ‘You lose the option of taking over your vehicle in an emergency situation’. A close follow up is also ‘Legislation i.e., in accident responsibility. Costs and the unemployment of professional drivers were not top 3 material according to many.

8. ”Mitkä asiat saisivat sinut luottamaan autonomiseen ajamiseen enemmän? Valitse 3 sinulle tärkeintä.” (What would make you trust automated driving more? Choose 3)

Other answers included the following: - Complete manufacturer transparency - Thorough testing in different circumstances - Legislative responsibility clearness; high fines for manufacturers for breaches in conduct of manufacturing and development, and demanding testing requirements - Use charge due to indirect costs. Again, a quite similar spread among the groups. Thorough testing gathering a majority of votes from our groups. Following up are ‘Better knowledge on autonomous vehicles’, and ‘Mandatory updating of software and maintenance’. ‘Manufacturers reputation’ along with ‘nothing’ did not reach the top 3 of many people when it comes to improving trust in automated driving.

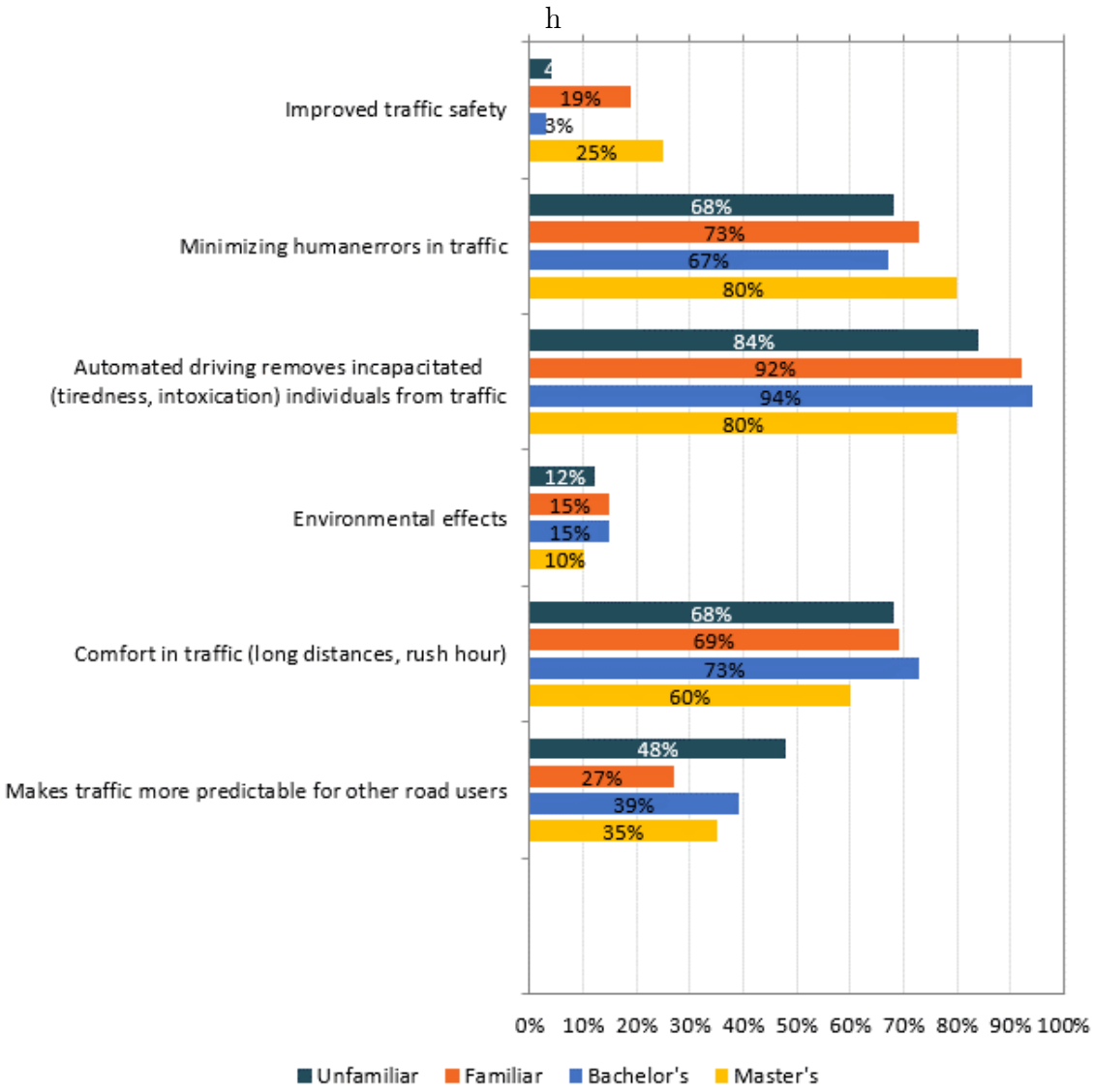


Figure 4.6: Answers to the 6th question: Advantages of automated driving. Choose 3.

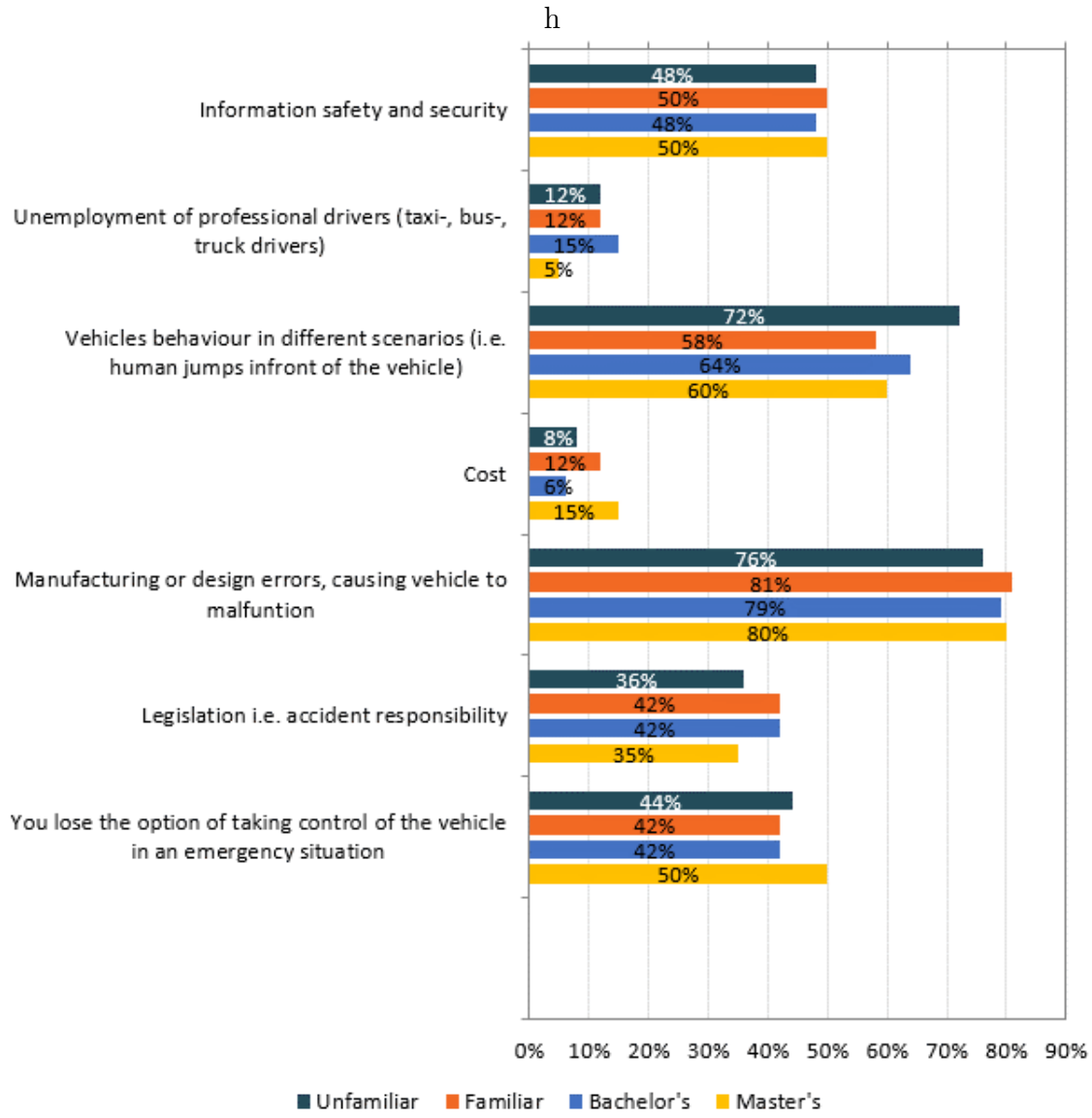


Figure 4.7: Answers to the 7th question: Disadvantages of automated driving. Choose 3

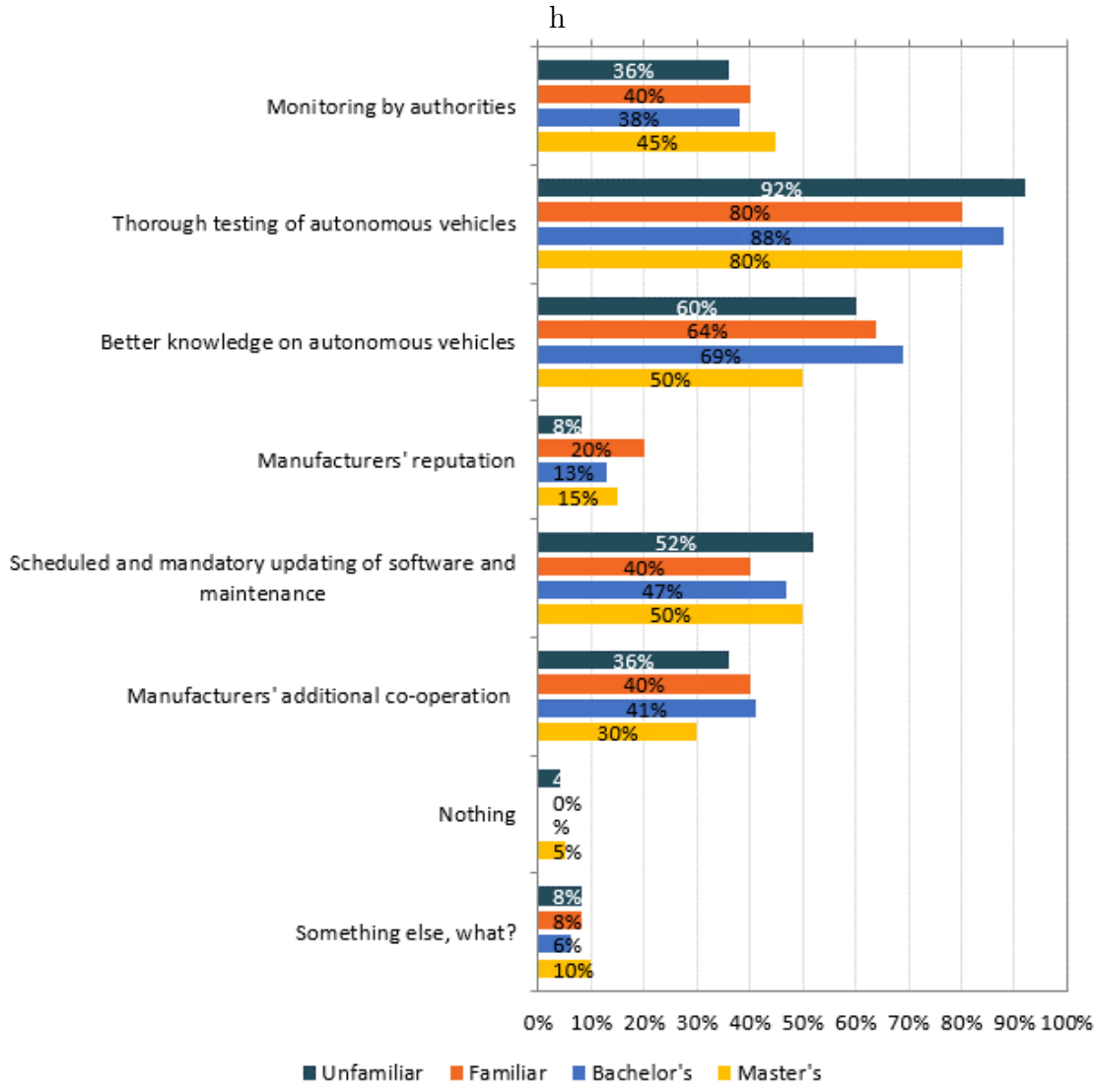


Figure 4.8: Answers to the 8th question: What would make you trust automated driving more? Choose 3

5 Discussion

The results discussed in the previous chapter are further discussed in this chapter. Implications of the questionnaire are presented, as well as possible future research opportunities and limitations for the study are identified for future researchers of the topic. Research questions are also answered in this chapter explicitly.

5.1 Interpretation of results

Interpret the findings from the data analysis in the context of the research objectives. If we compare the results of the questionnaire between our selected groups, and our research questions, we can find some rather interesting results and correlations between our groups.

If we compare questions 2-5 to question 1 we can see that generally answers, especially among "Unfamiliar", are below that of question 1 and in some cases even below the neutral level of answers, so we can see that they are somewhat cautious when it comes to automated driving improving safety in traffic and overall. Generally, the "Familiar" group had a more positive reaction to automated driving and were more open to perceiving it as a safer alternative. Their answers in question 2 averaged more positively than in question 1, which is rather a positive result in relation to testing automated driving in an actual traffic environment and the data shows that this group would be open to see automated driving tested in traffic, and they would like to see the progress that is being done with automated driving first

hand. Testing automated driving so that it would spark excitement is something that would help in technology adaptation. In these questions, answers between "Master's" and "Bachelor's" have little to no differences. Small differences however tip so that "Bachelor's" have a bit less of an average than "Master's". In the questions 3-5 however every group has a little doubt when it comes to the safety and current state of automated driving, "Unfamiliar" group has a bit more of said doubt and uncertainty than the other groups. Varying road and traffic conditions, along with automated driving from a pedestrian's point of view are seen as the most untrustworthy among the respondents across the board. "Unfamiliar" and "Familiar" groups offer more variation in these answers than "Bachelor's" and "Master's", which would indicate in this case that some knowledge on automated driving would improve your opinion of it, allowing you to better adapt the newly developed technology, whereas education overall does not have such a large impact. Being a bit familiar with automated driving showed improved trust in automated driving to some extent in this questionnaire. These results are however to be taken with a grain of salt, for the previously stated reasons.

If we move down to question 6 and discuss the perceived benefits of automated driving according to our groups, we don't see too much variation. Every group appears to believe that the 3 most important improvements stemming from automated driving are getting people who shouldn't be driving out of traffic, minimizing human errors in traffic, and finally improved comfort during transportation. Environmental effects, overall traffic safety and improved predictability in vehicle behaviour were not seen as important in automated driving. This would indicate that basically familiarity and education doesn't matter as to what you view as a top 3 clear potential benefits in automated driving. Also, 2 of the items that were considered important are not reliant on your own driving comfort, but rather on reasons that traffic can be perceived currently as dangerous. Driving under the influence or on no sleep,

as well as reducing human errors such as not paying attention or reacting hastily are perceived as bad, and because these are problems that automated driving would solve, they are seen as a great benefit of automated driving. Then there was also the item that did include your own comfort during longer rides or traffic jams. Automated driving could also enable efficiency and allowing you to not have to focus on driving, providing comfort. The items that were not seen as critical benefits, but benefits non-the-less, involved environmental effects, and other benefits to other road users as well, instead of just improving your own safety and comfort in traffic. As they are not that critically affecting your life right now drastically, they were not viewed as important as the top 3. These results were also across all groups.

In question 7 we determined what factors in automated driving are perceived as disadvantageous. Here we can see an interesting, small correlation between "Unfamiliar" and "Familiar" groups again. "Unfamiliar" have set their clearly biggest disadvantage to be the automated vehicle's behaviour in difficult or unexpected situations, we as "Familiar" did not view it as important when it comes to the disadvantages. However, these answers were still in the top 3 of both groups. This type of correlation could be again coming from the fact that "Familiar" could have a bit more knowledge of machine learning, and information systems as a whole so they know how they operate, where as "Unfamiliar" are more concerned, because the lack of knowledge on the subject leaves room for doubt and untrust. All groups selected the biggest threat or disadvantage to be design and manufacturing errors. This is something that affects everyone equally and immediately. Also, because nothing is ever perfect and will most likely require fine tuning, this is a completely rational opinion. Other important disadvantages were legislative issues, information security, and not being able to take control of your vehicle in an emergency. These are all issues that can affect you very quickly and cause you problems that you either don't want to deal with or don't want to happen to you. The least important reasons

included cost of the vehicles, and the unemployment of professional drivers. Cost was not perceived as that important, as well as the unemployment of drivers, which probably affects professional drivers' opinions the most.

In the last relevant section of the questionnaire, we discuss possibilities of improving trust and what would be important in relation to technology adaptation. This answers a couple of our research questions. Thorough testing, presentation and documentation of results is by far the most requested option out of these alternatives among our groups. Better knowledge on automated vehicles and mandatory monitoring and maintenance of vehicles are also top 3 reasons for possible improvements in trust. Only option that didn't receive that many votes is nothing, and manufacturer's reputation. This question would indicate that the most prevalent improvements and steps towards technology acceptance in automated driving would be thorough testing and presentation of results, as well as better knowledge on automated vehicles as individuals. Others reasons mentioned. Legislation was also mentioned from the "other" category, which is also an important aspect of automated driving and technology acceptance related to it. Relate the results to the existing literature and previous research on X and Y.

If we compare our results with an actual driving simulation in relation to trust, we can see that according to [47], drivers' trust in automated driving increased over time, if no critical situations were introduced. Our study would suggest that more testing and knowledge on automated vehicles would increase our groups' trust, and a more practical study shows that this indeed can potentially happen. Prolonged positive interactions with automated driving will more than likely increase trust in automated driving, along with other reasons discussed earlier, but how much will the inevitable negative interactions create mistrust among our groups? [47] [48]

5.2 Implications and research questions

In this chapter we discuss our findings by viewing them using our chosen research questions, and explicitly answer them one by one. These questions have already been answered in the paper, but this is a summary.

5.2.1 How do different stakeholders trust automated driving?

There are plenty of different stakeholders in automated driving, but for the sake of this thesis, the questionnaire will focus on road users explicitly. Other stakeholders were not considered due to the difficulty in measuring trust by a survey. For example, the facilitators of infrastructure are stakeholders in automated driving, but it is difficult to measure their trust in automated driving sue to the small scale of this thesis. The stakeholders chosen were road users, which were then divided into 4 groups based on 2 categories, those categories were education and familiarity with automated driving. From the questionnaire we can just after a few questions see that those who were already not familiar with automated driving did not trust it as much as those who were a bit more familiar with it. Their answers differed about 15-20 percent in relation to the entire scale of the questions, which were between 1 and 4. The unfamiliar group's scale tipping a bit more to the untrusting side, while those who were a bit familiar with automated driving had neutral, or were hopeful in trusting automated driving as it is today or what it could be in the near future.

Education did not offer us such a result. The result was similar, but the differences were much smaller than with familiarity. Lower level of education was slightly untrusting of automated driving, while people with a bit of a higher education were on the neutral or slightly trusting in automated driving. Overall, the results were rather neutral in trusting when it came to trusting automated driving.

5.2.2 What are some of the key trust issues related to automated driving?

Some of the key trust issues in automated driving can also be found in literature and from the questionnaire in this thesis. The questions in the questionnaire are based on literature, so we can identify the most significant causes of trust issues in automated driving.

Manufacturing and design errors, and the vehicle's malfunction in general, were the most prevalent causes for untrust in automated driving across our stakeholders' groups. This is likely due to these malfunctions causing accidents which were not supposed to happen under normal circumstances, and they can sometimes lead to loss of life. Other considerable sources for untrusting automated driving included the behaviour of the vehicle in different, perhaps surprising situations. These can be referred as different moral dilemmas with automated driving, as an example, will the vehicle go out of its way to dodge a pedestrian who jumps in front of the vehicle, or will it try to preserve itself as well as its passengers? Also, Information security and safety, legislation, and losing the ability to take over the vehicle in case of an emergency were deemed to be sources of somewhat untrusting automated driving.

5.2.3 How to increase the trust of different stakeholders in automated driving?

This question is also mostly answered by the questionnaire. We can gather that thorough testing and documentation of said testing was most likely to improve trust according to the people who responded to the questionnaire. This was the result across every group we chose. Other significant factors to improve trust were selected as personal better knowledge on autonomous vehicles and the way they function, and scheduled maintenance and software updates. A few were not so significant but

factors to improve trust non-the-less. These options were manufacturing and traffic behaviour monitoring by authorities and manufacturers' additional co-operation. These were all mentioned as important factors previously in the thesis, but they were selected the most critical by our respondents. Manufacturer's reputation did not play a significant part in trust.

The results overall were rather similar across all groups, but the people who were familiar with automated vehicles did not see additional knowledge on automated vehicles as important as those who were unfamiliar with them in the first place. This is a rather interesting but expected result.

5.2.4 Possible difficulties with implementing trust increasing methods in automated driving?

Difficulties and challenges have been covered in the literature review section of the paper.

Technical challenges include insufficient sensor capabilities, limited data processing power, and software complexities and inefficiencies. They impact the automated vehicle's ability to accurately perceive and respond to the environment around them. Also, hardware among other aspects also has its limitations, regarding communication technologies for example. Software updating was mentioned as a method of increasing trust. But updating software using wireless connection can have a negative effect due to extreme connectivity creating many outside threats. However, offline updating requires it to be done by a trustworthy entity. This could mean increased costs to the vehicle's owner, and make it difficult for the manufacturers to be able to provide worldwide offline software updates by verifying entities that could be authorized to deliver the updates.

Safety challenges and other issues that affect building trust include the risk associated with automated driving, as well as a fear of accidents and possible mal-

functions. Inexperience with automated driving can increase these fears and create untrust in automated driving. Also, a lack of clear regulations and standards for autonomous vehicles can hinder the implementation of trust-enhancing features. Cyberattacks are a relevant threat in automated driving, however it is very difficult to prepare for attacks that are not yet known, so manufacturers have to use plenty of resources to try to create defensive methods to counteract a wide variety of high risk and high probability attacks. While developing automated vehicles, you are not as a manufacturer getting an immediate return for the cost of testing the product. This could mean that manufacturers go out of business before they can start producing a safe and complete automated road vehicle. Investing in cybersecurity also does not show an immediate reward, so investing in it after a certain monetary threshold can be difficult to justify, even if it were useful and necessary. It was also mentioned that co-operation between manufacturers would be a great way to increase trust in automated driving and possibly improve the products. However, how much is a company willing to share without revealing its competitive edge?

5.3 Limitations and future research

This thesis did not implement any of the suggested methods to possibly improve trust among different stakeholders in automated driving. Also, not all stakeholders were considered in the questionnaire of the thesis. The answer choices in the questionnaire can be subject to change, so the questionnaire might not have presented all possible issues or improvements to trust in automated driving. The questionnaire however addresses some of the identified key issues, and possible improvements that have been suggested, and identifies the most desirable trust improving factors. The scale of the questionnaire was on the smaller side, and mostly included people of a certain age range. In order to gain a more comprehensive view, a larger scale research that reaches more people from different age groups and backgrounds could be constructed.

Future research opportunities following this study can be manufactured. Especially research in a more practical environment based on this research could prove to be useful in the form of a long-term user study for example. This type of research could demonstrate how trust in automated driving changes over time and exposure. It could also be used to pinpoint factors that have been concretely increasing trust in automated driving. Another research opportunity that could be utilised based on this research in the future is to develop safety and reliability metrics in order to evaluate safety and reliability of automated vehicles. Or other similar methods to see if they can be used to improve trust in automated driving.

6 Conclusion

Transportation is rapidly evolving and the emergence automated driving systems represent a pivotal moment in our society, as the quest for safer, more efficient, and sustainability in driving is being explored. This thesis has covered the subject of automated driving by evaluating trust and its crucial role in adapting to new technologies. A questionnaire was conducted, as well as proper literature reviews on trust and automated driving, in order to draw several key insights that illuminate the path forward for the integration of automated driving systems into our lives.

In order to answer the research questions "How do different stakeholder's trust automated driving?", "What are some of the key trust issues related to automated driving?" and "How to increase the trust of different stakeholders in automated driving?" a questionnaire was developed. The questionnaire was mostly aimed at younger audiences, university students mostly. The questions in the questionnaire were developed with these questions in mind.

The most interesting results of the questionnaire included the differences of trust in automated driving between the "unfamiliar with automated driving" and "familiar with automated driving". We could draw the conclusion that more knowledge on the subject in this case increased trust in new technology. However, since we didn't have access to actual experts, the possible opinion gap between "familiar" and "expert" was not explored.

The biggest issues that caused distrust in automated driving among the respon-

dents of the questionnaire were possible manufacturing or design errors that could cause the vehicle to malfunction, as well as the vehicle's behaviour in different scenarios. These were both mentioned in different literature as well. Unemployment of professional drivers and potentially higher costs, meaning possible societal imbalance that may arise from it, were not considered big sources of not trusting automated driving among the respondents.

Methods of increasing trust varied between different groups. However, thorough testing, demonstration of abilities, and documentation was considered to be the biggest improving factor of trust. Better knowledge on automated vehicles was very popular among those that were unfamiliar with automated driving, and half of the respondts that said they were already familiar said they would like to know more about automated vehicles in order to improve their trust in automated driving. Manufacturers' reputation did not play in important role in the eyes of the respondents.

The last research question "Possible difficulties with implementing trust increasing methods in automated driving?" was answered through a comprehensive literature review. Technical aspects, as well as a lack of resources were some of the reasons that could hinder implementing different methods of improving trust. Lack of legislation and standardization were also determined to be relevant reasons that could hold back implementing trust improving methods, as well as the sheer complexity of vehicle's and automated driving systems.

The most important aspect however should not be forgotten. Losing human lives are not something that should not be taken lightly. The developers of automated driving systems carry a large burden on their shoulders. As society could learn to trust automated driving systems, the systems should also be worthy of that trust. Methods of improving safety and security of these vehicles should be a priority, and other vulnerable road users should be able to travel the roads feeling safe.

The research objectives of this thesis were fulfilled. The questionnaire had its limitations, but within those limitations this research was a success. A general idea of stakeholder's trust was collected, reasons for trust/distrusting were analysed, and improvements were collected, and suggested. Reasoning for the difficulty of implementation of certain methods was also provided. The limitations of the thesis leave room for plenty of further research. Different areas need to be researched a plenty before automated driving can become an everyday commodity.

Lähdeluettelo

[1] B. Schneier, *Liars and outliers*. John Wiley and Sons, Inc, 2012.

[2] M. Webster, "Trust", 2023.

[3] R. Hardin, *Trust*. Polity Press, 2006.

[4] S. Marsh and M. R. Dibben, "Trust, untrust, distrust and mistrust – an exploration of the dark(er) side", 2012.

[5] D. H. Mcknight and N. L. Chervany, "Trust and distrust definitions: One bite at a time", 2001.

[6] A. Hakkala, O. I. Heimo, S. Hyrynsalmi, and K. K. Kimppa, "Security, privacy'); drop table users; – and forced trust in the information age?", 2017.

[7] R. J. Lewicki and C. Wiethoff, "Trust, trust development, and trust repair", 2000.

[8] H. Aldowah, S. Ul Rehman, and I. Umar, "Trust in iot systems: A vision on the current issues, challenges, and recommended solutions", 2021.

[9] A. Koohang, C. S. Sargent, J. H. Nord, and J. Paliszkiewicz, "Internet of things (iot): From awareness to continued use", *International Journal of Information Management*, 2022. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0268401221001353`.

[10] F. Davis and F. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", 1989.

[11] L. Cai, K. F. Yuen, and X. Wang, "Explore public acceptance of autonomous buses: An integrated model of utaut, ttf and trust", 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214367X22001387.

[12] T. Koivumäki, A. Ristola, and M. Kesti, "The perceptions towards mobile services: An empirical analysis of the role of use facilitators", 2008. [Online]. Available: https://doi.org/10.1007/s00779-006-0128-x.

[13] E. Parliament and C. of the European Union, "General data protection regulation", 2016. [Online]. Available: https://tietosuoja.fi/gdpr.

[14] M. Barati, I. Petri, and O. F. Rana, "Developing gdpr compliant user data policies for internet of things", Association for Computing Machinery, 2019.

[15] D. George, K. Reutimann, and A. Tamò-Larrieux, "GDPR bypass by design? Transient processing of data under the GDPR", *International Data Privacy Law*, vol. 9, no. 4, pp. 285–298, 2019.

[16] S. of Automotive Engineers, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles", 2021.

[17] M. Wood, P. Robbel, M. Raass, and et. al., "Safety first for automated driving", 2019.

[18] W. Morales-Alvarez, O. Sipele, R. Léberon, H. H. Tadjine, and C. Olaverri-Monreal, "Automated driving: A literature review of the take over request in conditional automation", 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/12/2087.

[19] M. Wolf, "Security engineering for vehicular it systems", 2009.

[20] J. R. Perello-March, C. G. Burns, S. A. Birrell, R. Woodman, and M. T. Elliott, "Physiological measures of risk perception in highly automated driving", pp. 4811–4822, 2022.

[21] M. Li, B. E. Holthausen, R. E. Stuck, and B. N. Walker, "No risk no trust: Investigating perceived risk in highly automated driving", 2019. [Online]. Available: https://doi.org/10.1145/3342197.3344525.

[22] I. Y. Noy, D. Shinar, and W. J. Horrey, "Automated driving: Safety blind spots", pp. 68–78, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753517304198.

[23] I. O. for Standardization, "Safety of the intended functionality.", 2022. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:21448:ed-1:v1:en.

[24] K. Yoneda, N. Suganuma, R. Yanase, and M. Aldibaja, "Automated driving recognition technologies for adverse weather conditions", pp. 253–262, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0386111219301463.

[25] J. Rapp, J. Tachella, Y. Altmann, S. McLaughlin, and V. K. Goyal, "Advances in single-photon lidar for autonomous vehicles: Working principles, challenges, and recent advances", pp. 62–71, 2020.

[26] L. Westhofen, C. Neurohr, T. Koopmann, and et al., "Criticality metrics for automated driving: A review and suitability analysis of the state of the art.", 2023.

[27] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense", 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820304235.

[28] R. Jung and B. Wernerus, "Cybersecurity for automated vehicles", 2021.

[29] H.-J. e. a. Liao, "Intrusion detection system: A comprehensive review", 2013.

[30] I. Studnia and E. Alata, "A language-based intrusion detection approach for automotive embedded networks", 2018.

[31] G. Singh and Supriya, "A study on encryption algorithms (rsa, des, 3des and aes) for information security", 2013.

[32] I. O. for Standardization, "Road vehicles — cybersecurity engineering", 2021.

[33] L. Guo and J. Ye, "Cyber-physical security of electric vehicles with four motor drives", *IEEE Transactions on Power Electronics*, 2021.

[34] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, "Evaluation of can bus security challenges", 2020. [Online]. Available: `https://www.mdpi.com/1424-8220/20/8/2364`.

[35] S. Jin, J.-G. Chung, and Y. Xu, "Signature-based intrusion detection system (ids) for in-vehicle can bus network", in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2021.

[36] O. Vermesan, R. Bahr, M. Falcitelli, and et. al, "Iot technologies for connected and automated driving applications", 2020.

[37] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead", *Computer Networks*, vol. 76, pp. 146–164, 2015. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S1389128614003971`.

[38] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle", 2015.

[39] Z. Xiong, Z. Cai, Q. Han, A. Alrawais, and W. Li, "Adgan: Protect your location privacy in camera data of auto-driving vehicles", *IEEE Transactions on Industrial Informatics*, 2021.

[40] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks", *Transport Reviews*, pp. 103–128, 2019.

[41] J. J. Jones, J. Rabkin, and et. al, "Autonomous vehicles: Legal and regulatory developments in the united states", 2021.

[42] O. M. Lalude and N. J. Udombana, "Universality and particularity: Why universalism should be the standard for human rights", 2022.

[43] S. O. Hansson, M.-Ä. Belin, and B. Lundgre, "Self-driving vehicles—an ethical overview", 2021.

[44] A. Gupta, A. Anpalagan, L. Guan, and A. S. Khwaja, "Deep learning for object detection and scene perception in self-driving cars: Survey, challenges, and open issues", 2021. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S2590005621000059`.

[45] W. H. Dutton and A. Shepherd, "Trust in the internet as an experience technology", *Information, Communication & Society*, vol. 9, no. 4, pp. 433–451, 2006.

[46] V. Venkatesh, M. G. Morris, and et. al, "User acceptance of information technology: Toward a unified view", 2003.

[47] J.-B. Manchon, M. Bueno, and J. Navarro, "How the initial level of trust in automated driving impacts drivers' behaviour and early trust construction", *Transportation Research Part F: Traffic Psychology and Behaviour*, pp. 281–295, 2022. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S1369847822000249`.

[48] T. Zhang, D. Tao, X. Qu, X. Zhang, R. Lin, and W. Zhang, "The roles of initial trust and perceived risk in public's acceptance of automated vehicles", *Transportation Research Part C: Emerging Technologies*, pp. 207–220, 2019. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0968090X18308398`.