Autonomous Vehicles: A Convergence Between Informatics and Engineering

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)" im Studiengang Wirtschaftswissenschaften
der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: [redacted] Buschmann [redacted] Vorname: [redacted] René [redacted]

Prüfer: Michael Breitner

Hannover, den 30.08.2018

Table of Content

1. Introduction

The future trends of the automobile include drastic changes and new challenges as well as opportunities for the automotive industry. Considering the trends, the future vehicle is connected, electric and autonomous (cf. Jensen, Gruschka & Lüssem, 2016; p. 442). Due to large environmental issues and scandals in the automotive industry, a change in mobility is a logical step. As a most well known scandal of the industry the "diesel affair" of Volkswagen is especially noteworthy. This "exhaust scandal" includes the manipulation of emission values with a defeat device. Software in these manipulated vehicles is able to regulate the engine control during the official emission tests so that the emissions were reduced (cf. Zeit Online, 2015). Therefore, the automobile manufacturer is faced with high penalty payments and must rethink their strategy. An alternative is the change of mobility towards connected, electric and autonomous vehicles. While the technology for connected and electric vehicles is partly researched and launched, autonomous vehicles are still in the testing phase. There are different levels of automation from traditional cars with no automation to fully autonomous cars. In the vehicles with full automation, the human is only a passenger and the vehicle's system is responsible for the driving task during the whole time.
In the following thesis, the term "autonomous vehicles" is used synonymously for driverless vehicles, which have the highest automation level. Therefore, autonomous driving is a technology, which offers a broad range of possibilities for the mobility such as Shared Autonomous Vehicle Services (SAVS) or Highway Automation. The usage of autonomous vehicles for car sharing is possibly a solution for relocation problems of classic car sharing services (cf. Jorge & Correira, 2013; Wagner et al. 2015).
Nowadays autonomous driving is a strongly researched field and is interesting for different companies from different industries. Besides classic automobile manufacturers like Volkswagen, new manufacturers such as Tesla are breaking into the market. Furthermore, also IT and Internet companies have seen the high potential of the automotive. For example, Google and Apple are currently researching on autonomous vehicles and want to open up the vehicle as an important and lucrative platform, to generate personal data, new customers and sell new services. Furthermore, another incentive for the research is the prognosticated market volume. Referring to Statista (2017) the market volume is raising from 8 billion US Dollars in 2016 to 26 billion US Dollars in 2025.

The revolutionary case of fully autonomous vehicles offers a variety of advantages. The developments of these vehicles alter the mobility fundamentally and provide social, environmental and economic benefits. These include: Less accidents, reduction of emission and fuel consumption and a higher productivity as just some of the potential benefits (cf. Ernst & Reinelt, 2017; p. 1; Fagnant & Kockelman, 2015). Nevertheless, the development of autonomous vehicles is faced with many challenges and problems. Firstly, the acceptance, which is influenced by perceived driving enjoyment, perceived usefulness and perceived traffic safety, is low regarding autonomous vehicles. With reference to Solace (2018), 57% of connected car drivers would not buy a self-driving car even if money were not an issue. This

high share shows that the existing benefits of autonomous vehicles must be addressed. In addition, no fully autonomous vehicles are available and therefore no hands-on experience exists, which would probably increase the acceptance. Another challenge for the development of autonomous vehicles is the location and usage of different sensors. This sensor setup must ensure a reliable detection of movable and static obstacles even in poor lighting or weather conditions. Furthermore, solutions in case of power failure must be addressed and developed. Apart from the reliability of sensors, better solutions for the integration of informatics in the vehicle are necessary. Hereby, the main problem is the different lengths of time of software development and vehicle's development.
Although, major challenges of autonomous vehicles are in the field of IT security and data protection. Due to the connectivity with the environment (e.g. other vehicles, manufacturer backend, infrastructure and internet) and the high share of informatics and interfaces, "it is easy to imagine that, in the not-so-distant future, malicious hackers could cause traffic accidents by taking control of self-driving cars" (Lee, 2015; p. iv). If attackers get access into the vehicle's system a manipulation of security relevant functionalities is possible. At the level of full automation, the system is responsible for critical tasks like steering, braking or acceleration. Potential attacks have effects on the functional security of the vehicle and therefore on the life of the passengers (cf. Krauß & Waidner, 2015; p. 383). In addition, the aspect of data protection offers problems and challenges. In conjunction with the mentioned connectivity, the future vehicle stores and processes high amounts of personal data. This personal data, which is stored in the vehicle and transferred between different agents must be secured and protected for unauthorised accesses and manipulation. The volume of data allows conclusions on movement patterns, personality profiles, driving behaviour or the current location (cf. Krauß & Waidner, 2015; p. 383; Jensen, Gruschka & Lüssem, 2016; p. 448-449). However, autonomous vehicles depend on information of the sensors and their environment to ensure reliable vehicle guidance.

Besides the challenges on IT security, the resulting conflict of the data processing and storing is an interesting area of research.
Therefore, the central research issue of this thesis is:

> *How and why does the development of autonomous vehicles change the requirements for IT security and data protection?*

Another part of this thesis outlines the influence of the development autonomous vehicles on the vehicle concept. Additionally, a short consideration of the reliability is placed.

2. Structure and Methodical Procedure

This chapter describes the structure and methodical procedure of this thesis.
Firstly, chapter 3 defines the 5 levels of automation and gives an overview of the status quo of autonomous driving. In addition, some Use-Cases are presented and the Vehicle-to-everything (V2X) communication is considered. Later on in this chapter development circles are

Besides anonymisation, data minimisation is also included in the German Federal Data Protection Act to improve the data protection (cf. Recht, 2014). Data minimisation recommends a minimisation of collected personal data. In conjunction with data minimisation, the purpose of the storage and generation of data is also important (cf. Jensen, Gruschka & Lüssem, 2016; p. 452; Spaar, 2016; Recht, 2014; § 3a).
Regarding the different lengths between the development cycles of software and vehicles, it is recommended to adapt the vehicles development to the informatics development and to harmonise these cycles. Developing and adapting ECUs, which can realise new functionalities in the short term, can also improve the integration of informatics into the vehicle (cf. Expert Interview, Appendix C, p. VIII).
Also the reliability of sensors is improvable with more testing. Therefore, the development of sensors must be much more cost-efficient and democratised. Though, the detection can be improved by supporting sensors by V2X communication and infrastructure. The environment plays an important role to generate further information (cf. Expert Interview, Appendix C, p. VIII; Appendix D, p. XII). Referring to Van Brummelen et al. (2018), improving the detection and reducing uncertainty in poor lighting and weather conditions is necessary. Also the reduction of uncertainty in sensor data by cross-verifying obstacle locations and signals are recommended. More sensors and sources, further development of sensors and V2X communication can reduce this uncertainty. Another aspect of Van Brummelen et al. (2018) is to decrease the cost of autonomous vehicle sensor systems by further developing of sensor fusion algorithms using low-cost sensors or the usage of new low-cost and much more effective sensors.
Finally, an adaption of the regulative framework is required. The politics must design regulations with defined roles and responsibilities. Currently the focus of the framework is on the human. In case of full automation, the human only acts as a passenger and the system is responsible for the driving task. Therefore, a shift of the liability toward the manufacturer or service provider is possible and recommended.

After the recommendations, which are based on external sources and the expert interviews, the next chapter summarise the main aspects and provides a short outlook of future research.

9. Conclusion and Outlook

Summarising the main aspects regarding the research issue reveal the challenges of connected and autonomous vehicles. How and why does the development of autonomous vehicles change the requirements for IT security and data protection is the central point. Firstly, this connectivity poses the problem that the vehicle is connected with other vehicles, the manufacturer and other agents through a variety of interfaces. Furthermore, these connections are wireless as well as tethered. Ensuring this connectivity, different gateways and ECUs inside the vehicle is necessary. Nowadays, ECUs themselves, wireless interfaces (Wi-Fi, Bluetooth) and OBD interfaces do not offer strong safety precautions. Therefore, the vehicle's board network communication does not have a strong security standard (cf. Krauß & Waidner, 2016; p. 383-385). The characteristic of autonomous vehicles is that the system is

responsible for driving tasks. These security-critical systems are potential points of attacks. In case of an attack on these systems, the functional security and the humans' life are in danger. Improving the IT security of autonomous vehicles, a new Mind-Setting regarding the vehicle's development is required. The approach of Security by Design, which includes that IT security be already considered in the conception phase, is a potential solution. In addition, the identification, evaluation and solving of IT risks must be placed during the development phase. Additionally, the separation of security-critical systems (e.g. steering and braking) and other tasks (e.g. infotainment, navigation) is recommended (cf. Vereinigung der Bayerischen Wirtschaft, 2018; p. 1; Expert Interview, Appendix D, p. XIII). Finally, the exchange of data, which is stored in large quantities, must be secured with end-to-end encryption. This exchange between vehicles, manufacturers, service providers and other agents needs a high security standard. Concluding the IT security issue, general and standardised regulations of security standards must be clarified by law.

The next point of the central research issue is the data protection. Due to the high amount of collected data in autonomous vehicles, conclusions regarding driving behaviour, movement patterns and personality profiles are possible (cf. Krauß & Waidner, 2015; p. 383, 385; Jensen, Gruschka & Lüssem, 2016; p. 441). Also the majority of stored data in autonomous vehicle is personalised and therefore required a high level of privacy. In particular autonomous vehicles rely on information about the vehicle's environment. To gather these data, different sensors detect obstacles and connected vehicles, which exchange data and maps, will increase the reliability. The transferred maps include information about moving and static objects. Therefore, personal data, which allows conclusions on movement patterns and personality profiles, is exchanged with wireless connections between different vehicles and manufacturers. The recommended approach of this issue is Privacy by Design that requires data protection as an essential part of each business model. Supporting this approach, Privacy by Default suggests a default setting, which supports and ensures data privacy, is advantageous (cf. Vereinigung der Bayerischen Wirtschaft, 2018; p. 12; Krauß & Waidner, 2015; p. 387). In addition to that, transparency, self-determination and data security can ensure data protection in autonomous vehicles. Transparency includes the aspect that drivers and passengers are informed about stored data in its car. The self-determination has the permission of passengers regarding data storing and processing as a main requirement. Finally, data security is about the separation of security relevant systems and other applications (cf. VDA, 2014).

Besides the main components of the thesis, the IT security and data protection, also the changes and influences on the vehicle concept are noteworthy. The high share of informatics in autonomous vehicles is facing the car manufacturers with challenges of integrating software and IT systems in the vehicle concept. A major problem is the different lengths of software and vehicle development. While the vehicle development of Volkswagen is finished after 4 years, software is launched nearly every month. This inflexibility outlines a big problem, because short-term changes are pose a threat. Therefore, a harmonisation of these two development cycles is necessary. In addition, the development and adaption of ECUs, which are able to realise new functionalities at short term, can improve the integration of informatics into the vehicle (Expert Interview, Appendix C, p. VIII).

Another finding of the thesis is the required reliability of the sensors in autonomous vehicles, which must provide a maximum level of traffic security. The sensor setup must ensure a detection of movable and static obstacles at bad lighting and weather conditions. The worst case, power failure, must be secured and compensated. A vehicle with two different vehicle electrical systems, two batteries and separate ECUs is a potential solution (cf. Expert Interview, Appendix C, p. IX). The reliability and traffic safety plays a crucial role regarding the autonomous vehicle acceptance. As a main component of the needed acceptance of autonomous vehicles, this aspect is necessary for a successful launch of autonomous vehicles in the future.

For the further research in the field of autonomous vehicles, a consideration of the Use-Case, which will prevail on the market in the long term, is interesting. A specific analysis of problems, risks and challenges of each Use-Case is also interesting. This analysis should include acceptance as a main point. Also the time, when the first autonomous vehicle is launched for the public, is not clear. In conjunction to the IT security and data protection, further research about issues and methods to ensure these aspects is necessary. Therefore, practical implications are possible after the launch of autonomous vehicles. Finally, the development of V2X communication in autonomous vehicles is an interesting point of view. Though, a crucial point will be the most efficient sensor setup, which guarantees the reliability of autonomous vehicles. A consideration of the costs, different setups and positioning is also a potential field for future research.