Paper ID EU-TP1129

State of the art analysis for Connected and Automated Driving within the SCOUT project

Devid Will[1*], Lutz Eckstein[2], Steven von Bargen[3], Tessa T. Taefi[3], Roland Galbas[4]
1. Institut für Kraftfahrzeuge, RWTH Aachen University, Steinbachstr. 7, 52074 Aachen, Germany, +49 241 80 25676, will@ika.rwth-aachen.de
2. Institut für Kraftfahrzeuge, RWTH Aachen University, Germany
3. NXP Semiconductors GmbH Germany, Tropowitzstrasse 20, 22529 Hamburg, Germany
4. Robert Bosch GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany

Abstract
This publication gives a short introduction and overview of the European project SCOUT and introduces a methodology for a holistic approach to record the state of the art in technical (vehicle and connectivity, human factors regarding physiologic and ergonomic level) and non-technical enablers (societal, economic, legal, regulatory and policy level) of connected and automated driving in Europe. The paper addresses beside the technical topics of environmental perception, E/E architecture, actuators and security, the state of the art of the legal framework in the context of connected and automated driving.

KEYWORDS:
Connected and Automated driving, State of the art analysis, Connectivity, Security, Legal

1. Introduction: Overview of the SCOUT project
Connected and Automated Driving (C&AD) is expected to significantly alter our mobility. Amongst the high expectations, there are societal benefits such as an increased traffic safety and reduced emissions at single vehicle level; on the individual level enhanced driver's comfort; and on the economic level new business models that are arising in various industry segments. In this highly dynamic and complex environment, the project SCOUT (Safe and Connected Automation in Road Transport) aims to develop viable pathways for the large-scale rollout of high-degree automated driving in Europe.

The project brings together the automotive, telecom and ICT industries in order to conceive use cases and business models that will best leverage the investments into technology development and infrastructure deployment. User needs and expectations as well as technical and non-technical gaps will be analyzed and the results will be condensed into a cross-sectorial roadmap. Figure 1 shows the overall structure of the project.

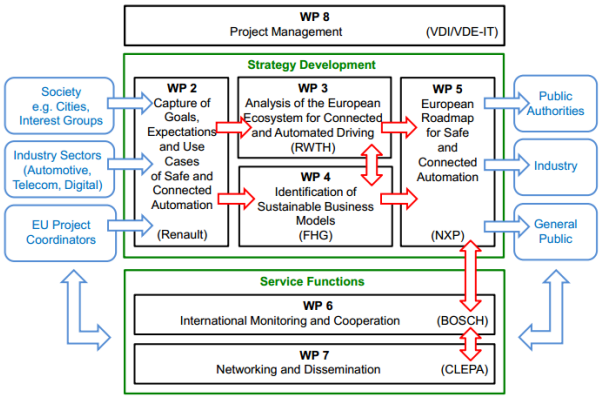


Figure 1: Structure of the SCOUT project

Work package 2 researches the essential expectations, ideas and goals, but also reservations of potential individual users and other relevant stakeholders towards automated driving. Based on this, ideas for solutions are collected in an open innovation process thereby identifying the potential use cases for automated passenger and goods transport. The overall goal of WP2 is to frame a comprehensive vision for connected and automated driving in Europe. WP3 evaluates the European ecosystem for C&AD by performing a state the art analysis (the focus of the paper) and then executing a gap analysis in comparison to the vision created in WP2. The goal of WP3 is to identify current and future gaps and challenges from technical, societal, economic, policy, legal and regulatory perspectives, in order to anticipate future development paths of the European ecosystem for C&AD. This supports the work on business models in WP4 and builds a thorough basis for defining a European roadmap for C&AD and deriving recommendations in WP5.

2. Methodology: State of the Art Analysis for Connected and Automated Driving

The field of C&AD impacts not only technology developments, but also various other domains, as reflected the 5-layer-model of Eckstein [1] on automated driving (Figure 2).

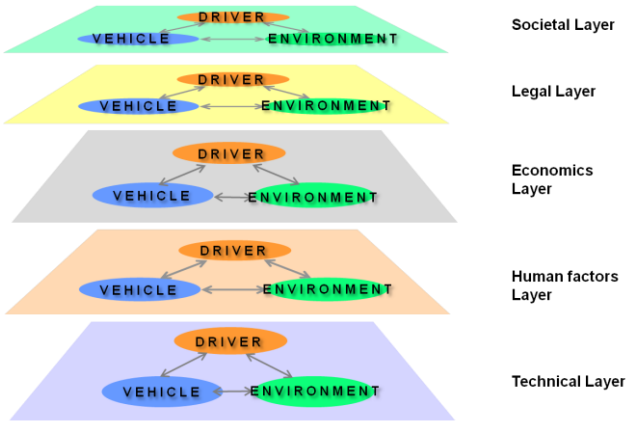


Figure 2: 5-layer model on Automated Driving [1]

The model contains the technical layer as a basis for C&AD functions. Four further layers enhance the model with mostly non-technical topics: a human factors layer; an economics layer; a legal layer; and a societal layer. In this publication, we focus the technical layer as an enabler for automated driving, as well as the legal layer. The technical layer is, as all others, subdivided into three main topics: the driver, the vehicle and the environment. These are the elements which interact all the time during driving (at least as long as the driver is in the vehicle) and the interaction needs special consideration during the development of automated driving functions. The data has been collected in desk-studies and workshops with stakeholders from the automotive supply chain in the first half year of 2017.

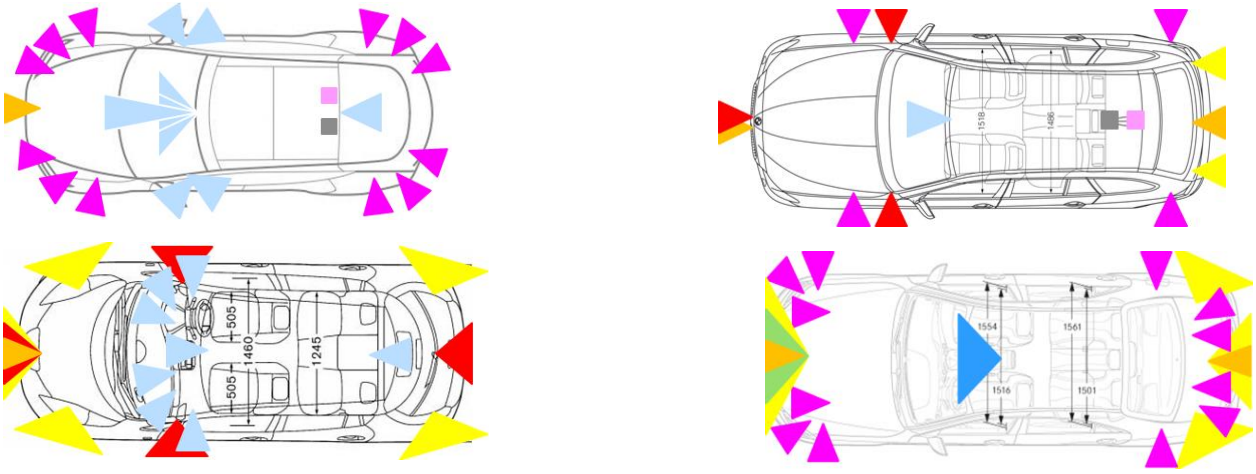
3. Results: Analysis of the state of the art enablers for connected and automated driving

The technical enablers are clustered into and discussed in the subsections perception; cognition and decision; actuation; and security. Additionally, the legal layer is discussed.

3.1 Perception

One main topic of research is the perception and understanding of the environment. Beside the choice of the sensor suite, the algorithms behind play an important role to achieve a sufficient safety level of environmental perception and prediction. The fully electric car manufacturer Tesla provides a new sensor suite in all new models consisting of eight surround cameras, twelve ultrasonic sensors and a forward facing radar processed on a new onboard computer by means of a neural net [2]. A different approach can be seen during Daimler's autonomous journey on the historical Bertha Benz Memorial Route, the S-Class S 500 Intelligent Drive was equipped additionally to the series sensor set with four short range radar sensors, two long range radars to the side, a wide-angle camera for traffic light recognition and one wide-angle camera to the rear for localization [3]. It is obvious that Daimler concentrates not only on vision sensors, but also uses long range and short range radar sensors also to achieve redundancy. Both companies are

not using laser scanners although they are extensively used in research vehicles and several start-ups are focusing on bringing them into the market. A very famous fleet of such research vehicles equipped with laser scanners was Google's autonomous driving fleet with several Lexus vehicles with a Velodyne HDL-64E on the roof of each vehicle. After Google stopped their self-driving car project, Google founded the company Waymo who still uses laser scanners for perception. The German OEM Audi announced that laser scanners are definitely needed for automated driving and they want to bring them into series production soon [4].
It is still under investigation which sensor suite is the best one for SAE level 3-5 functions. An additional difficulty is the unclear situation from the legal perspective. As long as the requirements (e.g. redundancy) are not finally defined, the final sensor suite might change over time. Figure 3 shows four examples of sensor suites which are used in production vehicles and concept vehicles (Tesla Model S (production), BMW 536i (concept) in the upper row, Nissan Leaf Pro-Pilot (concept), Mercedes S class (production) in the lower row).



Sensor Setup Examples			
Radar - Short Range	Radar - Long Range	GPS	Lidar / Laser
Camera - Mono	Camera – Stereo	V2X – Sensor	
Ultrasonic	Infrared	Maps	

Figure 3: Example of Sensor Setups

3.2 Cognition and decision making

The diversity of sensors around the vehicles presented in chapter 3.1, delivers various kind of information, but instead of single sensor sources it is essential to create a common, in the best case 360°-, representation of the environment to enable automated driving. This scene understanding (cognition) is the basis for the subsequent functional modules, namely behavior generation or decision making and trajectory planning. The whole central computing platform with its software modules which is necessary to realize this, can be understood as the brain of the self-driving car.

Since each single sensor source has its advantages and disadvantages, none of these sources can create a full understanding of the environment which leads to the necessity of a module which combines the single sources for automated driving. Therefore, the technique of sensor fusion is a well-established process to cancel out the weak points of several sensors by combining their information to gain a more robust detection with all necessary information.

Especially the fusion of cameras with distance measurement focused sensors like radar or LIDAR have a long history. This is done to not only detect obstacles and other road participants, but to also classify them beyond the capabilities of a single sensor. To do so, a fusion of the sensor sources is necessary. In general, this process takes the information gathered by two sources and a detection selection method (for example based on the similarity of reported object positions) and then uses the individual information to enhance the overall quality of the positioning. Also, information only available from one sensor can be added to the fused object by using a specific combination method. Additionally, some approaches use a prediction of past detections to obtain an additional source and means for tracking objects. Two mostly used systems for this in the context of Connected and Automated Driving are Kalman-Filtering and Occupancy Grid Fusion.

For the creation of an environment model, the access to all sensors and in the best case the sensor information with the highest information depth available without filtering or deriving objects based on raw data.

The state-of-the-art with regard to E/E architecture and the communication between ECUs is mostly realized by a distributed approach. Each sensor has a dedicated ECU attached to it which is responsible for the signal processing of the sensor and creates higher level information for the actuators. An example would be an ACC system which is based on a radar sensor with a dedicated ECU which generates longitudinal commands (e.g. acceleration/deceleration) for the engine control unit based on the detection of the radar sensor. The raw information of this radar sensor is nowhere else available except the dedicated radar ECU.
Since for the development of a 360°-environment perception all sensors must be available at one place, the introduction of a central ECU seems to be indispensable. Figure 4 shows the shift from a distributed architecture to a centralized approach.

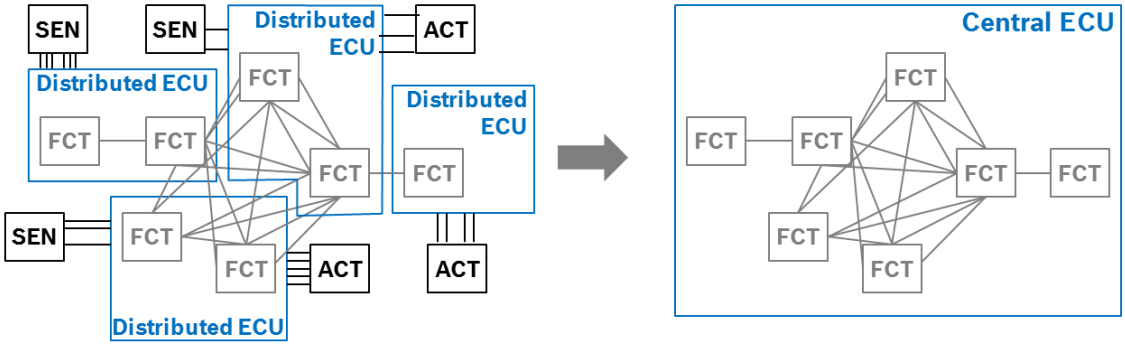


Figure 4: Distributed ECUs vs. Central ECU

Recently Audi introduced a central ECU following this motivation in the new Audi A8 called Audi zFAS. A centralized ECU with heterogenous hardware adapted to each processing task. All environment sensors (radar sensors, front camera, ultrasonic sensors) are directly connected to the zFAS and the environment representation is calculated here.[5] These central computing platforms have to deal with a massive and still increasing amount of data and therewith the need of increasing processing power is still there.

As soon as the environment is well-known and understood, the central vehicle brain of the automated vehicle is capable of making a decision based on this, i.e. choosing the next maneuver and planning a valid trajectory which is forwarded to the vehicle's actuators.

3.3 Actuation

Currently all scenarios for possible failures caused by the vehicle are using the driver as an observer and physical backup (Level 0-2 functions according to SAE levels). In case the driver does not conduct the driving task this assumption is not valid anymore. Depending on the level of automation the driver cannot take over the physical driving task fast enough or not at all.

- For common – not highly automated systems - the driver can take over the driving task. In this case the safety analysis typically could qualify the vehicle or a subsystem as “fail safe”. This is possible because in case of a malfunction of the vehicle the driver has the task to bring the vehicle into a minimum risk state. Example: In case of a malfunction of the brake booster, the driver has to enforce the missing braking power and bring the vehicle to a minimum risk state as fast as possible.
- For future - highly automated systems – the driver cannot be considered as mechanical backup. In this case the safety analysis requests the system to be “fail operational”. Thus - in case of a possible malfunction of the vehicle - the vehicle has to bring itself into a minimum risk state. Consequence out of this “fail operational” requirement: For certain possible malfunctions, e.g. a single point failure of a system, the vehicle has to cover a remaining driving task to ensure a minimum risk scenario.

The state of the art requirement for actuation systems is “fail safe” which leads to a “serial” dependency of actuation systems (braking and steering) and their supporting systems as power-net and data-processing-net.

Thus the state of the art of brake- and steering systems

- do not require functional redundancy in terms of using the ESP system to cover up the steering system within given constraints,
- do not have strong interdependencies concerning redundancy as e.g. multiple power net plugs for steering systems.

For future - highly automated systems all solutions applying redundancy to the systems and subsystems highly belong on the level of automation. All solutions will be carefully selected between concepts for functional redundancy and internal redundancy. The redundancy-distribution of the power-net and the data-system strongly depends on the concepts for braking and steering systems.
The given interference leads to a considerable complexity – especially because every kind of redundancy or even only changes cause additional costs.

3.4 Security

85% of vehicles are expected to be connected to the internet by 2020 with more than 50 vulnerable points opening the door for cybercrime [6]. Prominent examples are the “Jeep-Hack” and the "Tesla-Hack” [7], where researchers took over the remote control of a Tesla Model S to interfere with the brakes. These incidents show that functional safety needs to be supported by functional security in a connected vehicle.
A multi-layer security model should be considered on all layers of the vehicle’s architecture in the design process (“Security-by-Design”). The layers are the Interfaces, Gateway, Network and Processing. Adding Car Access as classical part of security, this model results in a 4+1 Layer Model (Figure 5). We briefly describe the available security solutions already in the market, or soon to be implemented for each layer.

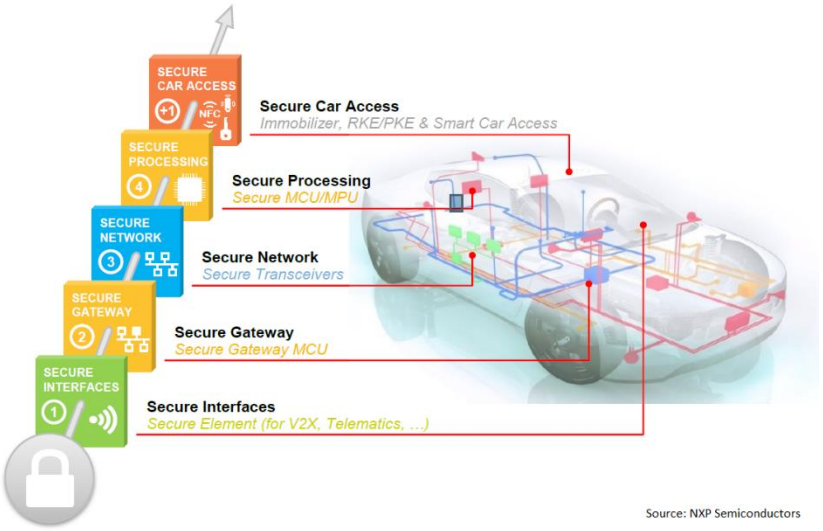


Figure 5: The 4+1 Layer Model for a Secure Connected Vehicle

Secure Interface: the external interfaces of the In-Vehicle-network (IVN), such as the Telematics Control Unit (TCU) or the On-Board Diagnostics port need to prevent unauthorized access. A strong M2M authentication can be implemented by attaching a Secure Element. These are dedicated security microcontrollers with advanced cryptographic accelerators and proven advanced physical and electrical attack resistance that can be used to establish an end-to-end secure channel to the external world. They also act as an ultra-secure vault for keys and certificates. To prove the level of security it is necessary to have 3rd party assessment and certification in the future, like e.g. Common Criteria EAL6+ or EMVCo.

Secure Gateway: A central gateway is needed to prevent attackers from getting access to the IVN once they hacked the interface (as in the “Jeep-Hack”). The gateway’s firewall separates the interfaces from the safety-critical IVN. The gateway includes accelerated crypto capability (HSM/SHE), bus monitoring, public key cryptography and a security software library for message authentication. The adoption rate of a central gateway in vehicles is around 20% today, with an expected increase to 50% by 2020.

Secure Network: One way to secure current CAN-based IVNs is to use secure transceivers. These secure transceivers can help containing spoofing attacks by monitoring and filtering messages based on their CAN ID. They can also help preventing denial-of-service attacks by applying rate limitation. A network-centric approach would be the economical upgrade path. By implementing such security features at the network level, inside the transceiver, security can be retrofit to existing networks with existing ECUs, while significantly reducing the amount of ECU software re-development.

Secure Processing means to ensure that the software running on the processor is genuine and trusted and has not been manipulated. Modern microcontrollers feature a secure boot and run-time integrity checking schemes using SHE and/or HSM. In addition, mechanisms for controlled lock-down of the MCU and ECU through manufacturing are employed to lock out debug and serial download features, which would be

invaluable to hackers. Further, a secure upgrade mechanism such as over the air updates are already state of the art in some OEM's. The security standard for OTA updates must be high, as an altered firmware could cause serious damage to a high number of vehicles at once.

Secure car access is the traditional part of security in a car. Traditional car keys and immobilizers helped preventing intruders from getting physical access to the car (esp. to prevent theft). Today, car keys feature Passive Keyless Entry (PKE), a feature that ensures that the car is locked and secured as soon as the driver exits and leaves the surrounding of the car. Soon, they will be equipped with even more additional features, for example to enable remote vehicle monitoring, or to enable car access via NFC or BLE with a mobile device like a smartphone or wearable.

3.5 Legal

European legislation on traffic in general is subject of the Vienna Convention (VC). It is the main legal basis for regulation in the EU and thus necessary to look at, regarding potential roadblocks for connected and automated driving (CAD) in Europe and what has already been done to enable it. Furthermore, national regulations regarding CAD and (cross-border) testing possibilities must also be considered to round off the picture. Besides the regulation for road traffic, other legal questions like e.g. liability, privacy, security or type approval must be solved.

A recent amendment of the VC enables a system taking control of the driver's task, e.g. automated steering up to 10 km/h for parking scenarios. It was incorporated in the Articles 8, 13 and 39 and was a first step to enable CAD to a certain extent. It states that the driver must have the possibility to override or switch the system off and the system that takes over driving duties has to fulfill certain technical requirements. Fully autonomous driving without a driver is not possible with this amendment.

The nearly 50 years old VC has several more roadblocks for CAD which are in particular:

- The definition of the driver (extension to include technical systems necessary) (Art. 1 v)
- The need of a driver to maintain permanent control of the vehicle (Article 8)
- Keeping a certain distance between two vehicles while driving (Article 13)
- The technical requirements of vehicles (Article 39)
- Regulation regarding the steering system (UN-R 79)

Especially the UN-R 79 needs an amendment, as it regulates the technical requirements for steering functions and prohibits most use cases of CAD including some ADAS functions. Amendments are already issued by several signatories (incl. the EU), but are not in effect yet. To cover all needed changes and guarantee a holistic approach that enables all facets of CAD, an amendment should be issued by the EU on behalf of all member states.

Considering the slow process to align regulations with the technical development of CAD, member states reacted by allowing Field Operational Tests (FOT) and amended their national legislations accordingly. Extensive FOT in Europe are e.g. the "European Truck Platooning Challenge" [8] or "Drive Me" [9] in Sweden. Some member states like e.g. Germany [10] also prepared their law for future possible changes by allowing higher levels of CAD if the VC allows it as well and open the door for special approval under Art 20 of Directive 2007/46/EC.

Besides road regulation some other topics need attention too. Foremost, it's the question of liability and consequently insurance systems. With driving tasks being transferred from the driver to the system (in different shaping over the development-cycle) the question who should be liable in case of an accident is arising. The question is a hot topic, discussed by policy makers, academia and other stakeholders. This question has the potential to become a major barrier for CAD until it is solved. Other topics are privacy and data protection, with forecasts assuming a production of up to 25GB of mostly private data per car per hour. Furthermore, functional security will be needed to ensure functional safety for CAD. With lives at risk, security must have a high standard like safety already has with ISO 26262. EU-Directive 2007/46/EC which regulates the type approval of cars will very likely also need a revision to adapt to the technical development of CAD. Other (national) regulations to be assessed do concern e.g. driving licenses or maintenance.

4. Conclusion

During the state of the art analysis in the field of connected and automated driving within the context of the project SCOUT, it became obvious that there are still great research needs in each module of connected and automated driving and also pending decisions of the legislation. Today there is no approval plan available which deals as a guide for market introduction of connected and automated vehicles higher than SAE level 2. But also for the technical side, there needs to be funded research and development to solve the various problems and answer all open questions. As one example, the transition from “fail-safe” components and architectures to “fail-operational” vehicles, is a huge step, which needs to be solved before connected and automated driving in higher automation levels (> SAE level 2) is possible.

Overall it can be stated that with vehicles transforming into automated and connected vehicles, a new era in terms of complexity and connectivity is dawning. These vehicles are even more vulnerable to new kind of (cyber-)threats from the outside, which already exists today, as shown by several hacks in the near past. These hacks indicate that security is often still an afterthought – something that must change, especially in the light of the wireless connectivity that opens new entries for hackers into the vehicle networks. There won’t be functional safety without functional (cyber-)security for the connected car. The increasingly complex software to secure a car needs a matching hardware as a trust anchor. Therefore, the car of the future needs security-by-design – next to the existing safety-by-design. With some technologies being already available and state of the art, the complete design of vehicle security still needs to be implemented.

The idea of connected and automated driving is triggered since some years, but there is still a lot of time and research needed to introduce the technology in mass market products.

References

1. Eckstein, L. (2016). *Safety Assurance – Developing and Assessing Automated Driving,* In Proceedings of *Automated Vehicles Symposium 2016,* San Francisco. AUVSI and TRB.
2. Tesla (2016). *Autopilot – New Autopilot Hardware,* webpage: *https://www.tesla.com/de_DE/presskit,* visited on 14th January 2017.
3. Ziegler, J., Dang, T., Franke, U., Lategahn, H., Bender, P., Schreiber, M., Strauss, T., Appenrodt, N., Keller, C., Kaus, E., Stiller, C., Herrtwich, R, et al. (2014). *Making Bertha Drive – An Autonomous Journey on a Historic Route*, IEEE Intelligent Transportation Systems Magazine, vol. 6, no.2, pp. 8-20, 2014.
4. Audi AG (2016). *Laserscanner ebnet Weg zum pilotierten Fahren*, webpage: http://blog.audi.de/2016/09/14/audi-bringt-den-laserscanner-in-serie/, visited on 14th January 2017.
5. Audi AG (2017). *Der neue Audi A8: Zukunft der Luxusklasse*, Barcelona/Ingolstadt.
6. Cybersecurity in the automotive industry”, Frost & Sullivan, October 2014 (NE30-18).
7. https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes; https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
8. Dutch Ministry of Infrastructure and the Environment et. al., https://www.eutruckplatooning.com/, visited on 11th August 2017.
9. http://nordic.businessinsider.com/volvo-just-launched-the-worlds-most-ambitious-autonomous-driving-trial-in-gothenburg-2017-1, visited on 11th August 2017.
10. http://europe.autonews.com/article/20170515/ANE/170519866/german-industry-welcomes-self-driving-vehicles-law, visited on 11th August 2017.