



Challenges for Periodic Technical Inspections of Intelligent Cars

Mona Gierl

Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
mona.gierl@h-ka.de 

Felix Müller

Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
felix.mueller@h-ka.de 

Reiner Kriesten

Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
reiner.kriesten@h-ka.de

Philipp Nenninger

Institute of Energy Efficient Mobility
University of Applied Sciences
Karlsruhe, Germany
philipp.nenninger@h-ka.de

Eric Sax

Institute for Information Processing Technologies
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
eric.sax@kit.edu

Abstract—The periodic technical inspection is a regulatory measure to ensure road safety and environmental sustainability during the operation of vehicles. It contains a non-destructive visual and impact assessment of its systems and components. With the advancement of autonomous and connected cars, new technologies, growing number of sensors, and new electrical/electronic-architecture designs find their way into the vehicle, which implies new challenges for the evaluation of road safety and environmental sustainability. In this paper, the need for advanced inspection methods due to upcoming new technologies enabling autonomous driving is investigated. A brief background about ongoing research and regulations addressing the verification and validation of autonomous and connected cars is given. The current procedure of periodic technical inspections in Germany is summarized and prospect challenges - addressing both, advancing technologies for autonomous vehicles and cyber security considerations of connected cars - are identified. Based on the listed challenges, possible improvements are derived, which should serve as a reference work to upcoming discussion about the extent of Periodic Technical Inspections (PTI) for autonomous cars.

Keywords—periodic technical inspection, security, autonomous driving, homologation.

I. INTRODUCTION

As of today, human fault is still the main reason for accidents [1], whereas the advances in technology enable enhanced safety features leading to autonomous, connected vehicles. With the introduction and application of Advanced Driver Assistance Systems (ADAS) and connectivity features (as Car2X) the automotive industry provides intelligent vehicles as a solution for improved road safety.

Prospective vehicles are expected to have 20 times more computational power [2] and to be running on 100 million lines of code [3]. Thus, the technical advances come with an increase in sensor systems to reconstruct the surroundings and a growing number of software solutions which require a higher amount of data and computational effort. One side effect is the growing complexity which might lead to additional

unwanted technical errors. Thus, it is common consensus to apply functional safety and cyber security standards during the development as well as testing throughout the development process and afterwards.

Beside verification and validation activities during development by the Original Equipment Manufacturers (OEMs), the vehicle has to be approved by an accredited authority to get road admission. This allows for an independent analysis on the car's roadworthiness and environmental sustainability across various types and models. Further, road admission depends on the condition of the vehicle which is regularly checked through mandatory periodic technical inspections which, e.g., occur every 2-3 years for passenger cars in Germany [4].

a) Problem statement: Mandatory technical inspections review the roadworthiness of vehicles and probe compliance with national environmental sustainability regulations. Regulatory standards (e.g., Regulation (EU) 2018/858 [7], Directive 2014/45/EU [8], etc.) prescribe a minimum set of required test procedures to show compliance to these regulations. With the advance of autonomous vehicles, a growing number of electronic systems (cameras, RADAR, LIDAR, etc.) are added as common equipment and enable the car to drive autonomously which simultaneously leads to a higher number of safety relevant systems. Consequently, an adaptation from the current mandatory test procedures is required.

b) Contribution: In this paper, current efforts to establish new test procedures for technical inspections are briefly highlighted and upcoming challenges due to the advances of intelligent vehicles are presented. In addition, current test procedures of passenger cars in Germany are summarized and potential improvements for periodic technical inspections based on the listed challenges are elaborated.

c) Classification of driving automation: In the field of autonomous driving, the SAE J3016 Standard defines six levels of automation [5]:

- Level 0 - No automation

- Level 1 - Driver assistance
- Level 2 - Partial automation
- Level 3 - Conditional automation
- Level 4 - High automation
- Level 5 - Full automation

From Levels 0-2 the driver is considered as driving but might be supported by assistance features whereas from Levels 3-5 the driver is not considered to drive even if seated in the “driver’s seat”. These levels are important for the classification within this work as Level 3 or higher levels of driving autonomy features are considered to challenge future technical inspections.

d) *Paper structure*: Section II provides the background on current verification and validation efforts for autonomous driving functions. Two essential efforts are highlighted, namely the PEGASUS project [6] and the United Nations Regulation UN R155 concerning the approval of vehicles with regards to cyber security [9]. Afterwards, the Periodic Technical Inspection (PTI) in Germany is presented to elaborate on the current mandatory road inspection methods. Based on the legal framework, Section IV derives upcoming challenges for technical inspections. To address the challenges, potential improvements are presented in Section V.

II. BACKGROUND

A first effort towards new verification and validation methods for autonomous driving functions has been made by the PEGASUS Project, which was concluded in 2019 [6]. It is a “Project for the Establishment of Generally Accepted quality criteria, tools and methods as well as Scenarios and Situations for the release of highly-automated driving functions” [6].

A second effort is currently made by the United Nations Economic Commission for Europe (UNECE). It developed “two new UN Regulations on Cybersecurity and Software Updates [...] which are the first ever internationally harmonized and binding norms in this area” [10].

A. PEGASUS

Pioneering the efforts in Germany to create a standard to test autonomous driving functions, in order to clear them for use in production vehicles on public roads, PEGASUS project created a method to assess the Level 3 function “Highway Pilot”. The idea was to define a process that can be used to validate such a system in order to green-light its use on public roads. Instead of driving thousands of kilometers on the roads (distance-based validation), a scenario-based testing approach is presented, which enables a systematic validation of the automated driving function. The result of this project was a possible approach consisting of the following five steps [6]:

- Definition of requirements
- Data processing
- Information storage and processing in a database
- Assessment of the highly automated driving function
- Argumentation

Starting with a collection of all the information available, the PEGASUS Method aims to define logical scenarios and reuses recorded test drives to create a pool of relevant scenarios to test the function. In parallel, the requirements to assess the driving function are defined.

In succession to these two steps, all the gathered information is transferred into databases, where the data can be accessed and augmented with information gathered in the later stages. Based on the scenarios, the parameters for the different test runs are generated as well as the corresponding pass / fail criteria.

After these steps, tests of the driving function are performed and evaluated in order to allow for the creation of a risk assessment. These tests can be performed in simulation, driving on proving grounds and in real traffic, depending on the concrete test. As a final step, the results are compared to the predefined safety argumentation and can be reused for the next test iteration. Based on the results of PEGASUS, new projects are underway, to use the results for the development of procedures for systems of Level 4 and 5.

B. Security Regulations for Type Approval

In 2021, the UNECE WP.29 working party published the regulation text “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber management system” (UN R155) [9], which is planned to be mandatory for all new vehicle types within the European Union as of July 2022 [10]. The UNECE WP.29 working party for Automated/Autonomous and Connected Vehicles (GRVA) is responsible for the harmonization of vehicle regulations and addresses autonomous and connected vehicles. The proposal is the first regulatory step demanding the integration of security processes and measures during the development of vehicles. As of 2022, there are currently 64 contracting parties including the European Union and others [11].

At the time the regulation takes effect, type approval with regard to cyber security is only granted to vehicle types that satisfy the requirements of the UN R155 regulation. The regulation differentiates between the responsibility of the manufacturer to implement a cyber security management system and the requirements for the approval of a vehicle type. Thus, according to the regulation text [9], the vehicle manufacturer shall provide evidence for:

- Requirements for the Cyber Security Management System (CSMS)
 - CSMS shall be applicable to the development, production and post-production phase
 - demonstrate processes to adequately identify and manage cybersecurity related risks
 - implement incident response capabilities within “a reasonable timeframe”
 - identify and manage supplier-related risks
- Requirements for vehicle types
 - the vehicle manufacturer shall evidence a compliant CSMS

- identify and manage supplier-related risks
- identify critical elements of the vehicle type by performing exhaustive risk assessment
- manage identified risks with proportionate countermeasures
- verify effectiveness of the security measures by performing appropriate and sufficient testing
- provide monitoring and forensic capabilities to enable attack analyses

The exact implementation measures are not defined as these are specified by each manufacturer, ideally through applying relevant standards (e.g., ISO/SAE 21434). Thus, a variety of different security measures is expected to be implemented for next generation vehicles which have to meet the cyber security regulation's requirements. From the perspective of approval authorities, new challenges arise as to define the evidence and test scenarios which prove roadworthiness to grant type approval.

Both projects, PEGASUS and the UN R155 security regulation, indicate significant effort being made to develop advanced test methods for autonomous and connected vehicles and show how current these topics are for the automotive industry. Thus, in our understanding, these efforts are the first steps done to advance test methods for type approvals of intelligent vehicles, however, further research is certainly required. Further, regular technical inspections are also challenged by the introduction of intelligent vehicles, but currently not yet addressed in funded research projects or within regulatory initiatives. Hence, as a first step to also address PTI, in the subsequent sections the present PTI procedure is presented and prospective challenges are outlined.

III. PERIODIC TECHNICAL INSPECTION IN GERMANY

In Germany, as in many other countries, it is mandatory to have your vehicle inspected at regular intervals to ensure its roadworthiness [4, Anlage VIII, 1.2.1]. Depending on the vehicle and its use, these intervals vary. For the purpose of this paper, a standard passenger car is assumed. The work is supposed to include other types of vehicles, but all examples will focus on passenger cars. Here, the usual interval is set to once every two years, after an initial period of three years for new cars, starting with the day of the first registration [4, Anlage VIII, 2.1.2.1.1].

A. Extent

To give a report on the roadworthiness, the technical inspection covers different characteristics of the presented vehicle. As stated in [4, Anlage VIIIa, 6], these include:

- Braking equipment
- Steering
- Visibility
- Photometric equipment and other parts of the electric installation
- Axles, wheels, tires, suspension
- Chassis, frame, platform, attached parts
- Other equipment

- Environmental impact
- Identification and classification of the vehicle

The focus is therefore placed mostly on the mechanical state of the vehicle. These parts are to be inspected visually, through a functional and performance evaluation of the vehicle and its parts, as well as by the reaction of the car and its systems to an action performed by the inspector [12, pp. 75]. The inspection is set up deliberately as described, to allow for the inspection to be performed in a similar manner across different makes and models of vehicles and to not depend on the specific functional implementation of a specific vehicle, but to also assess the performance of certain components or systems.

B. Procedure

The inspection itself does currently consist of multiple parts:

Registration for Inspection:

The Registration for Inspection is the first step, so that the car and its specific testcases are known to the person conducting the inspection.

Test Drive:

A short test drive is performed, in order to ensure that all control units in the car are booted up and operational.

Emissions Test:

For cars with internal combustion engine, the emissions of the car are to be checked before or during the periodic technical inspection, to ensure they are within an accepted range.

Brake Test:

During the brake test, a series of measurements are taken to ensure that the brakes are performing within the expected limits [4, Anlage VIIIa, 4.4]. Multiple ways are available to take these measurements.

Further inspection:

Inspection regarding the composition, condition, function and effect of its components and systems

During the subsequent vehicle inspection, the car is checked visually, manually and electronically while sitting on the shop floor and while lifted up [4, Anlage VIIIa, 4.3].

C. Results

As the ideal result for a PTI, a car passes all tests and is good to continue driving on public roads for the next two years. Having only minor defects (e.g., defective bulbs or scratched exterior mirrors), it is possible to allow the vehicle back on the road with the requirement to have them fixed as soon as possible. If there is one or more major or dangerous defects (e.g., impacting the brake functionality), the car has to be repaired and presented again. If the car is deemed a hazard on the road, the car can be decommissioned. In this most severe case, the car cannot be legally driven on the road. The results of each technical inspection is communicated to a centralized institution, the so called "Zentrale Stelle (FSD)" [13], to be aggregated and evaluated.

TABLE I

ESTIMATION OF THE DEVELOPMENT OF THE AUTOMOTIVE MARKET IN REGARDS TO THE DISTRIBUTION OF CARS SHOWN IN MILLION UNITS, GROUPED BY THE CAPABILITIES ACCORDING TO THE SAE-LEVEL [14].

Year	SAE Level						Robot vehicles
	0	1	2	3	4	5	
2015	59.3	24	8.2	0	0	0	0
2016	59.1	26.9	9.8	0	0	0	0
2017	58.2	28.4	10.9	0	0	0	0
2018	55.7	29.9	11.9	0.1	0	0	0
2019	51.8	33.1	13.4	0.6	0	0	0
2020	49	35.4	15.1	1.1	0	0	0
2021	46.5	37.9	16.5	1.7	0	0	0
2022	42.8	40.2	18.5	2.6	0	0	0.1
2023	41.1	42.5	20.8	2.7	0	0	0.1
2024	37.7	45.3	22.8	5.8	0	0	0.1
2025	35.3	47.4	25.2	7.6	0.1	0	0.2

IV. CHALLENGES FOR TECHNICAL INSPECTIONS

According to estimations of [14], the number of autonomous driving cars is expected to grow and first Level 4 cars are predicted for 2025 to be found on the road. Prospective vehicles are announced to have 20 times more computational power [2], whereas automotive software and sensors are expected to exhibit a 9 % for the software segment and 8 % for the sensors segment compound annual growth rate (CAGR) between 2020 and 2030 [15]. Further, [15] estimate an overall market size of USD 84 billion by 2030 for software development including OS, middleware, functional domains (powertrain, chassis, energy, body, etc.), connectivity and security. Considering these estimations, the following major challenges to impact future PTI were identified:

- Challenge I The condition of vehicle sensors is essential for autonomous driving, thus new test scenarios are required to test the growing number of safety-relevant sensors.
- Challenge II Growing complexity of data to be processed and software which is prone to unintended technical faults.
- Challenge III Vehicle data might not be accessible but is essential for demonstration of roadworthiness.
- Challenge IV Security measures require validation methods that enable inspection engineers to evaluate the roadworthiness.
- Challenge V The composition of software and hardware determines the correct operation of the vehicle system, thus the detection of any unauthorized modifications (e.g., firmware alteration, etc.) is necessary.

V. IMPROVEMENTS FOR THE PERIODIC TECHNICAL INSPECTION (PTI)

With regard to new features in cars, specifically regarding connectivity and autonomous driving, the PTI has to keep up in order to fulfill its intended role to ensure the safety of the

different road users from a technical standpoint. Therefore, the subsequent ideas are proposed as an addition to the PTI to also address security and autonomous driving capabilities.

According to [4, Anlage VIIIa, 4.], the vehicle components and systems shall be examined for their composition, condition, function and effectiveness. As a result, Table II summarizes the proposed improvements based on the defined regulation's categorization.

A. To Inspect the Security of Vehicles

Security has the special characteristic that if it is running correctly, it should not be recognizable and it should not affect the driving functionalities of the car. Yet, the software also displays "aging effects" due to constantly new evolving attack methods that might allow bypassing implemented security measures. These aging effects are not identifiable by visual examination as it might be the case for mechanical components (e.g., braking pads, etc.). Instead, a regular threat and risk analysis for deployed vehicles as presented in [16] should be considered and could help to analyze the security condition of the vehicle.

Another challenge is the variety of integrated security measures - as the ISO/SAE 21434 aims to provide a security framework to facilitate security by design, it does not provide technology specific solutions. Each manufacturer has to integrate effective measures to protect their critical systems and functions adequately [10]. To prove effectiveness, security testing methods exist that aim to demonstrate both: a) the correct functioning of integrated security measures and b) a low risk for unintended or undefined system states that might provoke misbehavior. However, applying these test methods after the development phase, especially penetration testing, is not desired by manufacturers as the car is not able to differentiate between a hacker and a penetration tester. As a reaction the car might lock down affected electronic control units to protect its assets. To counter this worst-case, but to also be able to inspect the correct functioning and effect of the security measures for deployed vehicles, the approval authorities and OEMs should hold a dialogue on how to enable security testing techniques in a controlled environment including the PTI.

Lastly, lessons learned from the Information Technology (IT) domain show that securing assets is a race between attackers and security engineers, and that vulnerabilities or known attacks are valuable insights to improve the systems security. For this reason, a collection of all known vulnerabilities, similar to the Common Vulnerabilities and Exposures (CVE) database [17], would be beneficial for the automotive industry. First efforts are made by [18]–[20] but the main hindrance is still the strong competition between players in the automotive industry.

B. To Inspect the Operation of the Autonomous Driving Capabilities

In order to ensure the correct function of the autonomous driving system, different parts of the vehicle have to be

TABLE II

OVERVIEW OF THE CURRENT STATE OF THE PERIODIC TECHNICAL INSPECTION IN GERMANY AND THE PROPOSALS TO INCLUDE AN ASSESSMENT REGARDING THE SECURITY OF THE VEHICLE AND ITS AUTONOMOUS DRIVING FUNCTIONS.

Context	Composition	Condition	Function	Effectiveness
Current State	Assessment and identification of built-in parts and components	Assessment of wear and tear (aging, damage, corrosion, etc.)	Actuation of control devices (pedals, levers, switches, etc.) to assess whether the operation is correct in terms of time and function.	Measurement of a component or system for compliance with specified limit values
Security	Check hardware and software to correspond to the specifications of the OEM	Vulnerability analysis and/or threat and risk analysis to identify deprecated/missing security measures	Security testing and reading self-diagnosis results through OBD to monitor correct functioning	CSMS assessment and detection of unintended behavior
Autonomous Driving	Check hardware and software to correspond to the specifications of the OEM	Assessment of the current state of the sensor and actor systems required to perform the driving functions	On-Board-Diagnostic and inspection of the associated functions	Assessment of the performance of the sensors and actors required to perform the driving functions

checked. These include:

- the sensors detecting the surroundings,
- the actuators performing the driving function,
- the control units running the associated software and
- the software to perform the driving function itself.

Different parts of the driving system are subject to different kinds of problems during the daily use of the accordingly equipped vehicles. The hardware, for example, is aging from the moment the system is produced and the vehicle is leaving the assembly line. Therefore, the biggest differences between otherwise identical vehicles is the wear and tear the vehicle has been subjected to during its lifetime. Accidents, not properly performed repairs and just general misalignment can cause the autonomous driving system to malfunction. Therefore, it is proposed that a future PTI has to include a test of the sensor systems to ensure that they are detecting the surroundings, e.g., detecting the objects in the designated areas as well as locating them correctly. All major sensor systems used in the specific vehicle have to be inspected to ensure they are operating according their specifications.

In the same sense, the hardware to perform the driving function has to be inspected. This includes:

- steering,
- braking,
- acceleration and
- communication with other road users.

For the most part, the hardware of these systems is already part of the PTI today. The brakes, for example, are already tested for their performance (see Section III-B). In addition to these tests, triggering of these systems electronically via the driving function has to be tested, especially their capabilities to provide granular access to these functions.

The communication with other road users and infrastructure presents a special case. Nowadays, cars are getting more connected via Car2X communications aiming to enable the exchange of traffic information. In addition, the first visual and acoustic communication systems are getting mounted to luxury cars to enable an interaction with its surroundings [21]. These initiatives can also be seen as part of the autonomous driving systems and therefore have to be inspected during future PTI.

C. To Inspect the Security and the Autonomous Driving Capabilities

As software is essential for both fields of study, a process needs to be defined, which would allow a check for both research topics simultaneously, as that will streamline the inspection and helps to keep time and thus costs low. Therefore, the authors propose to implement a version control system that allows the verification of the installed software in the vehicle under test. Having this system in place allows checking for manipulation on the software side as well as for outdated software that might not include the latest traffic signs or rules and as a result would not be able to follow the latest traffic regulations. A first effort to identify type approval relevant software is done by [22].

As the software can nowadays massively alter the behavior of the car on the road, see for example [23], it is a necessity to have a suite of tests similar to the type approval of such a driver assistance system, to ensure correct functionality after the update has been installed. Such a system should be put in place for all systems which can alter the movement characteristics of the car under test. Having passed such a test scenario, key parameters, such as version identifier and checksums can be recorded in order to be able to match the installed software in the car with the list of approved versions.

VI. CONCLUSION

As of today, present regulations are adapted to enable autonomous cars to get road admission. The advancing technologies challenge these efforts which is the reason for research projects and developed amendments to existing regulations (see Section II). However, these efforts should also address PTI as these are responsible to regularly probe compliance over the life cycle of the vehicle until its decommission. The applied test procedures during a PTI have to adapt to upcoming technologies. Thus, new test methods have to be defined since an increase in autonomy leads to a growing number of safety relevant driving systems that have to be examined for possible technical failures due to wear, tear or tuning. The associated upcoming challenges were identified by the authors and listed in Section IV. Based on these challenges, improvements to address the safety and security of autonomous cars are proposed in Table II. This table was designed to match the current regulatory framework in Germany and elaborates improvements based on the categories: composition, condition, function and effectiveness. The provided information should serve as reference work to upcoming research and discussions about the extent of PTI. Thus, within future work, it is planned to identify evaluation methods for inspection engineers that enable an assessment of the roadworthiness of vehicles throughout their time of road admission. To address the challenges of intelligent vehicles, both advanced sensor systems and continuous security activities need to be considered.

ACKNOWLEDGEMENT

The work presented in this paper was funded by GTÜ Gesellschaft für technische Überwachung mbH in Stuttgart, Germany.

REFERENCES

- [1] Statistisches Bundesamt, "Fehlverhalten der Fahrzeugführer bei Unfällen mit Personenschaden" (Misconduct of drivers in accidents with personal injury), July 2020, online, <https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/Tabellen/fehlverhalten-fahrzeugfuehrer.html>, retrieved: April 2022.
- [2] Automotive World, "The new BMW iX xDrive40 and new BMW iX xDrive50" , March 2021, online, <https://www.automotiveworld.com/news-releases/the-new-bmw-ix-xdrive40-and-new-bmw-ix-xdrive50/>, retrieved: April 2022.
- [3] R. Charette, "This Car Runs on Code", 2009, online, <https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>, retrieved: September 2020.
- [4] 2. Straßenverkehrs-Zulassungs-Ordnung (2nd road traffic licensing regulations), Version including revisions until 18 May 2017.
- [5] SAE International, "SAE J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles", 2018
- [6] PEGASUS Project, "Pegasus Method An Overview", online, <https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS-Gesamtmethode.pdf>, retrieved: March 2022.
- [7] European Parliament and European Council, "Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC", 2018, online, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0858>, retrieved: January 2022
- [8] European Parliament and European Council, "Directive 2014/45/EU of the European Parliament and of the Council of 3 April 2014 on periodic roadworthiness tests for motor vehicles and their trailers and repealing Directive 2009/40/EC Text with EEA relevance", 2014, online, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0045>, retrieved: January 2022
- [9] UNECE, "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system", March 2021, Revision 3, online, <https://unece.org/sites/default/files/2021-03/R155e.pdf>, retrieved: April 2022.
- [10] UNECE, "UN Regulation on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles", June 2020, online, <http://www.unece.org/?id=54667>, retrieved: April 2022.
- [11] UNECE, "Status of the 1958 Agreement (and of the annexed regulations)", online, <https://unece.org/status-1958-agreement-and-annexed-regulations>, retrieved: January 2022.
- [12] H. Braun, J. Bönninger, S. Missbach, and R. Süßbier: "Erkennen und Bewerten von Mängeln an elektronischen Systemen und Bauteilen im Kraftfahrzeug" (Detection and evaluation of defects in electronic systems and components in motor vehicles) Kirschbaum, Bonn, 2015. – ISBN 978–3–7812–1920–5
- [13] FSD, "Die FSD - Zentrale Stelle stellt sich vor" (The FSD - Central Office introduces itself), online, <https://fsd-web.de/>, retrieved: April 2022.
- [14] C. Malaquin: "Towards ADAS to Imaging radar for automotive market and technology trends", Microwave & RF Conference 2019.
- [15] McKinsey & Company, "Automotive software and electronics 2030 - Mapping the sector's future landscape", 2019, online, <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/mapping-the-automotive-software-and-electronics-landscape-through-2030>, retrieved: March 2022.
- [16] M. Gierl, R. Kriesten, P. Neugebauer, and E. Sax, "Reverse Threat Modeling: A Systematic Threat Identification Method for Deployed Vehicles", 18th International Conference on Scientific Computing (CSC 2020), Las Vegas, USA, 2020
- [17] MITRE Corporation, "CVE Security Vulnerability Database", online, <https://cve.mitre.org/>, retrieved: January 2022.
- [18] AUTO-ISAC, "Automotive Information Sharing and Analysis Center", online, <https://automotiveisac.com/>, retrieved: April 2022.
- [19] Upstream Security Ltd., "Autothreat Intelligence Cyber Incident Repository", online, <https://www.upstream.auto/research/automotive-cybersecurity/>, retrieved: March 2022.
- [20] M. Ring, J. Dürrwang, F. Sommer, and R. Kriesten, "Survey on vehicular attacks - building a vulnerability database", 2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Yokohama, 2015, pp. 208-212, doi: 10.1109/ICVES.2015.7396919
- [21] K. Groeneveld, "The F 015 Luxury in Motion at the Ars Electronica Festival in Linz: Creative break on the journey to the future", September 2015, online, <https://group-media.mercedes-benz.com/marsMediaSite/ko/en/9919078>, retrieved: April 2022.
- [22] UNECE, "Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system", March 2021, online, <https://unece.org/sites/default/files/2021-03/R156e.pdf>, retrieved: April 2022.
- [23] C. Dhabhar, "Tesla Model 3 Braking Improves With On-Air Software Update", May 2018, online, <https://www.carandbike.com/news/tesla-model-3-braking-improves-with-on-air-update-1859322>, retrieved: April 2022.