Testing of OTA-enabled functions in electronic control unit development

Benedikt Jooß[1], Julian Schuld[2], Matthias Enderle[3] & Prof. Dr.-Ing. Dr. h. c. Dieter Schramm[2]

[1] CARIAD SE, Germany
[2] University of Duisburg-Essen, Germany
[3] Dr. Ing. h.c. F. Porsche AG, Germany

Abstract: Over-the-air technologies and especially over-the-air-updates are important for car manufacturers to gain a competitive advantage and higher customer satisfaction. In the near future most of the new cars sold will be digitally connected. Not only the increasing number of new regulations all over the world, but also the growing complexity implies challenges for developers and testers to overcome. For testers these technologies require new test methods and guidelines for testing. Therefore, in this article, we want to present a method for the testing of OTA-update-enabled functions. During a requirements survey 7 regulations were identified and examined. More than 350 paragraphs were analyzed and broken down into 15 sets of requirements. These sets led to 19 test techniques. This is the basis for a framework in form of a test procedure model, which is based on the fundamental test process. The focus of this model is on the support of the steps “test planning”, “test analysis” and “test design”. The added value of the method lies, on the one hand, in the legal compliance and, on the other hand, in the framework provided for testers.

1 Introduction

According to a McKinsey study, 95% of all new cars sold by 2030 will be connected [1]. Michael Steiner (CTO of Dr. Ing. h.c. F. Porsche AG) also assumes that networking will become standard and bring a competitive advantage. In particular, he sees the ability of a manufacturer to bring new functionalities to the market in a short time as crucial [2].

The networking of vehicles with the environment poses many challenges for developers. For example, the source code of software items doubles on average every 42 months [3]. To achieve the speed mentioned by Michael Steiner, "over-the-air" (OTA) functionalities are particularly relevant for vehicle development. With the help of networking via the mobile phone interface in the vehicle, future oriented potentials for new business models are emerging: live diagnosis, predictive maintenance, swarm services through big data or software updates. Due to the new, complex functions, testing is also gaining in importance. Software testing accounts for 40 % of the development effort [4]. With the help of testing, the dangers and risks inherent in the new technologies are to be reduced and the strengths and opportunities achieved. These are compared in a SWOT analysis in Figure 1.

To be able to test efficiently, strategies and processes must be developed in advance. Therefore, the risks must be considered and incorporated into the processes. Targeted tests must address different risks. Additionally, intensive testing should ensure that all weaknesses are found. For example, testing can reduce the risk of a loss of use due to

errors during the update, or resource usage tests can check the utilization of systems or ECUs resources due to large amounts of data in advance. With this knowledge measures can be taken at an early stage of development to reduce the risks. Overall, testing is also about ensuring that the functionalities meet the requirements and their intended application to fully exploit the strengths and opportunities.

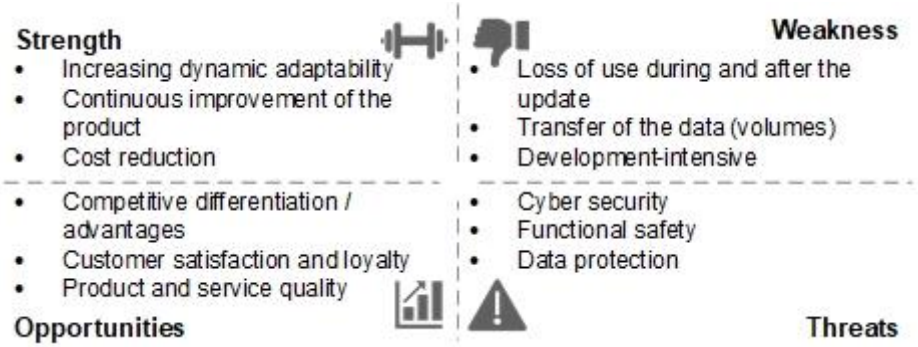

Figure 1: SWOT analysis on OTA functionalities that influences testing of OTA

Over-the-air is a collective term for all functionalities that take advantage of the networking of vehicles and receive or send data from a back-end. This includes many different functionalities with a wide variety of test efforts. This article focuses on over-the-air updates.

The aim of the method presented here is the identification and interpretation of requirements for testing of OTA-enabled functions and the development of a test process on that basis. Therefore, we present a method for testing OTA-update-enabled functions in this article. First, a schematically process for OTA-updates is shown. Then, a requirements survey and catalog are explained. This catalog builds the basis for the identification of test techniques necessary for testing OTA-update-enabled functions on different test levels. In addition, a test procedure model is presented that utilizes the test techniques for a generic test execution model. This model serves as input during different stages of the fundamental test process defined by the ISTQB [5]. To summarize the method, the added value of the approach is explained in detail.

2 Methodical Development Approach

2.1 OTA update process

A process of OTA-Updates, shown in Figure 2, is influenced by legal and technological requirements. The process can be split in three main parts: Creation, Distribution and Installation. The creation phase is the development of the update. First the necessity for an update of certain vehicles needs identification and second the software needs to be developed and tested. Various regulations specify how such a process can look like, for example UNECE Regulation 156 [6] or NHTSA Vehicle Cyber-security [7]. The transition between creation and distribution is the provision of the SW bundle. As cyber-security is a very important topic for vehicles, the provision needs several encryption and decryption mechanisms. These are applied before the start of the installation process.

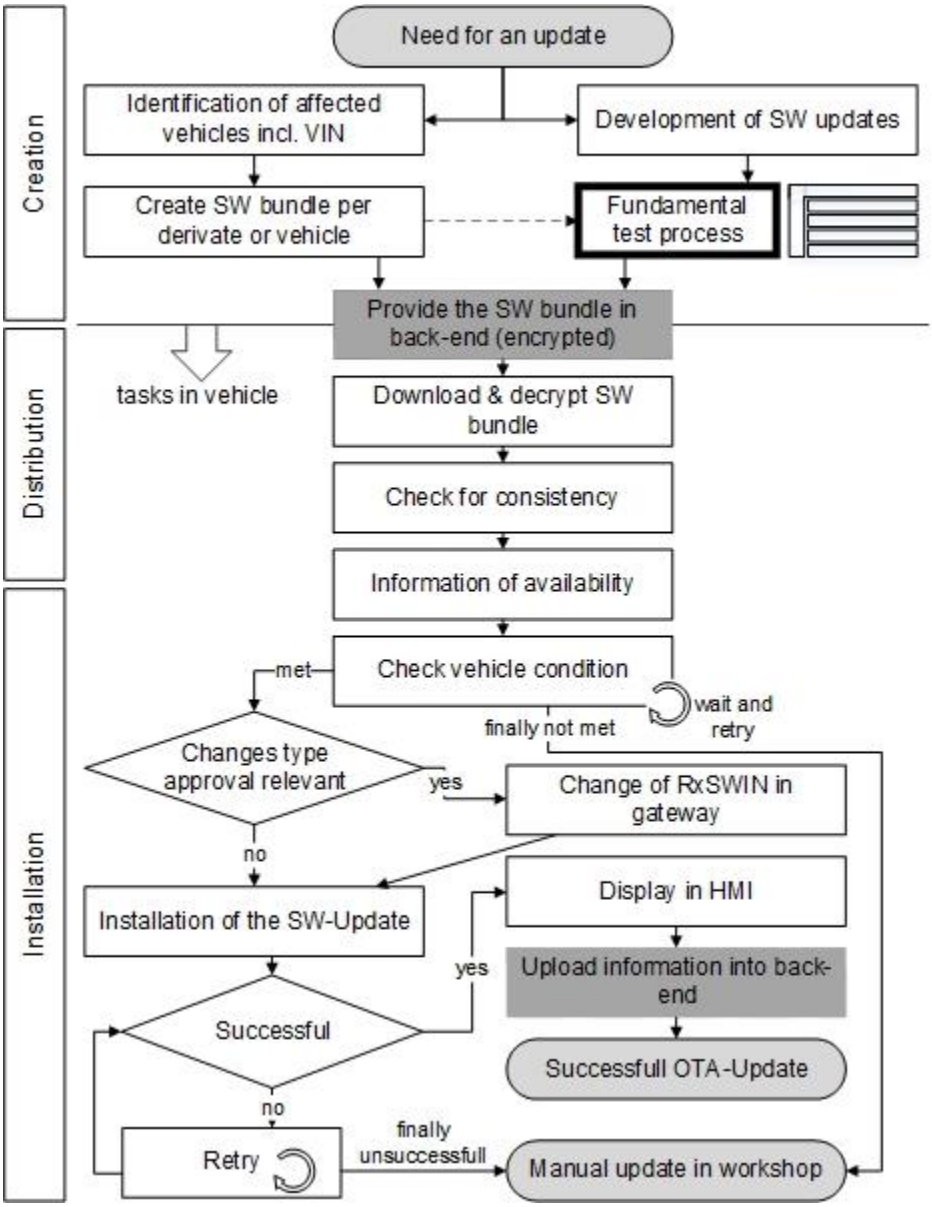

Figure 2: Schematical OTA-update process

The installation process is also influenced by several regulations e.g. UNECE R155 [8], the ISO 26262 [9] or the ISO/DIS 24089 [10]. In the first step several aspects need to be checked before the installation can start. Among other things the vehicle state needs to be in the required condition. If all preconditions are fulfilled, the installation can be initiated. When successful, the vehicle user will be informed, otherwise, after several retries, the update needs to be installed manually in a workshop.

The regulations do not only influence the OTA-update process, but also processes which are interwoven with it. This also includes the test process as can be seen in Figure 2. To ensure that these processes meet the requirements, the regulations must be known, analyzed and interpreted. In this paper, a methodological design for a requirements analysis and interpretation is developed and presented. This methods fits in a framework that is mostly based on the fundamental test process.

2.2 Requirements Survey

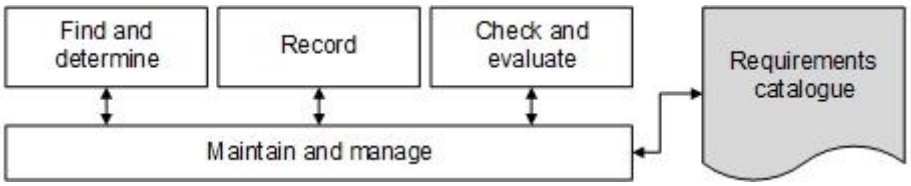

Figure 3: Methodical requirements management [12]

A test process for OTA-enabled functions needs to be based on corresponding requirements. These build the test basis, thus the foundation for the test condition, which is verified through at least one test case [11]. For the identification of the requirements a systematical requirements management method is used, see Figure 3. The first step is the identification of requirements. Considering the results from the SWOT analysis (Figure 1) the laws, standards and best practices listed in Table 1 were identified.

Table 1: Relevant regulations

Regulation	Title	Validity
AUTOSAR (CP R20-11) [13]	Requirements on Firmware Over-The-Air	International for all participating companies
GB201-5 [14]	General Technical Requirements for SW Updates of Vehicles	China
ISO/DIS 24089 [10]	Road vehicles – Software update engineering	International
ISO 26262 [9]	Road Vehicles – Functional Safety	International
NHTSA [7]	Cybersecurity Best Practices for Modern Vehicles	USA
UNECE R155 [8]	Cyber-security and Cyber-security Management System	Member states of the United Nations (EU)
UNECE R156 [6]	Software Update and Software Updates Management System	

Next is the documentation and subsequently the evaluation of the requirements. For this purpose, the regulations were broken down into their chapters, paragraphs and sections for a clear and comparable presentation. This ensures that for each aspect of the requirement, an evaluation can be determined regarding the significance for the testing of OTA functionalities. Experts of different fields were consulted for this assessment.

2.3 Requirements Catalogue

Based on this evaluation the requirements were categorized to generate a catalogue of requirements for the OTA-update test process. The broken-down aspects from the various laws, were summarized in terms of content. Thus, about 350 paragraphs were evaluated and merged into 15 sets of requirements. Pratley they were broken down in subsets. Overall, 25 single requirements emerged. Each set of requirements will be

tested on four different test levels: component test, integration test, system test and acceptance test. To prove that the requirement is met, at least one test technique is used. Aggregated, this forms the catalogue. An excerpt of the requirement sets and test techniques can be seen in Table 2.

Table 2: Catalogue of requirements and test techniques

<table>
<tr><th>ID</th><th colspan="2">Requirement</th><th colspan="2">Regulation</th></tr>
<tr><td rowspan="3">1</td><td colspan="2">Dependencies between the software update package on other systems and/or components must be analyzed</td><td colspan="2">UNECE R156: 7.1.1.5 / 7.1.1.10
ISO/DIS 24089: 6.3.2.3 / 8.3.3.3 / 9.3.2.8</td></tr>
<tr><td>Component test</td><td>Integration test</td><td>System test</td><td>Acceptance test</td></tr>
<tr><td>Interface Testing</td><td colspan="2">Interface Testing
Regression Testing</td><td>n/a</td></tr>
<tr><td rowspan="3">2</td><td colspan="2">Compatibility between update package and vehicle hardware must be ensured</td><td colspan="2">UNECE R156: 7.1.1.7.
AUTOSAR: RS_FOTA_00006
GB 201-5: 4.2.7.
ISO/DIS 24089: 9.3.3.10 / 8.3.3.2</td></tr>
<tr><td>Component test</td><td>Integration test</td><td>System test</td><td>Acceptance test</td></tr>
<tr><td>Technical review</td><td colspan="3">Non-functional testing of compatibility</td></tr>
<tr><td>3</td><td colspan="4">Rollback and restoration of the SW version</td></tr>
<tr><td rowspan="3">3.1</td><td colspan="2">It must be ensured, that the vehicle is in a safe state after a failed update</td><td colspan="2">UNECE R156: 7.2.2.1.1
GB 201-5: 4.4.4
ISO/DIS 24089: 6.3.5.1 / 9.3.3.8</td></tr>
<tr><td>Component test</td><td>Integration test</td><td>System test</td><td>Acceptance test</td></tr>
<tr><td>Fault-Injection</td><td>n/a</td><td>Fault-Injection</td><td>n/a</td></tr>
<tr><td rowspan="3">3.2</td><td colspan="2">ECUs must be able to restore the SW-Image, which was active before the last activation</td><td colspan="2">AUTOSAR:
RS_FOTA_CONSTR_00002
RS_FOTA_00013</td></tr>
<tr><td>Component test</td><td>Integration test</td><td>System test</td><td>Acceptance test</td></tr>
<tr><td colspan="3">Fault-Injection</td><td>n/a</td></tr>
<tr><td rowspan="3">3.3</td><td colspan="2">ECUs must be able to execute a rollback instruction received from the OTA master</td><td colspan="2">AUTOSAR: RS_FOTA_00006</td></tr>
<tr><td>Component test</td><td>Integration test</td><td>System test</td><td>Acceptance test</td></tr>
<tr><td>n/a</td><td colspan="2">Requirement-based Test
Fault-Injection</td><td>n/a</td></tr>
</table>

This excerpt gives an idea of the different test techniques which need to be considered for testing OTA-update-enabled functions. Theses, together with the model, code and other information, build the basis for the test analysis and test design phase. A total 19 test techniques were identified. In addition, the identified regulations also provide recommendations not directly linkable to a test technique or test case but are important for testing. They range from the management of other essential processes to the management of technologies such as cryptographic methods and are listed in Table 3.

Table 3: Further recommendations

Additional Processes	
Processes that accompany the test process must be established. Most important are project management, configuration management, change- and defect management.	ISO/DIS 24089: 4.3.5.4 / 9.3.5.1 / 4.3.5.7 / 5.3.3.1
Independent Testing	
To be objective, testers shall be independent of the development team to identify more failures.	NHTSA: G.14
Continuous monitoring and improvement of the CSMS	
A cyber-security monitoring system is needed. This needs ongoing improvement. The entire industry shall partition exercises against cyber-attacks.	UNECE R155: 7.2.2.4 NHTSA: G.14 ISO/DIS 24089: 4.3.2
Analysis of CS information + data protection rights	
Cyber-security threats and weak spots must be recognized by analyzing vehicle data. But it is important to consider data protection rights.	UNECE R155: 7.2.2.4 b) ISO/DIS 24089: 4.3.5.3
Testing of cryptographic modules	
Cryptographic modules must align with standards. If not, the usage must be justified and be protected from disclosure.	UNECE R156: 7.3.8 NHTSA: T.3
Usage of the latest communication protocol	
For communication the communication protocol “TSL” (Transport Layer Security) must be used.	GB 201-5: 5.1.9
Continuous optimization of integrity	
All data and mechanisms regarding OTA-updates must be state of the art.	NHTSA: T.22
Risk management for devices of suppliers in the system	
The risk for, devices provided by suppliers, must be reduced with appropriate protective measures.	NHTSA: G.39 / G.40

3 Application

3.1 Test Procedure Model

For successful testing, it is important to provide a usable framework. In the test analysis and design phase, a sequence is developed in which the test cases are to be executed. It can be evolved and adapted during the planning phase already. To support this, a test procedure is presented here that brings the test techniques into a flow process and considers possible interdependencies between them on the individual test levels.

Figure 4 shows a model of the schematical test procedure. The test levels are linked to the 19 test techniques, which are identified by the requirements catalogue (see Table 2). The layout of the individual test techniques also builds the order of the test execution. Those test techniques which are used on each test level and do not depend on the execution of other tests are listed on the lower part of the figure.

The fundamental test process was considered during the development of the model. It serves as an input for a test project in several phases of the process and should already be consulted during test planning in an early project phase. Through its use, test techniques and procedures can easily be planned. During the analysis and design phases this needs to be specified. Hence, the model is generalized the test techniques and procedures have to be tailored to the project. Abstract test cases are created within this step. Since the realization and execution phases are based on the steps, the model also serves as input in these phases - engineers can consult the model to ensure the correct setting of the tests and convert abstract test cases into concrete test cases.

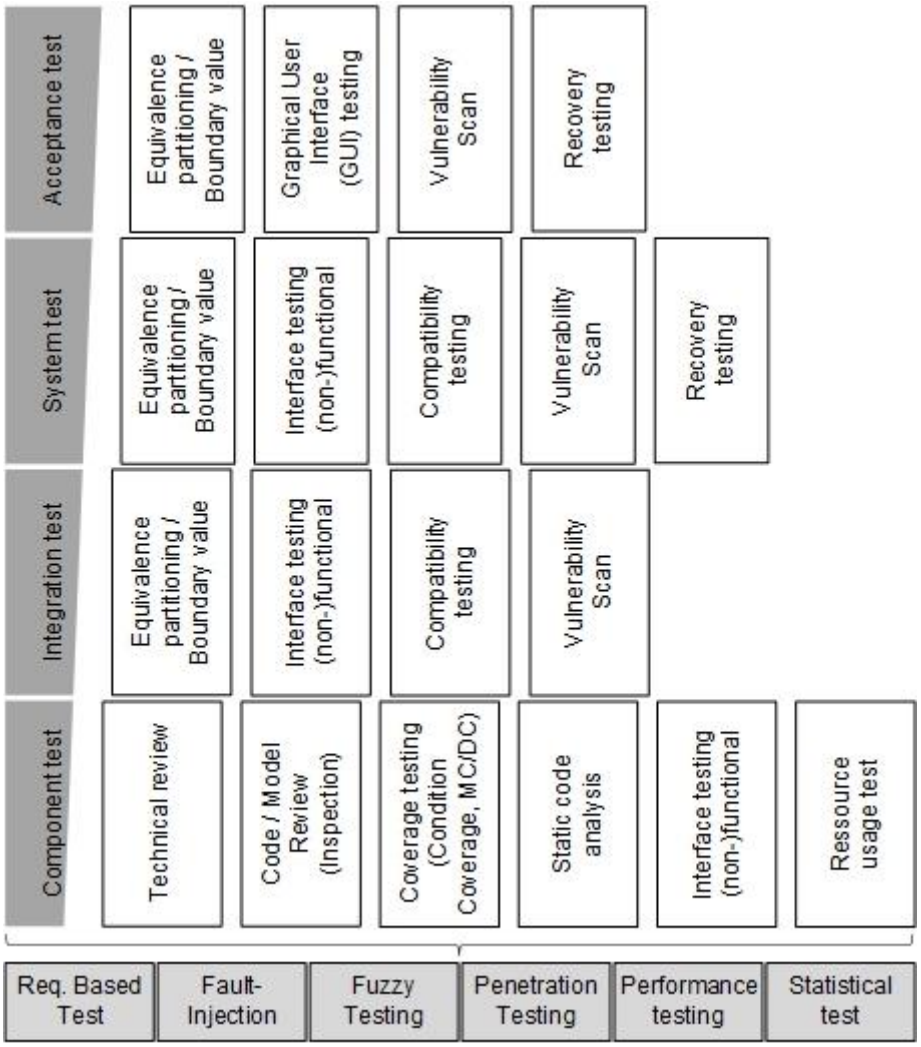

Figure 4: Schematical test procedure

3.2 Methodical Value

Testing of OTA-enabled functionalities is a complex yet increasingly important task. The test process for OTA-enabled functionalities is highly relevant for the entire automotive industry. Especially software updates over-the-air are subject to many regulations that have an impact on the type approval. For instance, the UNECE Regulation No. 156 underlines the need to establish an appropriate procedure for the

development and approval of such functionalities. Thus, it also influences testing procedures of OTA-enabled SW functions. In this paper a method for this purpose was introduced, that offers various added values for testers and developers.

Initially, the method serves as input for various steps of the fundamental test process and forms support to the tester. Beginning with test planning it is essential to define a test concept per test level. Within each test level, it is important to first define various quality characteristics that fit into the project context of over-the-air updates. These characteristics give indications on the quality level to be achieved, which is verified by testing. One part of the method is the definition of the test techniques. These are defined during test planning to ensure that the quality level can be proven. In addition, a generic test procedure was created, which also serves as input for test planning. A further part of the test concept is the resource plan. As the method specifies various test techniques, can be identified at an early stage. Subsequently the elements of the method serve as input for the test analysis and design phase of the test process. The requirements catalogue is analyzed together with other documents, e.g., the test object and design specifications. Based on the analysis and the techniques, provided by the method, the abstract test cases are specified, and the project specific test procedure is determined.

Secondly the method ensures legal compliance. The task of interpreting laws and standards is often left to the developer or a small group of developers. Since these are usually not legal experts, it is important to provide support and to define a uniform approach. By applying the method, testing of OTA-update-enabled functions is compliant with laws that impose requirements for the process. However, since laws are adapted over time it is important to establish a monitoring system that observers these changes and systematically (see section 02.3) includes them in the catalogue of requirements. Subsequently a continuous improvement of processes is indispensable for state-of-the-art testing.

4 Conclusion

OTA-update-enabled functionalities are important to gain competitive advantages and customer satisfaction. In the upcoming years vehicles will become increasingly connected with the environment. Such functionalities offer numerous strengths and opportunities. They can lead to cost reduction, dynamic adaptability of vehicles or service quality. For developing such functionalities new challenges must be considered. A major challenge is the doubling of code every 42 months. The resulting weaknesses and risks must not be ignored. Their existence must be identified at an early stage to be able to initiate measures to handle them. E.g. measures to reduce cybersecurity risks or to prevent the loss of use due to an update. These measures do have an impact on the development and on the testing of these functions. The challenges for testers are manifold. Not only does the large amount of code has to be tested, but evidence of different kinds must be provided, different regulations must be adhered, and different technologies must be considered. Therefore testing needs to be systematically.

In this article a method for testing of OTA-update-enabled functionalities is introduced, based on a requirements survey. Seven regulations were identified and systematically examined, by checking individual paragraphs for their relevance for testing. These paragraphs could be summarized to 15 sets of requirements, whereby three of the sets

being subsidized into 12 subsets. Each of these requirements lead to a test activity at component, integration, system and acceptance test level.

Next a generic test procedure model was developed to provide a framework for test managers. The model needs to be adjusted for each test project. Furthermore, six techniques were identified that are relevant for each level and have no interconnection between them. Therefore, they can be executed independent of the other techniques.

The method is designed to handle the challenges of testing OTA-enabled functions. The test techniques and the generic test procedure model serve as input in various steps of the fundamental test process. Especially during test planning, test analysis and test design. In this way, the quality of testing is ensured. Besides that, the method ensures the legal compliance of testing.

5 References

[1] McKinsey & Company, "Rewiring car electronics and software architecture for the 'Roaring 2020s'," 04 August 2021. [Online]. Available: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rewiring-car-electronics-and-software-architecture-for-the-roaring-2020s. [Accessed 30 January 2022].

[2] M. Steiner, "Porsche Newsroom," Dr. Ing. h.c. F. Porsche AG, 09 May 2019. [Online]. Available: https://newsroom.porsche.com/de/2019/digital/porsche-beteiligung-software-unternehmen-cetitec-entwicklung-digitalisierung-17568.html. [Accessed 30 January 2022].

[3] L. Hatton, D. Spinellis and M. van Genuchten, "The long-term growth rate of evolving software: Empirical results and implications," *Journal of Software: Evolution and Process,* 16 February 2017.

[4] B. Peischl and D. Wuksch, "Kosten- /Aufwandsabschätzung bei komplexen Software Projekten als Basis moderner IT-Governance," *Rundbrief des Fachausschusses Management der Anwendungsentwicklung und -wartung (WI-MAW) Gesellschaft für Informatik e.V.,* pp. 49-59, 2013.

[5] International Software Testing Qualifications Board, *Certified Tester Foundation Level Syllabus, Version 2018 V3.1,* -: International Software Testing Qualifications Board, 2019.

[6] United Nations Economic Commission for Europe, "UN Regulation No. 156 - Software update and software update management system," 22 January 2021. [Online]. Available: https://unece.org/sites/default/files/2021-03/R156e.pdf. [Accessed 30 January 2022].

[7] U.S. Department for Transportation NHTSA, "Cybersecurity Best Practices for the Safety of Modern Vehicles," 2020 Update. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf. [Accessed 22 January 2022].

[8] United Nations Economic Commission for Europe, "UN Regulation No. 155 - Cyber security and cyber security management system," 22 January 2021. [Online]. Available: https://unece.org/sites/default/files/2021-03/R155e.pdf. [Accessed 30 January 2022].

[9] *ISO 26262 Road vehicles — Functional safety Parts 1 - 12,* 2018.

[10] *ISO/DIS 24089 Road vehicles — Software update engineering.,* 2021.

[11] International Software Testing Qualifications Board, "ISTQB Glossary Version 3.6," 30 June 2021. [Online]. Available: https://glossary.istqb.org/de/term/. [Accessed 30 January 2022].

[12] M. Grande, 100 Minuten für Anforderungsmanagement - Kompaktes Wissen nicht nur für Projektleiter und Entwickler, 2. ed., Wiesbaden: Springer Fachmedien Wiesbaden, 2014.

[13] AUTomotive Open System ARchitecture, *R20-11 Classic Platform,* 2020.

[14] *GB 201-5 General Technical Requirements for Software Updates of Vehicle,* unpublished working status.