Functional Safety Assessment of High-Available 12V Power Supply Systems for Electric Vehicles with Automated Driving Functions

Shouzheng Wang [1, 2, 3] Christian Winter [2] David Cello [1]

1) Faculty of Mobility and Technology, Esslingen University, Esslingen am Neckar, Germany

E-mail: Shouzheng.Wang@hs-esslingen.de

2) Robert Bosch GmbH, Schwieberdingen, Germany

3) Institute for System Dynamics, University of Stuttgart, Stuttgart, Germany

ABSTRACT: In recent years, significant progress has been made in the electrification and automation of vehicles. A highly reliable 12V power supply is a prerequisite for SAE Level 3+ automated electric vehicles, particularly for safety-critical functions. A so-called high-available 12V power supply system can guarantee a safe and uninterrupted 12V power supply for automated electric vehicles. One possible approach is to use redundant power sources, typically batteries. Alternatively, a DC-DC converter with high availability regarding the power supply can also be used, which is defined in this paper as a high-available DC-DC converter. This paper introduces the definition of high availability as well as high-available DC-DC converters and presents three different classifications of high-available 12V power supply systems for automated electric vehicles. Finally, the reliability and probabilistic metric for random hardware failures (PMHF) of each system are calculated to analyze functional safety in accordance with ISO 26262. Based on these results, the high-available 12V power supply system with the best reliability and functional safety performance can be identified.

KEY WORDS: functional safety, 12V power supply system, automated electric vehicles, PMHF.

1. INTRODUCTION

The ongoing electrification of powertrains and automation of vehicles is leading to the integration of more and more electronic devices in vehicles. Some of them are safety-critical such as vehicle computers. Therefore, it is important to ensure the power supply of these components. In 2018, the International Organization for Standardization (ISO) released a new version of the Automotive Functional Safety Standard ISO 26262, which specifies the functional safety of related electrical and/or electronic (E/E) systems in the automotive industry. The assessment of the Automotive Safety Integrity Level (ASIL) is defined in ISO 26262. It is based on a hazard and risk analysis, which considers exposure (E), controllability (C) and severity (S). 4 ASIL ratings are defined in ISO 26262, where ASIL A is the lowest level and ASIL D is the highest level [1, 2].

To ensure the 12V power supply for safety-related functions, it is essential to install highly redundant power sources as backup, typically low-voltage (LV) batteries. It should be noted that all LV batteries in this paper refer to 12V batteries. In [3], several 12V power supply concepts are proposed for different levels of driving automation. All of them are equipped with LV batteries. As the level of driving automation and the safe stop level increase, the required power consumption and emergency operation duration also rise [3, 4]. As a result, the requirements for backup batteries are more challenging because the required battery capacity and discharge capability are significantly increased. Instead, a high-available DC-DC converter (HA DC-DC) can replace LV batteries as a redundant power supply source, eliminating the need for batteries while still meeting functional safety requirements. Thus, for a high-available 12V power supply system (HA 12V PSS), LV batteries and HA DC-DCs are two necessary components to guarantee a safe and uninterrupted 12V power supply for automated electric vehicles.

This paper introduces the definition of high availability as well as HA DC-DC and presents three different classifications of HA 12V PSS for automated electric vehicles. To determine whether functional safety meets the required ASIL rating, this paper employs a practical method based on reliability theory to preliminarily estimate the probabilistic metric for random hardware failures (PMHF) of each system topology. This paper is

organized as follows. Section 2 introduces the definition of high availability and presents three classifications of HA 12V PSSs. Section 3 describes the methodology and assumptions used. The results of functional safety assessment are presented and compared in Section 4. Finally, Section 5 provides a summary of the paper.

2. HIGH-AVAILABLE 12V POWER SUPPLY SYSTEM

For the definition of high-available or high availability (HA), three parameters are necessary: the power P_{HA}, the time interval T_{HA} and the associated ASIL rating, depending on the level of driving automation and the safe stop level [4]. Fig. 1 shows the definition of T_{HA}, which is the time interval between the occurrence of a fault in the power supply system and the transition to a safe state.

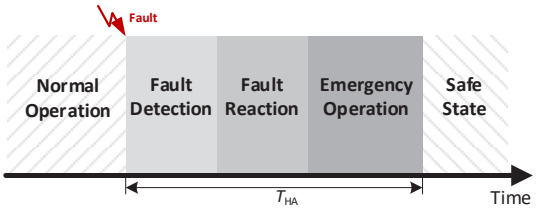

Fig. 1. Transition to safe state after fault.

The definition means that, during the time interval T_{HA}, the power P_{HA} must be delivered with ASIL X (X can be A, B, C or D). Such a 12V power supply system or a DC/DC converter capable of fulfilling the defined HA requirement is referred to as a HA 12V PSS or a HA DC/DC, respectively. Typically, the defined HA requirement is met using LV batteries. Alternatively, an HA DC-DC can replace LV batteries as a redundant power source, ensuring the necessary power transfer from high-voltage (HV) batteries within the required time interval. For certain safety-critical functions in highly automated electric vehicles, the power supply must meet the highest ASIL rating, requiring ASIL D compliance for HA. With ASIL decomposition, it is possible to decompose one power source with ASIL D into two independent power sources with ASIL B (D), significantly reducing development complexity [1, 2]. Depending on the type of redundant power sources, this paper considers three classifications of HA 12V PSSs, comprising six topologies, as shown in Fig. 2:

- HA 12V PSS with two LV batteries (topologies 1-3),
- HA 12V PSS with one HA DC-DC plus one LV battery (topologies 4-5)
- HA 12V PSS with two HA DC-DCs (topology 6)

The redundant power sources relevant to meet the HA requirement are highlighted in orange. The depicted Powernet Guardian (PNG), an intelligent power distribution switch, must be equipped to prevent interference from other loads. If a power source fails, the PNG will identify and isolate it, while the power supply can be maintained by other power sources. However, the power supply will be lost if all power paths in the system are broken down. Moreover, a pragmatic and generally applicable procedure is proposed in [5] for a comprehensive analysis of the advantages and disadvantages of these three classifications of HA 12V PSSs, using both quantitative and qualitative criteria such as cost, size and other factors.

3. METHODOLOGY AND ASSUMPTIONS

According to ISO 26262, the system must be well-designed to avoid systematic failures and to limit random hardware failures. Three hardware metrics (HW metrics) are required for the

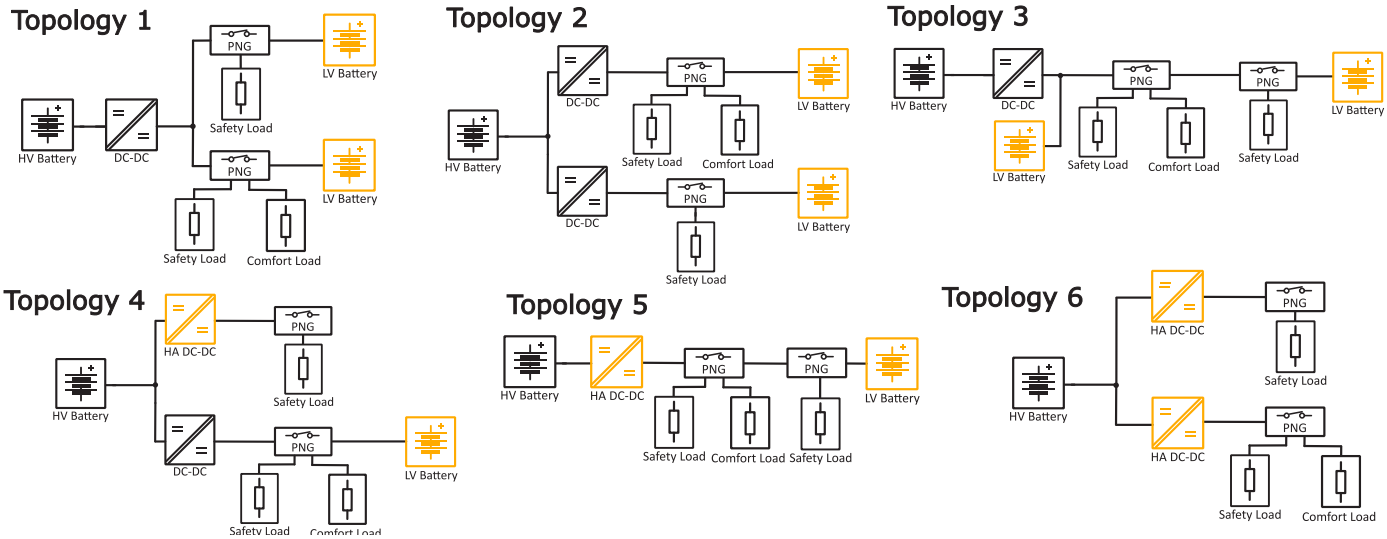

Fig. 2. Six topologies of HA 12V PSS.

quantitative evaluation of random hardware failures. These HW metrics must meet the target values corresponding to the ASIL rating, as shown in Table 1. PMHF is defined as the average probability of failure per hour over the lifetime:

$$\mathrm{PMHF}(t) = \frac{1-R(t)}{t} \quad (1)$$

where *R(t)* is reliability, *t* is time. For single-point failures with constant failures rates, PMHF can be approximately equal to the failure rate λ only when λt is small [6]:

$$\mathrm{PMHF}(t) = \frac{1-e^{-\lambda t}}{t} \approx \lambda \quad (2)$$

In case of multiple-point failures, it can be approximated as:

$$\mathrm{PMHF}(t) = t^{n-1} \prod_{i=1}^{n} \lambda_i \quad (3)$$

where *n* is the number of independent failures. Although PMHF has the same unit (in FIT, Failure in Time) as failure rate λ, they should not be confused. The other two HW metrics, single-point fault metric (SPFM) and latent-fault metric (LFM), indicate the fault diagnosis coverage for single-point fault and latent-fault, which depends on the development of safety mechanisms. Therefore, they are not considered in this context. The focus of this paper is solely on the evaluation of PMHF using reliability analysis methods from previous studies, such as Reliability Diagram Method (RDM) [7], Fault Tree Analysis (FTA) [8] and Markov Chain (MC) [9]. All of these methods are applied to the proposed HA 12V PSSs in this work and demonstrated below.

Table 1. Target value of HW metrics for different ASIL [1].

	ASIL A	ASIL B	ASIL C	ASIL D
PMHF	-	< 100 FIT	< 100 FIT	< 10 FIT
SPFM	-	≥ 90%	≥ 97%	≥ 99%
LFM	-	≥ 60%	≥ 80%	≥ 90%

To perform reliability analysis at the system level, the system structure and the failure rate λ of each system part must be known. However, in the early development stages of a power supply system, it is difficult to obtain all information in detail. Therefore, some empirical failure rate values from previous research [7, 10, 11] are used (shown in Table 2), sufficient for a preliminary evaluation and comparison. Moreover, the following assumptions are made for simplification:

- Time-constant failure rate for all components.
- Ideal fault detection and isolation.
- Independent failures, without interference between loads.
- The HV battery is perfectly monitored by the Battery Management System, so its FIT value is ignored.
- An 8,000-hour operating time over the vehicle's 15-year lifetime [2].

Table 2. Failure rate of each component used for calculation. [7, 10, 11]

Component	Failure rate	Component	Failure rate
HV battery	ignored	LV battery	1100 FIT
Normal DC-DC	1000 FIT	HA DC-DC	100 FIT
Safety load	10 FIT	PNG	50 FIT

The LV battery failure rate model in [10] is used. It consists of two parts: a constant failure rate $\lambda_{\mathrm{constant}}$ (1100 FIT) and an aging-related failure rate λ_{aged}. After unit conversion, the reliability and failure rate model of LV batteries are shown in Fig. 3. The differences between the situations with and without the LV battery aging effect are also discussed and compared in Section 4.

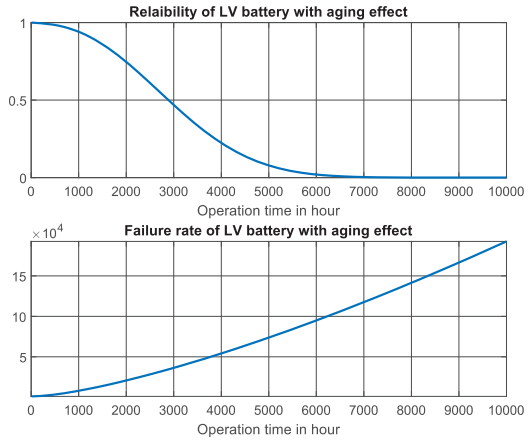

Fig. 3. Reliability and failure rate model of LV batteries [10].

4. EVALUATION AND COMPARISON

In this section, three evaluation methods are demonstrated, each using one HA 12V PSS topology as an example. Subsequently, the proposed six HA 12V PSS topologies are compared in terms of reliability and PMHF. Additionally, the differences between scenarios with and without the LV battery aging effect are analyzed.

RDM is demonstrated with topology 1 as an example. There are three power sources in total: one from the HV battery via a normal DC-DC converter and two LV batteries. Based on the system structure, the corresponding reliability diagram can be easily obtained, as shown in Fig. 4. Each block represents the corresponding component in the HA 12V PSS, along with its

specific failure rate. If a path can be traced through the block diagram from start to finish, the safety-relevant function can still be ensured. To execute the calculation, the block diagram must be equivalently converted into a simplified structure based on Bayes' theorem. More details about RDM can be found in [7].

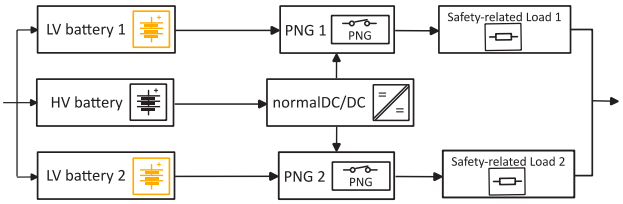

Fig. 4. Reliability Diagram of HA 12V PSS topology 1.

FTA logically combines top-level, intermediate and basic events using AND and OR operators to assess the impact of component faults on system failures. Topology 4 is used here for demonstration. The system includes one LV battery, one HA DC-DC and one normal DC-DC converter. From this system structure, the corresponding fault tree can be easily derived, as shown in Fig. 5. The top-level event represents the failure of the safety-relevant function, while the basic events correspond to individual component failures. PMHF can be derived from the probability of failure of the top-level event in FTA. Further details on FTA can be found in [8].

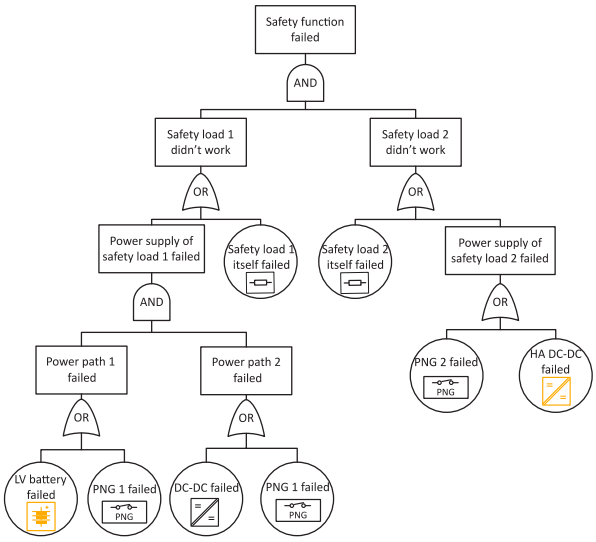

Fig. 5. Fault Tree Analysis of HA 12V PSS topology 4.

A Markov chain is a stochastic process that models a sequence of events in which the probability of each event depends only on the state of the previous event, a property known as memorylessness. Consequently, it is widely used for reliability evaluation. Topology 6, consisting of only two HA DC-DCs, is used to demonstrate the MC method, as shown in Fig. 6. Each circle represents a state, with transition probabilities between states corresponding to the failure rates of the relevant components. By solving the MC, the probability of each state can be determined. Reliability is then calculated as the sum of the probabilities of states S_1 to S_3.

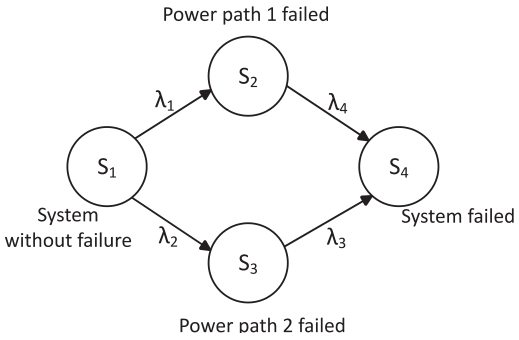

Fig. 6. Markov Chain of HA 12V PSS topology 6.

From the models above, the reliability for each topology can be calculated, as shown in Fig. 7. Subsequently, the PMHF of each topology can be derived [6, 8], which are shown in Fig. 8. As the time increases, the system reliability deteriorates, and the PMHF value increases. When the LV battery aging effect is ignored, the PMHF values for all topologies are far below the ASIL D target

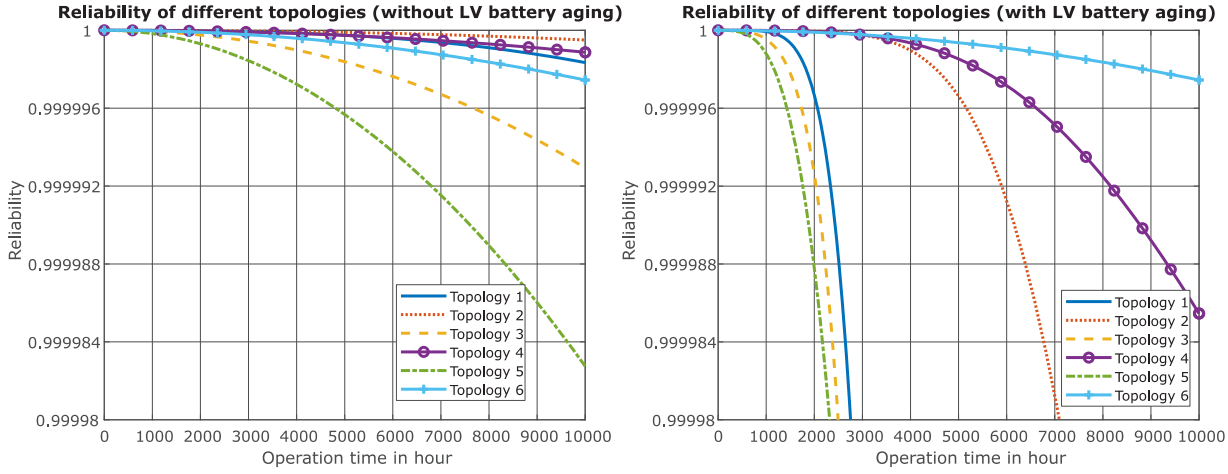

Fig. 7. Reliability without and with consideration of LV battery aging effect.

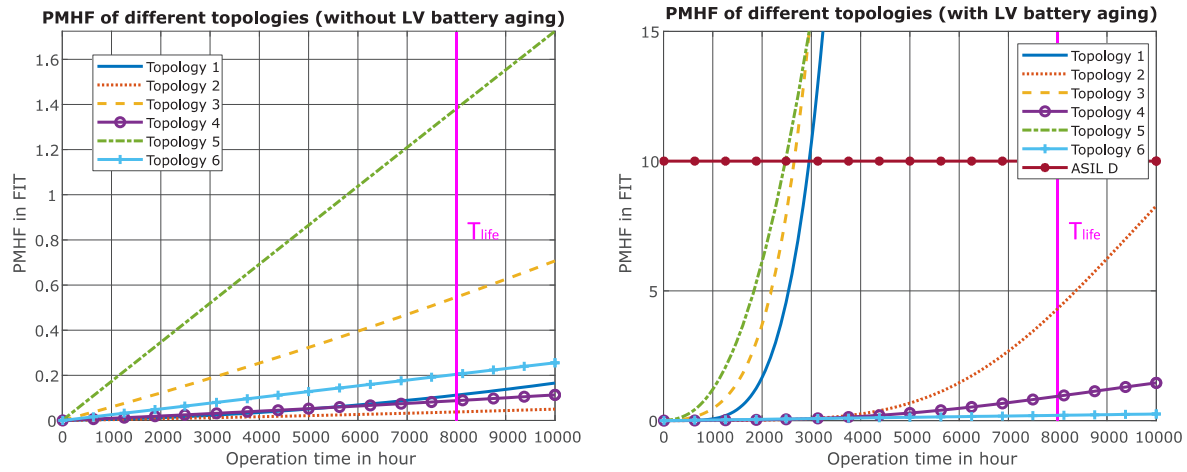

Fig. 8. PMHF without and with consideration of LV battery aging effect.

value of 10 FIT within 8,000 hours, indicating that the novel topologies with HA DC-DC converters can also satisfy the ASIL D criterion. The effectiveness of the novel topologies with HA DC-DCs is verified: HA DC-DCs can theoretically replace LV batteries to serve as redundant power sources. Since the failure rate of the HV battery is neglected, each DC-DC can also be considered as an independent power source. Among the topologies with two LV batteries, topology 2 has four independent power sources and therefore exhibits the best performance. Similarly, among the topologies with one LV battery and one HA DC-DC, topology 4 demonstrates the best performance.

To make the models more realistic, the LV battery failure rate model with the aging effect, as introduced in Section 3, is used. Considering the aging effect, the reliability of topologies using LV batteries decreases significantly, while PMHF increases considerably, indicating that the aging effect of LV batteries has a significant impact on system reliability and functional safety. Over the 8,000-hour lifetime, the PMHF values of some topologies will exceed the ASIL D limitations. For the topologies with two LV batteries, two normal DC-DCs are necessary for two independent power paths from the HV side to fulfill the ASIL D requirement over the entire lifetime (Topology 2). And the topologies with one LV battery plus one HA DC-DC require one additional power path from the HV side using one normal DC-DC (Topology 4). However, the topology with two HA DC-DCs still meets the ASIL D requirement within the entire lifetime (Topology 6). To fulfill the ASIL D requirement for other topologies (1, 3 and 5) over the total lifetime, it is necessary to use more reliable LV batteries with less ageing effect or to update the LV batteries regularly.

5. CONCLUSIONS

This paper introduces the definition of high availability as well as HA 12V PSSs in automated electric vehicles. Three classifications of HA 12V PSSs are presented. The first classification uses two LV batteries, the second classification uses two HA DC-DCs and the third is a combination by using one HA DC-DC plus one LV battery. To preliminarily estimate the PMHF for HA 12V PSSs, a practical functional safety analysis method based on reliability theory is proposed. Three different methods of reliability analysis (FTA, RDM and MC) are implemented for PMHF calculation. Based on the proposed methods, the reliability and functional safety of each system topology are evaluated and compared.

It can be deduced that HA DC-DC converters can replace LV batteries as redundant power sources for safety-critical functions, as they can also meet the functional safety requirements. This theoretically verifies the feasibility of a battery-free 12V power supply system. In addition, the situations with and without consideration of the LV battery aging effect are compared. It can be concluded that the aging effect of LV batteries has a significant impact on system reliability and functional safety. For some HA 12V PSS topologies, the LV batteries should be regularly updated to meet the ASIL D requirement throughout the vehicle's operational life, which means that more reliable batteries with less ageing effect are beneficial. Future research should also explore hardware implementation, specifically how to achieve the defined HA DC-DC converters with high reliability.

REFERENCES

(1) ISO 26262-2018, *Road Vehicles - Functional Safety*, 2018.

(2) VDA Recommendation 450, *Electrical Power Supply System regarding automated driving in the context of ISO 26262*, 2021.

(3) S. Schumi, and A. Graf, “Energy and supply concepts for automated driving”, *AmE 2018-Automotive meets Electronics, 9th GMM Symposium*, Dortmund, Germany, 2018, 1-5.

(4) T. Shen, et al., “Design of a fail-operational powertrain for automated electric vehicles”, *19. Internationales Stuttgarter Symposium: Automobil- und Motorentechnik*, Springer Fachmedien Wiesbaden, 2019.

(5) S. Wang, C. Winter, and D. Cello, “High-available 12V power supply systems for electric vehicles with automated driving functions,” *International Conference on Electric Vehicle and Vehicle Engineering (CEVVE 2024)*, Dec. 2024, to be published.

(6) A. Kleyner, and R. Knoell, “Calculating Probability Metric for Random Hardware Failures (PMHF) in the New Version of ISO 26262 Functional Safety - Methodology and Case Studies”, SAE Technical Paper 2018-01-0793, 2018.

(7) S. Schumi, and D. Watzenig, “Semiconductor Safety Concepts for the Power Distribution of Automated Driving”, *SAE International Journal of Connected and Automated Vehicles* 2.12-02-04-0017 (2019), 233-239.

(8) N. Das, and T. William, “Quantified fault tree techniques for calculating hardware fault metrics according to ISO 26262”, *2016 IEEE Symposium on Product Compliance Engineering (ISPCE)*, IEEE, 2016, 1-8.

(9) J. F. Kitchin, “Practical Markov modeling for reliability analysis”, *1988. Proceedings, Annual Reliability and Maintainability Symposium*, IEEE, 1988, 290-296.

(10) M. Mürken, et.al., “Analysis of automotive lead-acid batteries exchange rate on the base of field data acquisition”, *2018 IEEE International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles & International Transportation Electrification Conference*, IEEE, 2018, 1-6.

(11) M. Mürken and P. Gratzfeld, “Reliability Comparison of Bidirectional Automotive DC-DC Converters”, *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, ON, Canada, 2017, 1-7.