Optimization of Power and Signal Distribution Systems for Advanced Safety Features

Nils Potthoff, Aptiv Services Deutschland GmbH, Wuppertal, Deutschland, nils.potthoff@aptiv.com
Timo Feismann, Aptiv Services Deutschland GmbH, Wuppertal, Deutschland, timo.feismann@aptiv.com
Dr. Rainer Denkelmann, Aptiv Services Deutschland GmbH, Wuppertal, Deutschland, rainer.denkelmann@aptiv.com
Michael Kiffmeier, TU Dortmund, Dortmund, Deutschland, michael.kiffmeier@tu-dortmund.de
Marvin Rübartsch, TU Dortmund, Dortmund, Deutschland, marvin.ruebartsch@tu-dortmund.de
Prof. Dr.-Ing. Stephan Frei, TU Dortmund, Dortmund, Deutschland, stephan.frei@tu-dortmund.de

Abstract

The goal of the funded project "AFFiAncE" is to provide a universal infrastructure to develop, evaluate and select next generation vehicle system architectures for advanced safety features. The focus is on the communication and the on-board energy network. In a test bench currently under construction, it will be possible to play back and manipulate different sensor sets with a replay system and to configure and test the communication infrastructure. In order to evaluate the behaviour of the on-board energy network for critical safety functions, various faults in the on-board energy network will be simulated and evaluated. The simulation results are used to test the real hardware in a realistic scenario based on the current and voltage profiles from the simulation. This test environment makes it possible to evaluate the fail-operational behaviour of the on-board power system.

Kurzfassung

Das Ziel des Förderprojektes „AFFiAncE" ist es eine universelle Testumgebung zur Entwicklung, Bewertung und Auswahl von Fahrzeugarchitekturen für Sicherheitsfunktionen zu entwickeln. Hierbei wird der Fokus auf das Kommunikations- und das Energiebordnetz gelegt. In einem zurzeit im Aufbau befindlichen Prüfstand wird es möglich sein, verschiedene Sensorsätze mit einem Replay-System abzuspielen, zu manipulieren und die Kommunikationsinfrastruktur zu konfigurieren und zu testen. Um das Verhalten des Energiebordnetzes für kritische Sicherheitsfunktionen zu bewerten, werden unterschiedliche Fehler im Energiebordnetz simulativ untersucht und bewertet. Die Simulationsergebnisse werden genutzt um die echte Hardware in einem realistischen Szenario, basierend auf den Strom- und Spannungsprofilen aus der Simulation, zu testen. Diese Testumgebung macht es möglich, das fail-operational Verhalten des Energiebordnetzes zu bewerten.

1 Introduction

Tomorrow's mobility will be mainly characterized by advanced safety features. The goal is to increase the safety in road traffic. However, enhanced reliability and safety requirements increase the complexity in the development of vehicle systems and therefore new challenges arise. In some cases, the driver will no longer be available as a sufficient fall-back factor and the system itself must be able to guarantee functionality in all situations. This includes technical malfunctions or failures. At the same time, the general acceptance of new mobility concepts will largely depend on the trust in safety and reliability that end customers have in these systems. The upcoming challenges focus on aspects of security in addition to suitability for series production, standardization and legal compliance. Independent fault detection and correction are mandatory to maintain a state of safe operation. Appropriate fault handling can be ensured, for example, by redundancy at system level.

This paper presents the scope and selected results from the consortium project "Adaptierbare Fahrzeugarchitektur Für AutomatisiErte Fahrzeuge" (AFFiAncE), funded by the "Europäischen Fonds für regionale Entwicklung" (EFRE). First of all, possible influences and error sources, as well as their effects on the communication network, on sensors and the perception of the environment are discussed. This is followed by a closer look on the power supply system. It is shown how random wiring faults can be modelled and how power supply architectures can be checked for safety characteristics in the simulation. Subsequently, it is shown how the results are used to create a test bench which can be used for extensive tests of the communication and power supply topology. Ultimately, this leads to the selection of the most suitable architecture and diagnostic strategy.

1.1 Environment sensing and communication network

The system architectures for advanced safety features in vehicles can be fundamentally described by the organization of components. A formal description of a system, down to the design on a component level, supports the system implementation. One important aspect is the scalability over different equipment versions and the need to support vehicles with different Autonomous Driving Levels, starting with level 0 up to higher levels.

Robustness is a core characteristic to evaluate systems providing safety features. Robustness is the ability of a system to handle errors and erroneous inputs. The output should in either case be stable. Errors and erroneous inputs can result from malfunctions in the sensors, communication errors or power failures (see Figure 1). Additional factors to be considered are environmental conditions which affect the perception performance. E.g., this can be special lighting conditions or heavy rain.

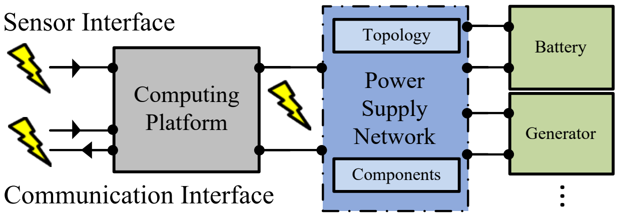

Figure 1 – Interfaces where various errors can occur, with regard to the Computing Platform

The aim is to optimize the architecture during development and testing to increase robustness while keeping the architecture lean and as cost efficient as possible. This is a method to guarantee safety and security for a system. On the architecture level a high reliability is to be achieved. In moving the technology towards market-ready products, it is essential that these systems are safe, reliable and the availability of the features needs to be high. Ultimately, this will convince end customers to have trust in new features.
The goal is to optimize an embedded system for safety features. Therefore, KPIs are needed to measure the “quality” of ADAS systems while malfunctions are synthesized. Different topologies of the communication networks are expected to show different behavior in critical situations. The variety includes the transmission technologies as the linkage between senders and receivers. Different configurations can be individually evaluated and finally compared, so that the safest and most reliable variant can be identified in the end.
The evaluation concept is based on the fusion of all sensor types. The environmental representation will be realized with an occupancy grid. The comparison of the occupancy grid of the same scenario with changed parameters gives an impression of the effects of these changes.

1.2 Power supply network

In the area of energy supply, it is of crucial importance to identify the best topologies for next generation vehicles. Such topologies should be robust against faults.
For this purpose, evaluation criteria for power network architectures are developed. Critical states are then provoked in the simulation in various architectures by means of fault simulations, whereby short circuits, wire interruptions or electric arcs can cause malfunctions of the electrical system. A cable short for example will trigger the wire protecttion. A wire protection can be a melting fuses (in future such melting fuses are expected to be substituted by electronic fuses), that will cut the short from the power supply. Even when a safety critical component is not affected directly by such a short, there will be a voltage drop in the overall supply system and subsequent voltage ringing. Such disturbances can cause malfunctions of electronic components that are difficult to analyze.
In AFFiAncE an advanced testing approach is proposed. The voltage or current profiles in a power supply during a failure in the supply network can be investigated model based. This way, a large number of different supply failures can be analyzed and the termination behavior at any point in the supply network can be found.
Safety critical components should be robust against failures somewhere in the power supply. The simulated voltage and current profiles can be used to test the robustness in the event of a fault. To emulate the various disturbances, an “arbitrary voltage generator” is needed. Such a generator should be able to replay simulated voltage profiles and consider the impedance of the power network. As such “arbitrary voltage generators” with required specifications are not available from the shelf, the development of a special device based on a half-bridge topology (see Figure 2) was started.

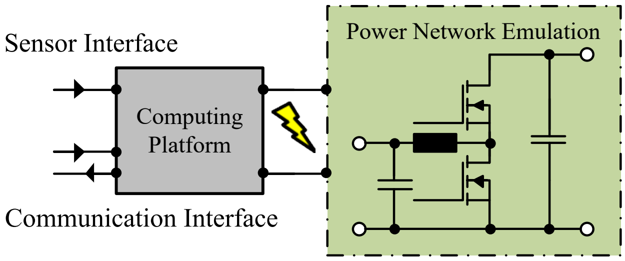

Figure 2 – Concept of the Power Network Emulation based on fault simulation results

Based on the defined evaluation criteria, all architectures can be individually evaluated and compared in context so that an optimal architecture can be identified. In addition, diagnostic concepts can be tested and optimized this way.

2 Simulation based energy system fault analysis

The goal of the project is to provide a universal infrastructure to develop and evaluate different system architectures for advanced safety features. The simulation environment for power supply systems ensures a testing of user defined architectures. Finally, the defined architecture can be evaluated.

2.1 Model library and fault simulation

A large number of possible topologies and diagnostic concepts is available when designing power supply networks. As shown in [1], many combinations of different voltage levels, converter concepts, voltage sources, etc. may have their own advantages and disadvantages. When systematic analysis of many topologies with various operating strategies is needed, simulation can be very beneficial.

For this purpose, firstly all relevant network components are modeled. Among other things, energy converters, energy storage and energy consumers are considered [2]. By connecting the components with the corresponding cable and contact models, a complete power supply system model is created. Here, the overall behavior in the event of a fault can be simulated and evaluated by using fault models. Faults to be considered can be serial faults, i.e. line breaks or changes in contact resistance, as well as parallel faults, i.e. short circuits. At the 48 V voltage level, serial and parallel arcs must also be simulated, as well [3]. Figure 3 shows the general workflow, in which the different architectures can be tested.

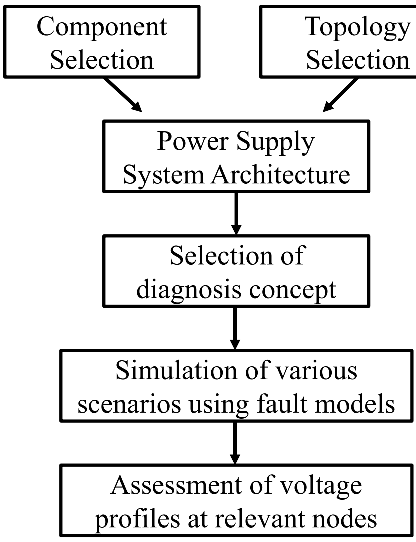

Figure 3 – Workflow from the creation of an electrical power supply system to the evaluation of the simulation results

Any power supply network architecture can be evaluated within the workflow shown. Random faults can occur anywhere at any time [4]. According to this principle, the relevant faults have to be simulated at all nodes or branches in order to enable a comprehensive evaluation.

The evaluation of the voltage profiles at the relevant points can be done from different points of view. Simple time criteria for voltage dips can be used here [5] or load characteristics can also be evaluated [6]. In particular, the new focus on robust diagnostic methods creates new criteria, which are discussed in more detail in the following chapter.

2.2 Assessment criteria for automotive power supply systems

In order to ensure a reliable analysis of different power supply architectures, evaluation criteria must be defined. These criteria can be divided into three parts:

Table 1: Assessment criteria for power supply systems

Component and topology selection	Number of components (batteries, generators, converters, fuses/electronic fuses, …) Cable design (cable cross-sections, lengths, …) Laying and installation of the components (critical installation spaces and automated production, …)
Functionality in the event of a fault	Redundant supply nodes must never be exposed to critical (static and/or dynamic) faults at the same time
Diagnosis and protection concepts	Possibility of fault detection Possibility of fault identification Possibility of fault localization Possibility of fault isolation

This assessment approach is discussed below.

2.2.1 Component and topology selection

The design of energy networks starts with the selection of the power consumers. Then these components are connected to power supply, distribution and protection elements. The interconnecting cables are part of the corresponding topology. Redundancy can increase availability of the functions.

Furthermore, other framework conditions can be included to evaluate the component selection. The locations of the components in the overall vehicle can also be considered. Critical installation spaces can be found from various crash scenarios and it can be concluded from the arrangement of the components how many components are affected in different accident scenarios.

2.2.2 Functionality in the event of a fault

Whether a power supply system is able to maintain its function even in the event of a fault (fail-operational) is an important question. An important criterion from this point of view is that redundant supply nodes must never be exposed to critical faults at the same time. In addition to a redundant power supply for safety-critical consumers, the control units can also be designed directly redundant.

2.2.3 Diagnosis and protection concepts

Furthermore, the diagnosis and protection concept of the on-board power supply system must also be included in the overall assessment. It should be assessed whether robust detection, identification, localization and fault handling is possible [7]. When selecting a fuse concept, melting fuses or electronic fuses can be used, for example. Electronic fuses offer greater flexibility in the design of the power supply system and offer greater degrees of freedom for diagnosis and protection.

The evaluation criteria presented here are qualitative descriptions. It is important to quantify these evaluation criteria so that they can be linked to the various (fault-)simulations to achieve an automatic evaluation of the overall system. The aim is to compare the advantages and disadvantages of different power supply topologies and to select a topology suitable for safety features.

2.3 Simulation and evaluation example

A symmetric, simplified power supply network in Figure 4 has been chosen to demonstrate the simulation process. Two sources supply two redundant power zones via a power distribution unit (PDU). Such PDUs may include semiconductor switches/fuses and measurement equipment in order to observe the power network and switch off single branches in case of a failure. So, the PDU is able to separate both power zones in the case of a fault. As a fault scenario, a short circuit in zone 2 is assumed.

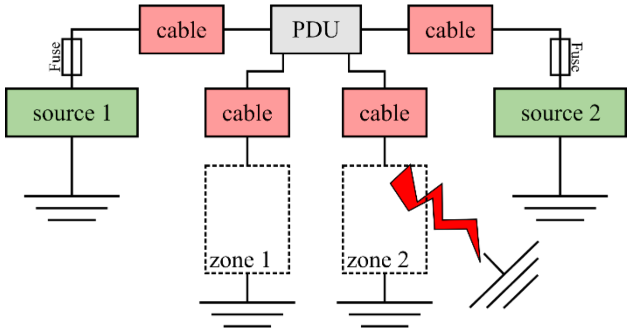

Figure 4 – Simplified power network as simulation example

The before mentioned power network component models for sources, fuses and cables have been used. As terminations of zone 1 and zone 2, ohmic capacitive loads have been used, which simulates a voltage stabilizing capacitor and the static behavior of various loads. A simulation result is shown in Figure 5.

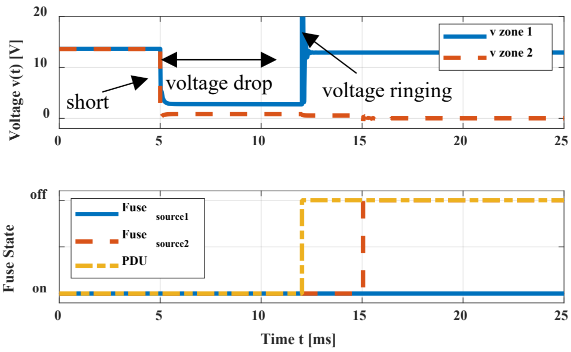

Figure 5 – Simulation of a short circuit in the example power network, Figure 4

After 5 ms the short circuit happens. After a detection time of 7 ms, the PDU separates zone 1 from zone 2. Another 3 ms later the fuse of source 2 trips and stops the short circuit supply. By taking the before mentioned functional criterion into account and evaluating the redundancy, voltage drops in both zones for 7 ms can be observed. A voltage peak at 12 ms, caused by the switching operation of the PDU, and as a result of the inductance of the cables, can be observed, as well. Depending on the supply demands of the considered components, this transient behavior of the power network and the diagnosis concept may be acceptable or has to be reduced.

3 Test bench to emulate malfunctions

The goal of the project is to provide a universal infrastructure to develop and evaluate different system architectures for advanced safety features. The test bench shall provide a basis to evaluate the communication and power supply system architecture to comply with the demands of safety requirements.

3.1 Replay system for injection of communication and sensor errors

With regard to the communication, suitable sensor sets (with cameras, radar and lidar sensors) are selected in the AFFiAncE project. These sensor sets are required to evaluate the functionality for the features under test.

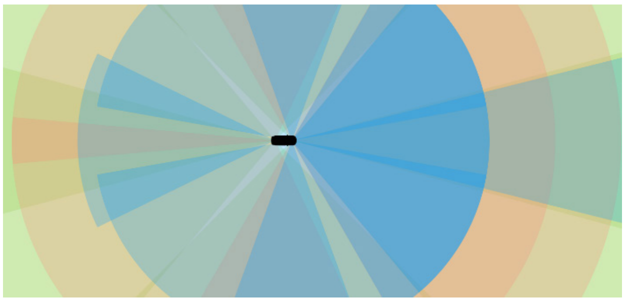

Figure 6 – Example of environment coverage through radar sensors (green), lidar sensors (red) and cameras (blue).

For each sensor set, error states that emulate a degraded perception of the environment are defined. The influence of extreme environmental conditions shall be investigated. The consideration of all imaginable component malfunctions is also necessary. There are different approaches for components and system testing. For instance, this could be done by simulated or real world testing. Each method has advantages and disadvantages. The combination of different approaches will finally provide a complete view.
The focus of this project is the test bench approach. It is challenging to provoke critical situations during vehicle operation, even on dedicated test tracks. A test bench avoids this challenge. Furthermore, a test bench gives a well-defined environment for system testing and access to many parameters. For system optimization the circumstances are better due to its flexibility. Finally a high efficiency of investigation can be reached in combination with test drives.
Reproducible manipulation of the sensor data can cover as many scenarios as possible and make them testable while defining a communication system. The defined test environment also enables good comparability of the results. The virtual variation of different communication topologies can make it possible to evaluate and finally compare different configurations individually. The safest and most reliable variant can be identified noticeably.
The (AFFiAncE) test bench concept makes it possible to implement architectural changes with reduced effort. Nevertheless, the validation can be done on the basis of real

ISBN 978-3-8007-5202-7

embedded hardware. This yields a better and more detailed validation than a simulation could.
The stimulation of an architecture with sensor data can come from different sources. Within this project corner cases are intended to be created with a combination of real and synthetic sensor data. Besides recorded data, a performance comparison with synthetically generated sensor signals out of a virtual environment is aimed for.
The final test bench will include a data replay system, a physical and logical modifiable and configurable architecture as well as embedded computing platforms. Configurable architectures are to be realized for each eligible communication interface. Different abstraction methods are needed depending on the network topologies and the physical layer. The test definition is independent thereof.
The improvement we are aiming for results from an enhancement of test scenarios. This can be realized through adding manipulated data to recorded sensor data. The recorded sensor data is captured and contains environmental and scenario data. An architecture configurator allows modifications to the communication architecture. These can be carried out quickly and cost-effectively.
Any malfunction in the processing and communication chain from perception to the computing platform, can either be provoked by manipulating recorded sensor data or interference with the physical transmission. For this purpose the architecture configurator provides access to the communication links. The full concept is shown in Figure 7.

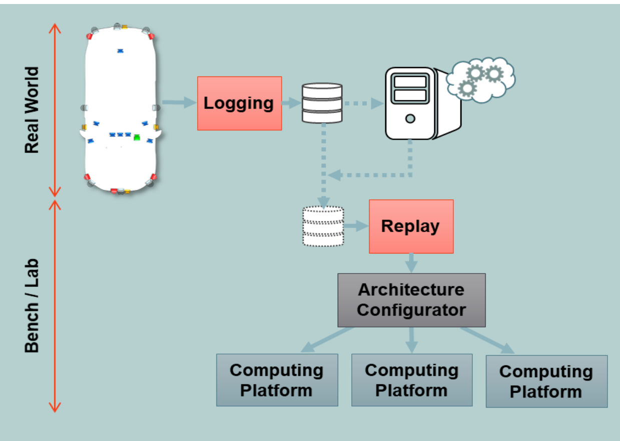

Figure 7 – Concept of the test bench approach. Sensor data are recorded in the real world. An architecture under test can be stimulated with this data, manipulated or full synthetic data. An abstraction reduces the effort to change the communication architecture.

Figure 8 shows the design of the planned testbench setup.

Figure 8 – Planned design of the testbench setup

3.2 Emulation system for power supply malfunctions

The power supply simulation can be used to investigate the effects of faults on the basis of the calculated current and voltage profiles, but it is unclear how the different consumers actually behave under voltage variations with complex profiles. In order to include the behavior of every consumer in the simulation, the simulation effort would be very large. Furthermore, it can only be assessed at great expense how redundantly designed electronic components react to the current and voltage profiles obtained from the simulation at several different supply nodes. An investigation of different real on-board network topologies in the laboratory would also involve massive efforts. With the help of power electronics, an on-board electrical system emulator is developed, which can be used as a source for the voltage curves v(t) at different supply nodes based on the simulation results (see Figure 9). Whereas general topology evaluations may be performed in simulation, tests of safety-critical newly integrated components should be done with actual hardware.

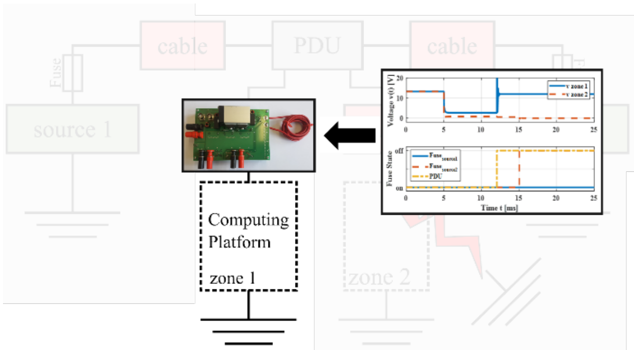

Figure 9 – Flexible emulation of the power supply system based on the voltage profiles v(t) (see Figure 5) gained in simulation

Due to the possible high-power consumption of the power supply system components, the power supply system emulator must be able to transmit high currents. This can be resolved by using multiple emulators in a parallel configuration. The parallel configuration of two half-bridge emulators is visualized in Figure 10.

ISBN 978-3-8007-5202-7

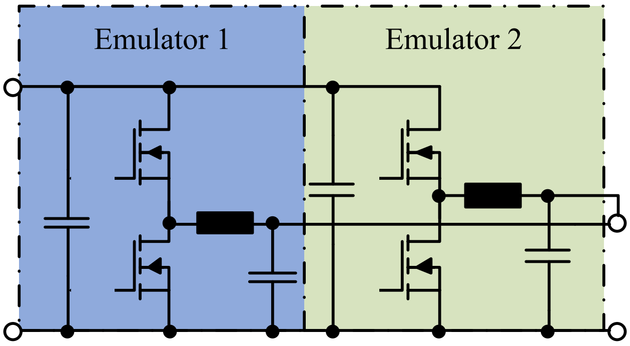

Figure 10 – Parallel configuration of multiple emulators

Figure 11 shows the first developed prototype of the emulator. An air coil is used to minimize saturation effects while investigating the behavior of the half bridge topology for the application.

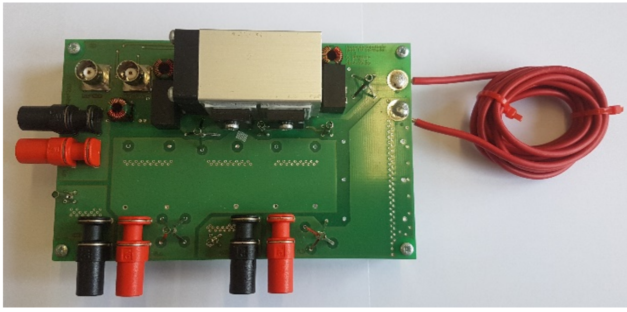

Figure 11 – Photo of the emulator prototype

The application requires a high switching dynamic to emulate the voltage profiles obtained in the simulation. The first approach here is to evaluate the dynamic behavior of the half-bridge topology by varying the control duty cycle of the high-side and low-side transistor. Furthermore, this approach is suitable for implementing a control algorithm for the emulator.
The first measurements have been done by using the half-bridge topology as a buck converter. The input voltage is 16 V. At the output a capacitance of 100 µF is used. The inductance of the air coil is approximately 18 µH. To achieve a large voltage jump, the duty cycle jumps from 90 % to 10 %. Figure 12 shows the jump of the output voltages for two different load configurations.

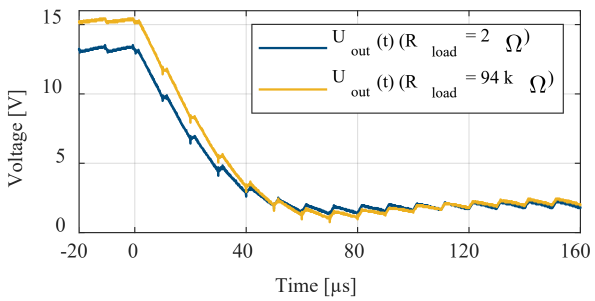

Figure 12 – Measurement of the dynamic response while the duty cycle jumps from 90 % to 10 % at 0 µs

The measurement results show that the response of the output voltage is approximately the same for both loads. The capacitance discharges both through the load and through the low-side transistor which automatically implies the storage inductance as well. At a high load resistance, the capacitance discharges mainly through the low-side transistor and the inductance. The measurements also show that the change in the output voltage is stabilized after approximately 120 µs. To further optimize the power supply system emulator, the discharge time of the output capacity must be shortened. It is possible to reduce the output capacity, but this will lead to a higher output voltage ripple which is also a problem in the optimization process. Optimizations in the layout and control method of the emulator are currently being examined to reduce the discharge time. Ultimately, the goal is to integrate several of these power supply system emulators into the test bench so that flexible residual power supply system emulations can be carried out.

4 Conclusion and Outlook

An overview of the objectives, approaches and concepts of the funded project “AFFiAncE” was given. In order to provide the needed safety and reliability advanced safety systems, a flexible test bench is being developed. This test bench allows to evaluate different communication or power supply architectures in regard to their safety and reliability. To ensure the necessary safety for end consumers and to build up trust in these systems, the possibility of creating various design options with low effort while developing vehicular communication or power supply systems are an important aspect. The testbench is supposed to meet these criteria. Furthermore, qualitative assessment criteria to evaluate different power supply architectures are given. As the project progresses, these criteria are going to be quantized to give a comparison factor between different topology approaches.
Various possibilities to access the system at different spots and to cause malfunctions were explained and depicted. In addition to the communication level, the power supply also plays an important role as an essential level in the overall system. Here, the approach of an emulator with the underlying simulation approach was introduced.

5 Acknowledgment

The work for this conference contribution was partly financed by the European Fund for regional development (EFRE), Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie of the State of North Rhine-Westphalia (MWIDE NRW) as part of the AFFiAncE project.

6 References

[1] S. Schumi and A. Graf: “Energy and Supply Concepts for Automated Driving,”, AmE 2018 - Automotive meets Electronics; 9th GMM-Symposium, Dortmund, Germany, 2018, pp. 1-5.

[2] R. Gehring: “Beitrag zur Untersuchung und Erhöhung der Spannungsstabilität des elektrischen Energiebordnetzes im Kraftfahrzeug“, München, Verlag Dr. Hut, 2013.

[3] C. Austermann, M. Kiffmeier and S. Frei: “State Transition Based Behavioural Model for Electric Arcs in 48 V Automotive Power Supply Networks,“ 2018 IEEE International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles & International Transportation Electrification Conference (ESARS-ITEC), Nottingham, 2018, pp. 1-6.

[4] ISO, “ISO/FDIS 26262 Road vehicles – Functional Safety – Part 1-10”, 2011.

[5] S. Schwimmbeck, Q. Buchner and H.-G. Herzog, “Evaluation of Short-Circuits in Automotive Power Nets with Different Wire Inductances,“ 2018 IEEE International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles & International Transportation Electrification Conference (ESARS-ITEC), Nottingham, 2018, pp. 1-6.

[6] L. Brabetz, M. Ayeb, G. Jilwan, P. Graebel and T. Kerner: “A New Approach to the Test, Assessment and Optimization of Robust Electrical Distribution Systems,” SAE International Journal of Materials and Manufacturing, 2013, pp. 382-388.

[7] R. Ghimire et al., “Integrated model-based and data-driven fault detection and diagnosis approach for an automotive electric power steering system,“ 2011 IEEE AUTOTESTCON, Baltimore, MD, 2011, pp. 70-77.

