A Model based Test Environment for the Analysis of the System's Behaviour during Power Supply Faults

M.Sc. Marvin Rübartsch, TU Dortmund University, On-board Systems Lab, Dortmund, Germany
M.Sc. Michael Gerten, TU Dortmund University, On-board Systems Lab, Dortmund, Germany
Prof. Dr.-Ing. Stephan Frei, TU Dortmund University, On-board Systems Lab, Dortmund, Germany

Abstract

The introduction of highly automated driving features demands a high reliability of safety critical components. Whether a critical component can maintain its function even in the event of a fault (fail-operational) is an import question. To ensure the needed safety and identify power supply architectures suited for this task, simulations can be very beneficial. Various power supply architectures can be tested in case of various power supply faults and the voltage stability of the overall system can be determined. Even though the voltage stability of the system can be a good measure to evaluate the systems behaviour during power supply faults, such disturbances can cause malfunctions of electronic components that are difficult to analyse in a simulation. Hence there is a need to access and evaluate the behaviour of safety critical components under these disturbances and ensure that they are working as intended. A new concept to evaluate the behaviour of safety critical components during the exposure of power supply system faults is presented. This concept uses time dependent voltage profiles from detailed system simulations for the supply of real safety critical components with the help of arbitrary waveform generators (AWG) and amplifiers. First results with this concept are shown with special attention on the robustness of communication during power supply faults.

1 Introduction

Tomorrow's mobility will be characterized by automated driving features which also demand for advanced safety features. However, enhanced reliability and safety requirements increase the complexity in the development of vehicle systems and, therefore new challenges arise. High levels of automated driving must operate completely on their own. The driver will no longer be available as a fall-back factor and the system itself must be able to guarantee functionality in all situations. Appropriate fault handling can be ensured, for example, by redundancy at system level. Not only the electronic components for automated driving and the operating software must support the high reliability demands, also the power supply system and communication networks must be designed accordingly.

In the area of energy supply, it is of crucial importance to design a robust power supply architecture. Many possible topologies and diagnostic concepts are available when designing power supply networks. Therefore, a general topology concept must be first determined. The best topologies suited for next generation vehicles should be robust against faults. As shown in [1], many combinations of different voltage levels, converter concepts and energy sources may have their own advantages and disadvantages. Among other things, energy converters, energy storage and energy consumers are considered [2]. Furthermore, the choice of the diagnosis and protection concept is another important question. It should be assessed whether robust detection, identification, localization, and fault handling is possible [3]. Whether a power supply system can maintain its function even in the event of a fault (fail-operational) is an important question. Faults in the power supply system can occur at various fault locations at any time [4]. A wire protection, for example, can be a melting fuse. In future, melting fuses are expected to be completely substituted by electronic fuses which are considered in this work. All these aspects factor into the final realization of a power supply network. Systematic analysis of many power supply architectures with various operating strategies is needed and the voltage stability needs to be evaluated for the overall system. Therefore, designing a robust power supply network while considering all influences to evaluate the systems robustness is no trivial task. At this point, simulation can be a solution to quickly examine parameter variations and overall energy supply concepts.

Due to the high complexity, modelling every relevant detail of a real system may not be practical. **H**ardware **i**n the **l**oop testing (**HiL**) is a common approach for functional testing of electronic components and systems [5]. Electronic components are operated in an emulated environment controlled by simulation models and behaviour of HW and SW is analysed under different operating conditions [6]. Also, failures are taken into account. Failures of the supply system are often emulated according to ISO 16750 [7] or ISO 7637 [8] where typical fixed voltage profiles over time are given. Testing against such voltage profiles is important but reality can be more complex. For each vehicle an individual power supply system is developed, leading to a specific failure behaviour with significant variations in the failure voltage profiles. Only individual testing could give a final answer if requested reliability is given or not.

The presented work proposes a step towards more realistic testing by enhancing HiL testing with supply system simulation and an emulation system for injecting the supply faults into the electronic components. Special attention should be paid to the on-board communication system.
In the case of highly automated driving features, the communication network must be robust against faults in the same way as the on-board power supply system to ensure the needed safety. Therefore, many different realisations of an on-board communication network can be pursued. Hence, different bus systems must be taken into consideration. The scope of this paper won't discuss the selection of a suited on-board communication network for advanced safety features but will focus on the effects of power supply faults on the communication system.

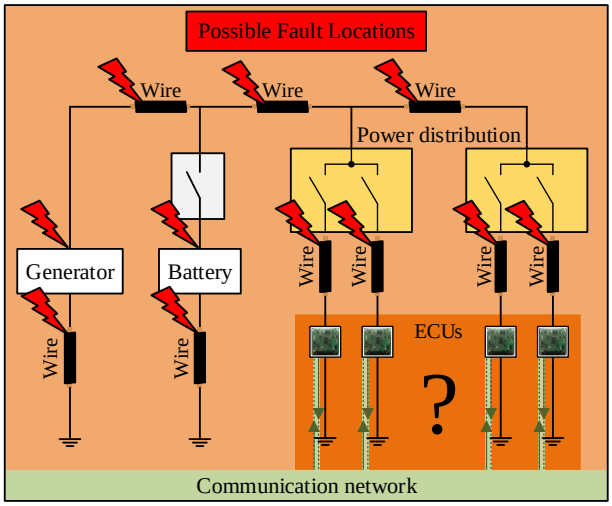

Figure 1: Interaction between the power supply system and the communication network to be evaluated

Figure 1 illustrates the described problem. A component communicating safety critical information could be exposed by various power supply faults at various fault locations.

A simplified power supply network can be seen. The power supply network consists of a starter generator, a battery, two **p**ower **d**istribution **u**nits (**PDU**'s), **e**lectronic **c**ontrol **u**nits (**ECU**) and wires to connect the components. In the overall system various faults can occur. A wiring fault, for example a short circuit, can happen at any location in the power supply system. Also, component faults must be considered. For example, a faulty generator control can lead to a rise in the overall supply voltage of the system and possibly cause malfunctions of a safety critical component.
The interaction between the communication network and the power supply system during fault exposure must be identified. It must be assessed whether a safety critical component is able to transmit safety critical information, for example environment sensing information, even in the event of a fault.
The paper is structured as follows. At first, the overall simulation based testing concept is described. A 12 V power supply network with a redundant power supply concept is chosen. This power supply system is used for demonstration of the overall concept of the test environment for the analysis of real hardware's behaviour during power supply faults. A simulation model is derived from the description of the 12 V power supply network. The simulation model is used to perform a fault simulation in the energy supply system. Taking the interaction between the power supply system and the communication network into account, the simulation results are used to supply a **d**evice **u**nder **t**est (**DUT**) under these fault conditions and the communication lines of the DUT are evaluated.

2 Overall Simulation Based Testing Concept

In this chapter, an exemplary power supply architecture is selected to demonstrate the overall concept. The behaviour of selected components during complex power supply faults should be analysed. For this purpose, a simulation model must be developed. This model should be able to

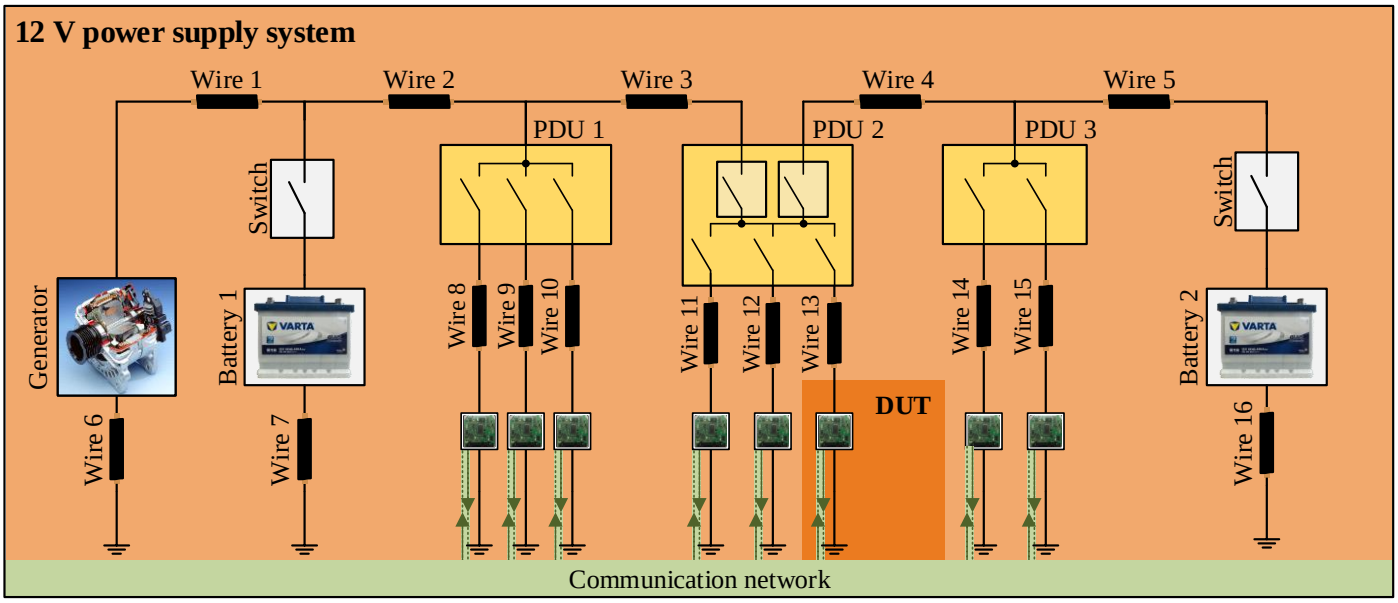

Figure 2: Exemplary power supply system

simulate various faults of the system. Simulations of possible faults give voltage signals at the different components. These voltage signals are the input for the **a**rbitrary **w**aveform **g**enerators (**AWG**) with amplifiers for the independent flexible supply of critical components.

2.1 Power Supply System

Figure 2 shows the exemplarily selected 12 V power supply system for demonstration. The system consists of two batteries which could be placed in the front and the back of a car. The two batteries enable a possible redundant supply concept. A generator is used to deliver electrical power for the electronic components and charge the batteries. Several PDUs are used to distribute the power to the various components and disconnect them in the event of a fault. PDU 2 can connect the left and right part of the electrical system in the case of an undervoltage in either partial system. In the investigated scenario, the right switch of the PDU is open, and the partial electrical systems are not connected to each other. The left switch is closed to supply the components connected to the PDU. If the voltage on either side drops below a critical threshold, the switch will be closed, and the partial electrical system will be connected to each other. If the voltage can be stabilized by closing the right switch, the partial electrical systems remain connected. In the overall system all switches can be semiconductor switches or relays. One of the loads on PDU 2 is assumed to be a safety critical load and connected to the communication network. This load is the DUT and is connected to the communication network. The communication network is used to exchange safety critical information, for example the sensor information of the environment sensing, which needs to be robust against faults. Thus, the behaviour and the influence of a power supply fault on the communication lines of this consumer needs to be investigated.

2.2 Modelling of the Power Supply System

The simulation environment is implemented in Matlab/Simulink and is partly based on modelling concepts presented in [9] and [10]. The models for wires, batteries and the generator model are derived from the reports. Figure 3 shows the model of the power supply system.

The components supplied by the PDUs are modelled as purely ohmic or a mix of ohmic capacitive loads which simulates the static behaviour and a voltage stabilizing capacitor of a typical electronic control unit (ECU). A purely resistive load can be used to model a component like the rear window heating. The generator is assumed to deliver a maximum current of 150 A. The batteries are also modelled with resistances and capacities which simulate the internal resistance of the battery as well as the dynamic behaviour. The parameters for the RC-elements are typical for a battery with a capacity of 80 Ah [11]. The capacitors have values of $C_1 = 1\,\mathrm{F}$ and $C_2 = 300\,\mathrm{F}$. The resistors have values of $R_1 = R_2 = 3\,\mathrm{m\Omega}$. The internal resistance R_3 of the batteries is is assumed to be $30\,\mathrm{m\Omega}$. The **S**tate **o**f **H**ealth (**SoH**) and **S**tate **o**f **C**harge (**SoC**) of the battery can be assumed to be constant for fault simulations since the simulation times are only a couple of seconds [12]. The switches in PDU 2 are modelled as two anti-serial MOSFETs (refer to [1]) and the right switch of the PDU is used to connect the partial electrical systems when the voltage on the left side drops below 6 V. The DUT in this case is also modelled with a capacity to stabilize the input voltage and a resistor to model the static power consumption. The wires are modelled by their resistive and inductive behaviour [13]. Copper is used as the wire material to calculate the resistance in dependence of the length and cross section area. The inductances are estimated to $1\,\mu\mathrm{H/m}$. For Fault simulations various fault models (e.g. a short circuit or an open circuit) have been implemented. For example, a simple model for a short circuit consists of a resistor

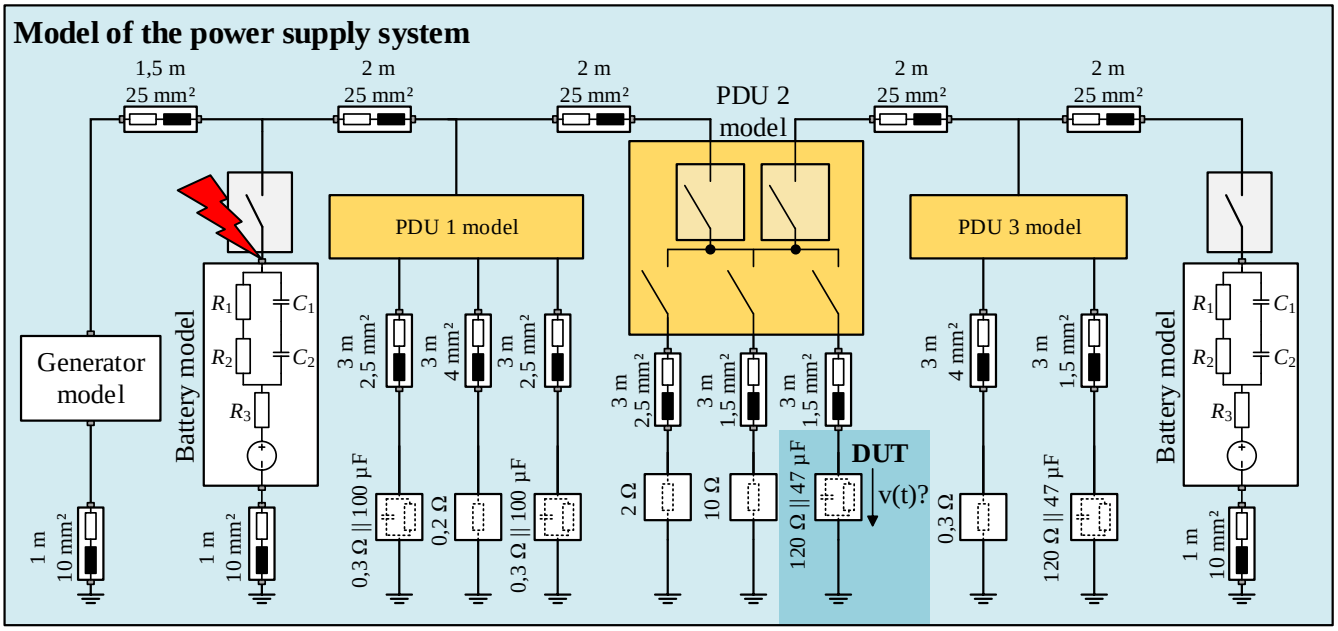

Figure 3: Power supply system model

switching from a high impedance to a low impedance. Finally, fault simulations can be performed, and the voltage stability can be analysed.

2.3 Emulation Concept

The simulation is performed and delivers the voltage $v(t)$ directly at the DUT. This voltage should now be emulated by a hardware setup. Figure 4 shows the emulation concept.

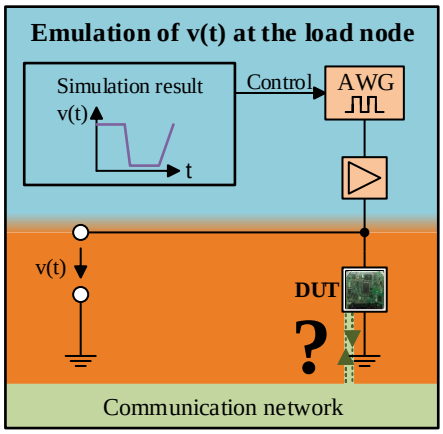

Figure 4: Emulation concept

The simulation results are converted to a waveform for the AWG and the AWG delivers the control voltage for a power amplifier that finally generates the simulated supply voltage $v(t)$ obtained at the investigated ECU. The communication of the DUT is analysed.

3 Proposed Voltage Emulator

In this section, the emulator hardware setup and the necessary control process is summarized. Figure 5 shows the setup.

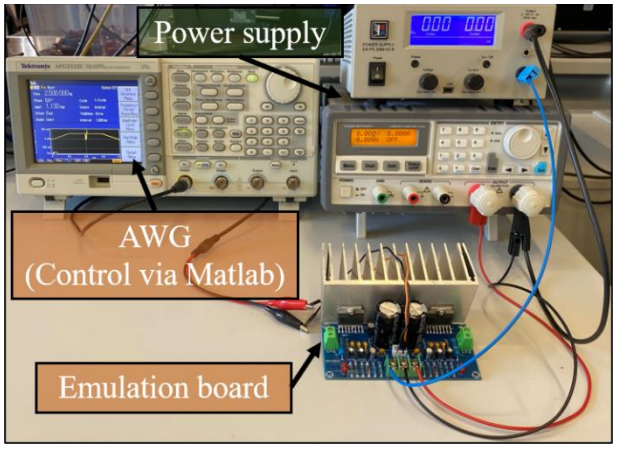

Figure 5: Photo of the test setup

The test setup consists of an AWG (Tektronix AFG 3152C) which is controlled by a PC with Matlab. The necessary control signals for the amplifier are directly converted by a script which loads the simulation results and converts them for use with the AWG. The power amplifier used in this setup is a modified Class-AB audio amplifier which can apply voltage changes in the range of 7 V/µs. The emulator is capable to amplify DC signals. It uses two TDA7293 IC's in a parallel configuration which can supply voltages in a range from -50 V to +50 V and currents up to 13 A (6,5 A per IC). Using additional boards in parallel can emulate even the voltage waveforms of high-power ECUs. The voltage gain of the amplifier amounts 30 dB which is further used to calculate the necessary control signals. Finally, the amplifier is driven by two power supplies to be able to generate the needed voltages in range of $\pm$ 50 V.

4 First Demonstrator

For demonstration, the communication of a microcontroller featuring a CAN-bus communication is investigated. First the DUT and the associated communication setup is presented. Then, a concrete fault scenario for the simulation model is described. The emulation of the power supply system is compared to the simulation result and the communication lines during the exposure are evaluated.

4.1 Simplified ECU

As simplified ECUs two Atmel microcontroller development boards are used. Such components can easily be extended to behave like a real automotive ECU. The microcontrollers are assumed to exchange information over a CAN bus communication. As CAN transceivers 3,3 V CAN bus transceivers (SN65HVD230) are used. The second microcontroller development board is used to read messages from the first one. At the first microcontroller board, the voltage is varied, i.e. it is the DUT. The CAN bus uses a transfer rate of 500 kBits/s. Accordingly, a full CAN frame takes 160 µs to send. The board sends a new frame every 200 µs. Therefore, the CAN bus load amounts 80 %. The current consumption of the microcontroller boards is 100 mA and the input capacitor has a size of 47 µF. Therefore, the DUT is modelled as a 120 Ω resistor in parallel to a 47 µF capacitor (see Figure 3).

4.2 Simulation of the Fault Scenario

In this section, the investigated fault scenario is described. Critical faults can take place in the energy supply path. Therefore, a short circuit at the left battery (see Figure 3) is considered below. Figure 6 shows the simulation result. The short circuit is assumed to appear at 0 ms.

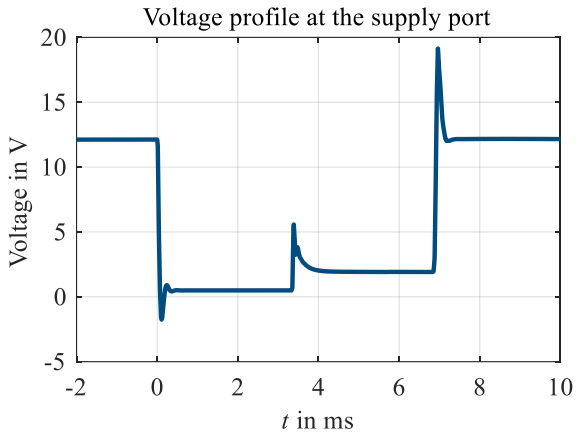

Figure 6: Simulation result

As described in chapter 2.1, the left switch of PDU 2 is closed and the right switch to connect the partial electrical systems is open before the fault is injected. Therefore, the voltage at the load will first drop to approximately 0,5 V. Then, it is assumed that after 3 ms the switch of PDU 2 connects the partial systems. The voltage rises to around 2 V with a short peak voltage of 5 V. Finally, the electronic fuse at the battery detects and isolates the fault and the short circuit is disconnected after another 3 ms. Due to the switching of the fuse, the voltage shows a peak at around 20 V and returns finally to 12 V.

4.3 Emulation of the Fault Scenario

The fault voltage found in the simulation described in 4.2 is used now as supply voltage for the DUT microcontroller board. The comparison of the simulation results with the measured voltage at the input terminals can be seen in Figure 7.

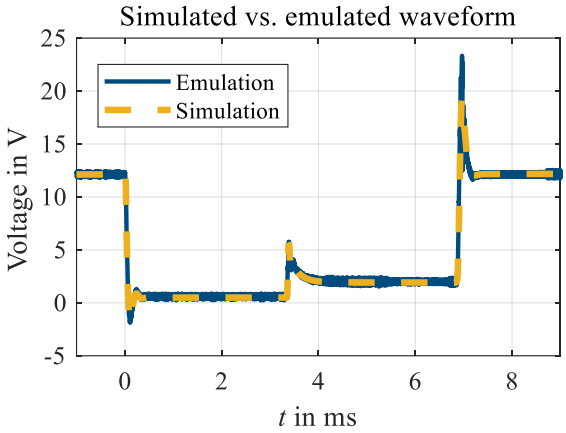

Figure 7: Comparison of the emulated and simulated waveform

A deviation in the peak voltage after the triggering of the battery fuse can be observed. This is because the microcontroller board is a very low power load and the amplifier cannot control the voltage jump of such small loads. A better controller would be required to reduce the overshot.

4.4 Assessment of the Communication

In the last step, the communication is analyzed. Therefore, the CAN-High and CAN-Low signals are measured, and the differential signal is calculated. Figure 8 shows the comparison of the emulated power supply voltage, the internal DUT voltage as well as the differential CAN bus signal.

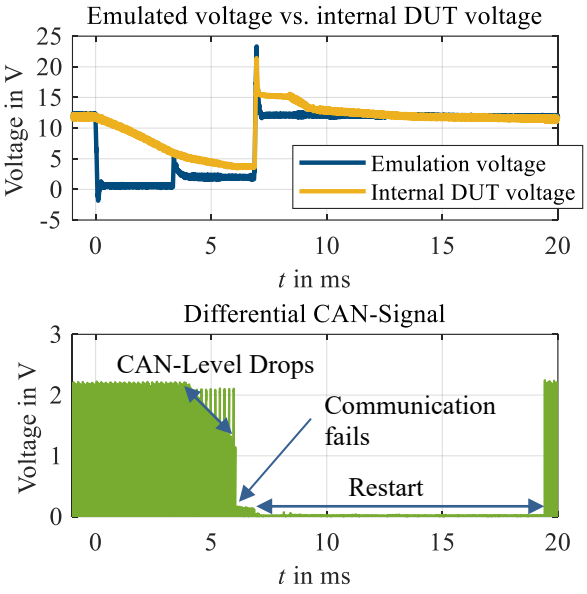

Figure 8: Evaluation of communication under emulated supply conditions

The internal DUT voltage is measured after the protection circuit of the microcontroller board. The microcontroller board has an internal reverse polarity protection diode. Therefore, the internal DUT voltage varies from the emulation voltage at the input terminals. The internal DUT voltage offers a better understanding of what is happening on the communication lines.
The reverse protection diode prevents the input capacitance from discharging over the emulation board. Therefore, the internal voltage drops slower than the emulated voltage at the input terminals. After reaching approximately 5 V, the differential CAN-level drops slowly as well. At about 6 ms the communication fails and the DUT cannot send messages anymore. Even though the supply voltage rises again, the DUT still needs 13 ms until it has restarted. During the exposure of the fault, the communication fails for a total of approximately 14 ms.

5 Conclusion and Outlook

In this contribution a new model-based test setup for the detailed analysis of electronic system's behaviour during complex power supply faults has been introduced.
An exemplarily power supply system has been presented and a model for this system has been derived. The model-based fault analysis offers a much wider range of fault scenarios than the commonly used test standards can provide. Using this information for feeding a voltage emulator a link

to the real ECUs is given. Testing of ECUs can be closer to the real threads. Critical faults can be identified, and safety critical systems can be tested during the occurrence of realistic faults.

The concept was demonstrated based on a laboratory application example. The fault simulation results are converted to a waveform for an AWG and the AWG delivers the control voltage for a power amplifier feeding the ECU. As a demonstrator an Atmel microcontroller development board was used to show the behaviour on the CAN-bus communication lines during the fault exposure.

It could be seen that even small undervoltage periods can be critical to communication and messages can be lost during the fault exposure. A possible restart of the component due to an undervoltage pulse can delay the reestablishment of the communication.

The power amplifier offers a modular application which also allows this concept to drive high power loads in future investigation. The behaviour of various components under different fault conditions can be evaluated.

6 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.

7 Literature

[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] 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.

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

[5] P. Baracos et al., “Enabling PC-based HIL simulation for automotive applications," IEMDC 2001, IEEE International Electric Machines and Drives Conference, Cambridge, MA, USA, 2001, pp. 721-729.

[6] J. Chalupa, R. Grepl and V. Sova, “Design of configurable DC motor power-hardware-in-the-loop emulator for electronic-control-unit testing”, 2015 21st International Conference on Automation and Computing (ICAC), Glasgow, 2015, pp. 1-6.

[7] ISO, “ISO 16750-2 Road vehicles – Environmental conditions and testing for electrical and electronic equipment – Part 2: Electrical loads”, 2012.

[8] ISO, “ISO 7637-2 Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only”, 2011.

[9] P. Schwarz, J. Haase, “Erstellung einer VHDL-AMS Modellbibliothek für die Simulation von Kfz-Systemen“, FAT Schriftenreihe, vol. 207, 2006.

[10] VDA/FAT 334, “Simulationsgestütze Analyse und Bewertung der Fehlertoleranz von Kfz-Bordnetzen“, FAT Schriftenreihe, vol. 334, 2020.

[11] M. S. Bechteler, C. M. Scheßl and T. F. Bechteler, “Electrical Power Net Systems in Cars – Impedance Modeling and Measurement“, IEEE Transactions on Vehicular Technology, vol. 59, no. 3, pp. 1148-1155, March 2010.

[12] F. Ruf, “Auslegung und Topologieoptimierung von spannungsstabilen Energiebordnetzen“, München: Technische Universität München, 2014.

[13] J. Wang, “Simulationsumgebung zur Bewertung von Bordnetz-Architekturen mit Hochleistungsverbrauchern“, Kassel: Universität Kassel, 2016.