EVS30 Symposium
Stuttgart, Germany, October 9 - 11, 2017

Dimensioning of Power Net for Automated Driving

Tunan Shen[1], Ahmet Kilic[1], Kirill Gorelik[1]

[1]*Robert Bosch GmbH, Renningen, Germany*

Email: {tunan.shen, ahmet.kilic, kirill.gorelik}@de.bosch.com

Summary

For automated driving, the reliable power supply (power net) for safety critical components, e.g. braking and steering systems, must be guaranteed. However, the availability and robustness of the state of the art power net design cannot fulfil the increased requirements for automated driving systems. This paper introduces a fail-operational power net topology and presents a simulation-based method for dimensioning the power net components, such as DC/DC converters and 12V batteries. Based on the simulation results, the reliability of the power net is quantified, the optimal dimensioning of the power net components are determined and new functional requirements are derived.

Keywords: automated, EV, simulation, energy, power

1 Introduction

According to the definition of conditional and high driving automation in the **S**ociety of **A**utomotive **E**ngineers (SAE International) [1], the driver is allowed to deal with other tasks during the trip without focusing on the vehicle control. Hence, if a sudden component failure leading to the deactivation of the automated driving system occurs, the driver might not be available to take over the control of the vehicle immediately. In this case, the automated driving system should give the driver sufficient time for taking over the control. If the driver does not take over the control, the system should bring the vehicle to a minimal risk condition and ensure the safety of the passengers in the vehicle and its surroundings. In other words, the system should still operate despite a failure, which is the so called fail-operational behaviour. For fulfilling the system fail-operability, much more effort must be invested in the system design. The behaviour of the components, subsystems and the system in total must be analysed for the case of a sudden failure. The electrical power supply system (power net) provides the energy for all electrical components in the vehicle, including the automated driving system. However, the state of the art power net topology cannot fulfil the requirement for fail-operability. For this reason, new fail-operational power net topologies for automated driving as well as a method for optimal dimensioning and sizing of its components are required.

2 Functional Safety and Legacy Requirements

Since the driver is not always available as a for executing the fall-back driving task in automated driving systems, the safety requirements of power supply availability and robustness increase dramatically [2, 3, 4]. The power net system must be developed in accordance with the norm ISO 26262:2011 [5], requiring the failure analysis of the whole power net system with respect to the loss of power supply of safety-related

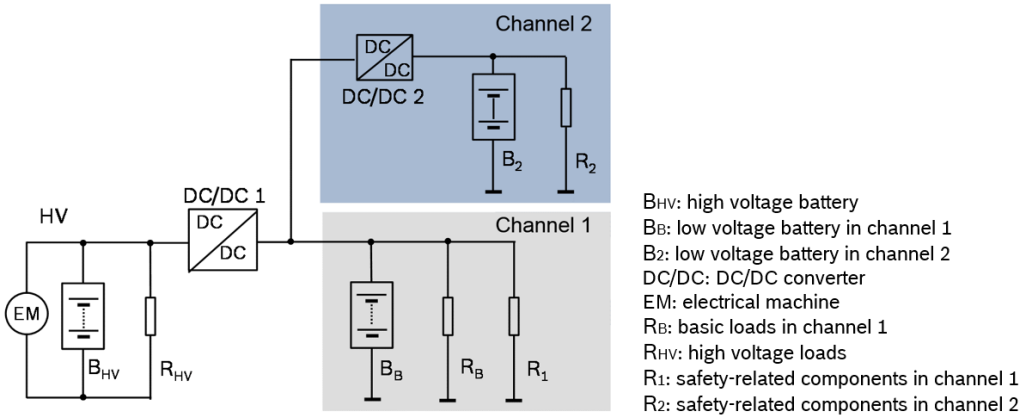


Figure 1: Fault tolerant power net topology for automated driving

sensors, electronic control units (ECU) as well as actuators needed by the automated driving system. Different system faults (safe faults, single-point and multiple-point faults) must be identified, an appropriate safety concept must be developed, the diagnostic coverage as well as the ability of safety mechanisms to avoid single-point faults must be evaluated.

Additionally, the power net system design must conform to the legacy regulations. ECE R13-H [4] requires two independent braking systems (including energy reserves). In ECE R79 [6], the availability of the steering system is required in case of an energy source failure or a failure within the energy transmission. Each of these two legacy regulations requires redundant energy storages. Furthermore, it is highly recommended to use various sensor technologies and ECUs for advanced driver assistance system (ADAS) in order to improve the recognition of the environment. A redundant design of these systems as well as of their power supply is required despite no law or regulation currently enforces this [7].

The state of the art power net does not have redundency and cannot fulfill the functional safety and legacy requirements. For this reason, a fail-operational power net topology for battery electrical vehicles (BEV) was developed. As shown in Figure 1, this topology consists of one high voltage channel and two low voltage (12V) channels. A main DC/DC converter (DC/DC1) transfers the energy from the traction battery to the low voltage channels. DC/DC2 is a 12V/12V DC/DC converter. It connects channel 1 and channel 2 at normal condition and decouples the both channels in case of a failure. A 12V Lead-Acid (PbAc) battery serves as an energy reserve in each 12V channel, stabilizing the voltage and suppling the loads while the DC/DC converters are not available. Safety-related sensors, ECUs and actuators are divided into two groups (R_1 and R_2) in order to fulfil the legacy requirements. R_1 and R_2 form a functional redundancy of automated driving.

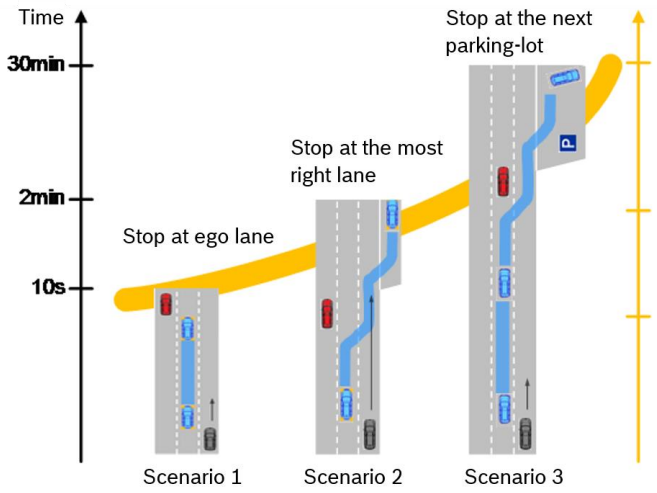


Figure 2: Different safe stop levels (SSL)

The high voltage auxiliary loads (R_{HV}) are supplied by the traction battery, the low voltage auxiliary loads (R_B) by the energy available in channel 1.

In case of a failure in channel 1, DC/DC2 see Figure 1 will be shut down to make sure these two channels are decoupled. The loads in channel 2 will be supplied by B_2 for a defined period of time needed by the system to bring the vehicle to a safe state. Depending on the requirements of the original equipment manufacturers (OEM), there are different scenarios to achieve the safe state. Figure 2 illustrates three scenarios and their required time and energy to achieve the safe state. For example, the vehicle will stop at the current lane in scenario 1. The duration of the safe stop scenario is about 10s and the required energy for supplying the electrical braking system is low. In Scenario 3, the vehicle is able to drive to the next parking-lot automatically and needs much more energy. In addition, the steering system, the sensors and even the propulsion components are needed in Scenario 3 to reach the next parking lot.

3 Power Net Simulation for Normal Operation

The previous section introduced the fail-operational power net topology and the scenarios for reaching the safe state after detecting a failure. After a power net topology is selected, the appropriate power net components must be dimensioned. In conventional vehicles with internal combustion engine (ICE), electrical power is generated by the alternator. It transforms the mechanical power of the engine to electrical power and provides the energy for all the electrical loads in the vehicle. The 12V battery is used to start the engine, to stabilize the voltage during the trip and to supply the loads while the engine is off. In a BEV, 12V loads are supplied from the traction battery via DC/DC converters. A DC/DC converter is usually controlled by high-frequency pulse width modulation (PWM) signal and has a reaction time of approximately 10ms. Therefore it is able to react much faster than an alternator to possible load dumps or load changes. Furthermore, the 12V battery only needs a very small current to start the electronics in BEV instead of more than 100A for starting the combustion engine. The big difference between conventional vehicles and BEVs results in different design of power net components. A simulation-based method for identifying the right dimensioning of the power net components is presented in this paper.

As shown in Figure 3, the power net topology as depicted in Figure 1 was modelled in Saber [8]. This model consists of batteries (traction battery, 12V batteries), DC/DC converters, cables, fuses and different loads.

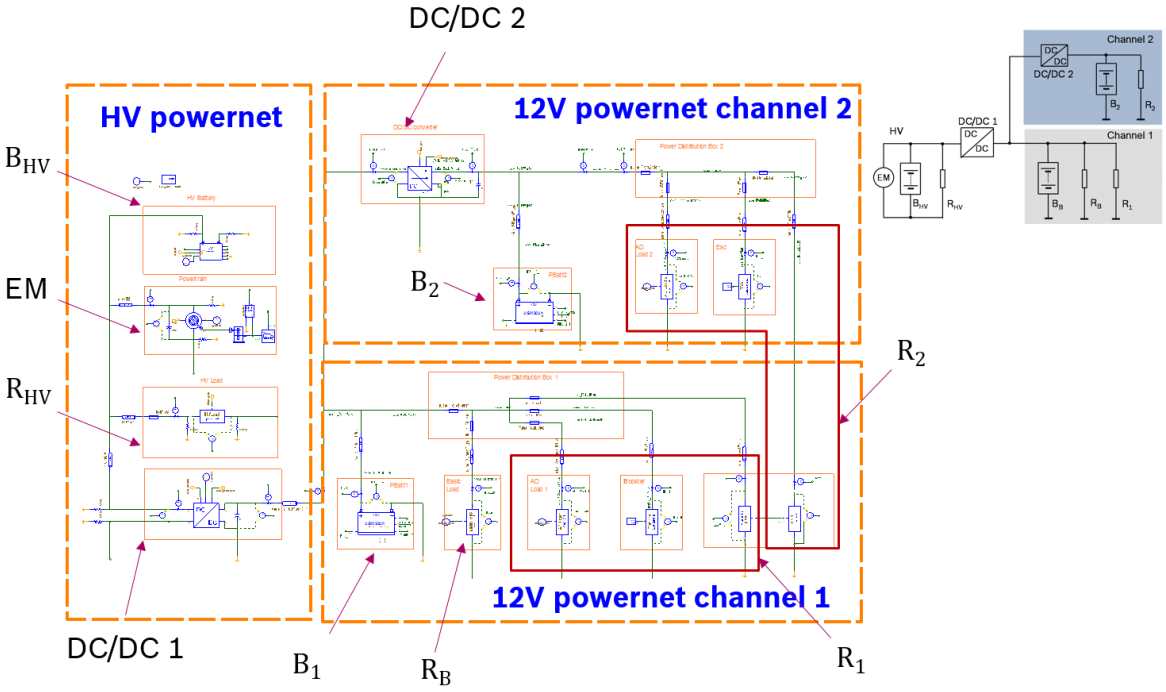


Figure 3: Overview of simulation model in Saber for a BEV

Behavioural models of these components were developed and validated by using measurement data. Using this model, the behaviour of the entire power net in different conditions can be simulated and analysed. Two types of simulations (load balance and voltage stability simulation) are proposed in this paper in order to design the power net in an optimal way.

3.1 Load Balance Simulation

With the load balance simulation, the energy flow in the power net is simulated and analyzed. The power net must provide sufficient energy to the loads for operating without any derating or degradation during a driving cycle and the batteries must have enough energy reserve after completing the driving task. Different factors such as ambient temperature, time (day or night) and weather (sunny, rainy or snowy) have to be taken into account, since the load profiles, driving situations as well as the behavior of the components are quite different depending on the conditions. Furthermore, different use cases (long trip, short trip, parking, still stand without HV system etc.) also influence the dimensioning of 12V batteries and DC/DC converters. For example, the 12V batteries should supply the hazard lights for at least 3 hours in the case of the inactivity of the HV system. In addition, for extending the lifetime of the 12V PbAc batteries, they should not be discharged below a certain state of charge (SoC) limit.

After defining several use cases and scenarios, the load profiles are determined or measured. Three different types of loads are used in this paper. Permanent loads, such as a battery management system or vehicle control unit, are always active and their energy demand is almost constant during a driving cycle. Long-time loads, such as 12V heating systems (seat heating, rear window heating etc.) are active for a long time and their energy demand can vary over time. Short-time loads are only active for a short time (turn signals, braking system, servo motor for seats etc.). Some of these loads have very high peak power but are only active for a few seconds. Their average energy consumption during the whole driving circle is very low. Considering the duration of the driving cycle and the simulation time step, these short-time loads can be neglected in a load balance simulation.

In the next step, the energy flow in the power net is simulated. In order to find out the optimal combination of DC/DC converters and batteries, the rated power of DC/DC converters and the capacity of the two batteries are varied and several criteria, e.g. the battery voltage and the SoC, are monitored and evaluated. An example of a simulation run at the ambient temperature T=-20°C is depicted in Figure 4. The initial condition of SoC of the two 12V batteries equals 60% and 90% respectively. At the beginning of the test, the power demand of the 12V heating system (R_B) exceeds its maximum after a short time and stays constant for several minutes. As shown in Figure 4, the battery B_1 is discharged to a very low SoC after 20 minutes, since the rated power of DC/DC converter 1 was dimensioned too low and it was not able to provide sufficient energy for all loads in channel 1. In contrast, the SoC of the battery B2 stays at a high level, indicating that the rated output power of the DC/DC converter 2 is sufficient in this case. As a result, higher output power of the DC/DC converter

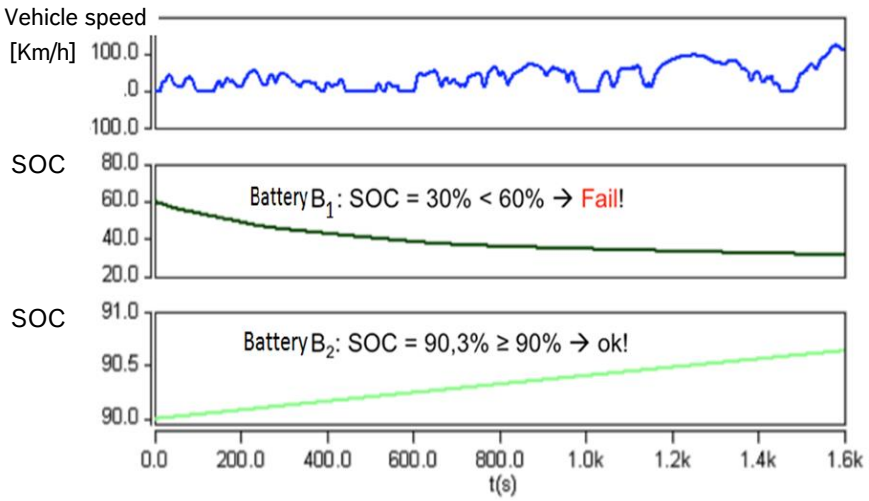


Figure 4: Results of load balance simulation

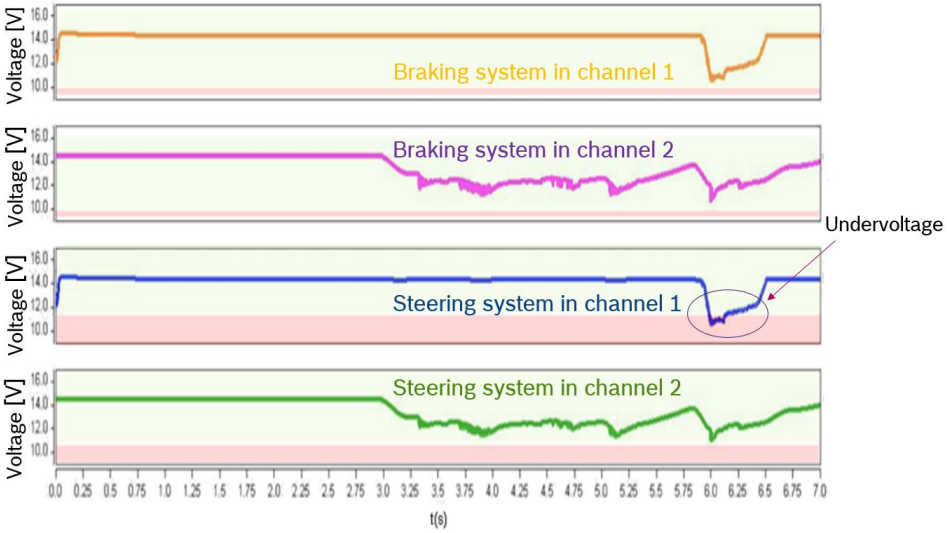


Figure 5: Results of voltage stability simulation

1 is required and it should also be tested for avoiding the overdesign whether a lower rated output power of DC/DC converter 2 would be sufficient.

3.2 Voltage Stability Simulation

In addition to the load balance, the voltage stability is another important characteristic for a power net. By adding new functions to the vehicle, more and more highly dynamic components were integrated in the vehicle. Electrical loads like the electrical stability program (ESP), the electrical power steering (EPS) and the roll stability control require very high peak power (up to 2kW) for a short time and a current slope up to 50A/ms. If the battery is dimensioned too small or the DC/DC converter cannot cover the dynamic load change request in appropriate time, it may lead to unavailability of these safety-related systems due to under/overvoltage, which is not allowed for automated driving. The goal of the voltage stability simulation is to evaluate the functionality of all safety-related systems and to ensure that all components are operating in the specified voltage range even in the worst case.

Based on several vehicle measurements and tests, the worst case load profile of highly dynamic components is identified. During a double lane change test [9], the iBooster [10], EPS and ESP are active at the same time and require a peak current of more than 230A. In addition, critical weather conditions such as snowing night in winter make the situation more problematic [11]. Furthermore, the voltage drop at the wire harness also influences the voltage stability. In order to ensure the voltage stability, the operating voltage of safety-related components is analysed. The most critical loads in vehicles are usually actuators for braking and steering systems. For example, as shown in Figure 5, a test scenario is simulated at the ambient temperature T=-20°C. During the whole scenario, the 12V heating system is active and working at its maximum. From 3s to 7s, the vehicle executes the double lane change test, in which the iBooster [10], EPS and ESP are active simultaneously with a resulting peak current at t = 6s. The orange and blue curves show the operating voltage of braking systems in channel 1 and 2, the purple and green curves of the steering systems. A decrease of the voltage in channel 1 (orange and blue) and channel 2 (purple and green) can be seen. The blue curve drops under a defined threshold, meaning that the actuator of steering system in channel 1 cannot operate with required power. A well-designed power net should ensure the functionally of all safety-related components and avoid possible over- or undervoltage. As a result, the dimensioning of the DC/DC converter 1 or battery in channel 1 should be changed in order to fulfil the power requirements. The power distribution between DC/DC converter 1 and battery 1, affecting the sizing and dimensioning of the components, should be also analysed with respect to additional component cost for an optimal solution.

4 Fault Injection Simulation

A fail-operational power net should be operational despite a failure. As mentioned in Section 2, the power net for automated driving must be developed in accordance with the norm ISO 26262:2011 [5]. Hardware or software failures of a fail-operational power net system which could lead to the loss of power supply of safety-related components must be analysed. The probability of system malfunction must be evaluated. If the failure rate is higher than required by the norm, additional safety mechanisms avoiding the system malfunction must be defined and implemented. For example, using better components can reduce random failure in the hardware. A redundant hardware design can also reduce the failure rate of the whole system. Reliable diagnostic concepts detecting possible failures in advance and allowing to execute the fall-back driving scenario before the power supply breaks down increase the system reliability as well. In this section, a method of analysing the power net behaviour in case of a failure is presented. First of all, hardware failures and their impact on the power net are analysed at component level. The impact of single component failures can be grouped to several failure classes at the system level, which are then modelled in the simulation. After that, the defined failure classes are injected during the simulation and the power net behaviour as well as the defined fault reactions are simulated in Saber. After executing a set of fault injections covering all possible failure combinations, the total failure rate leading to system malfunction can be determined.

4.1 Failure Analysis at the Component Level

The entire power net is a complex system. It is not possible to simulate every single hardware failure at the component level. Analysing the hardware failures at the component level and grouping them to several failure classes helps to reduce the complexity. In the automotive industry, several methods like the fault tree analysis (FTA), the failure mode and effects analysis (FMEA) or the failure modes effects and diagnostic analysis (FMEDA) are used. In this work, FTA is applied for estimating the failure rate of the defined failure classes. Figure 6 illustrates the fault tree for the failure class “no energy transport from HV channel to 12V channel” of the DC/DC converter 1 as an example. A failure class builds the so called top event of a fault tree (see abstraction level 1 of Figure 6). Starting with the top event and using the Boolean logic (AND-gate, OR-gate etc.) the fault tree is built with the top down approach ending with the single component failures, the so called basic events. Different levels of abstraction might be used for increasing the readability and comprehensibility of the fault tree. As an example, three abstraction levels are shown in Figure 6. In this example, the abstraction level 1 contains three different sub events which might lead to the top event. The sub events are connected using the OR-gate, meaning that each of this sub events can cause the top event. The cause of these three sub events is then analysed at the next lower level of abstraction. As already mentioned, the fault tree ends with its leaves, the basic events, which are coloured red in the Figure 6. These are the faults of the hardware parts of the DC/DC converter 1 (e.g. short circuit of a resistor). Finally, based on the failure rates of the basic events, the failure rate for the failure class (the top event) can be determined.

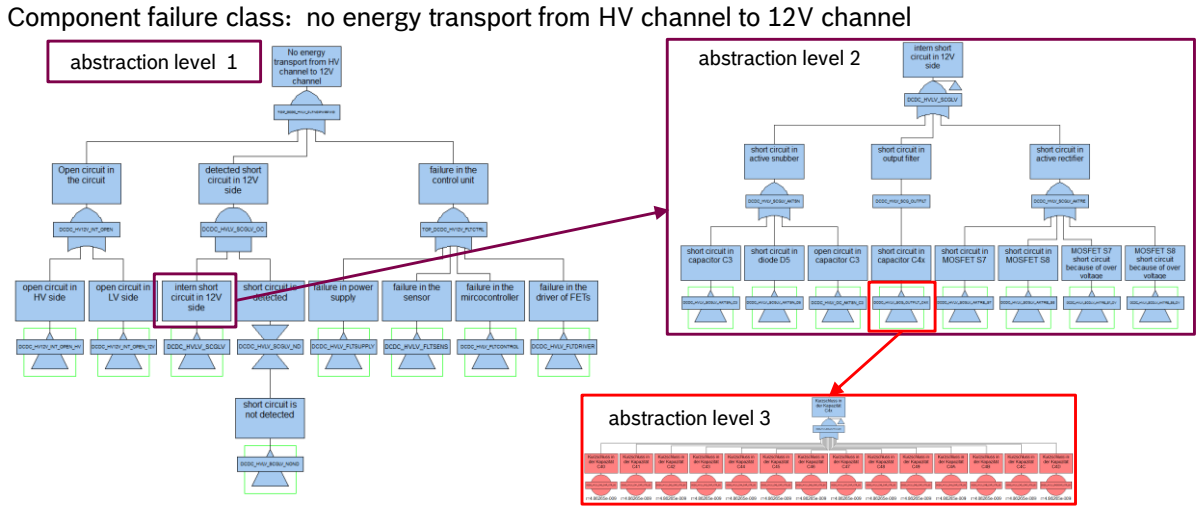


Figure 6: Fault Tree Analysis

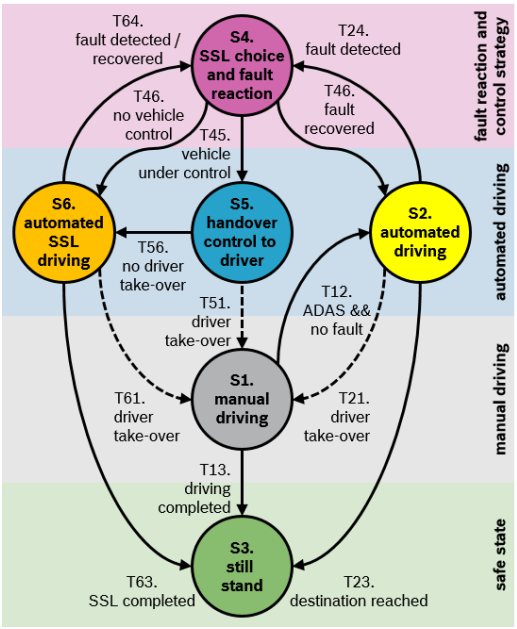


Figure 7: Safety concept

The failure rate of the basic events depends on the operational conditions and can be determined by using the standards or handbooks for reliability prediction like Siemens SN 29500 [11] or MIL-HDBK-217F [12] or by using the data acquired from the field by the quality management. A failure of one component in the power net could cause one or more top events with the impact on reliable power supply for safety critical components.

4.2 Failure Analysis at the System Level

At the system level, the impact of each failure class is analysed using the fault injection simulation. For this, the defined failure classes at the component level must be modelled first. Typical failures like short or open circuit between two nodes can be modelled as a connection with very low or very high resistance. For other failures, e.g. limited output power or failure in a control system, the simulation parameters of the model must be changed.

In the second step, a safety concept which was developed in the concept phase in accordance with ISO 26262:2011 [5] needs to be implemented in the simulation model, meaning that the fault detection as well as the defined fault reactions must be modelled. Figure 7 depicts the transition between different states of an automated driving system. The automated driving can be started if no fault is detected (transition from state 1 to 2). If a fault is detected by the system during the trip, the system will automatically transition to the state 4, in which the fault reaction is initiated. Based on the current system state, an appropriate level of fall-back driving task will be selected. In case the vehicle is under control, the driver will be requested to take over the control (transition T45), otherwise the fall-back driving task will be started automatically (transition T46). The main goal is to bring the vehicle to a safe state and ensure the safety of the passengers in the vehicle and the persons in the surroundings.

After modelling the failure classes and the safety concept, the failure classes can be injected and the system behaviour can be analysed using the fault injection simulation. The system state must be continuously evaluated by checking whether the safe state can be reached or not. More details on fault injection simulation can be found in the next subsection.

4.3 Fault Injection Simulation

The goal of the fault injection simulation is to analyse the impact of the failure classes on the power net behaviour as well as to verify the defined fault reactions. Figure exemplifies the procedure of the fault injection simulation for the failure class “short circuit to ground in channel 1”. The simulation starts with a

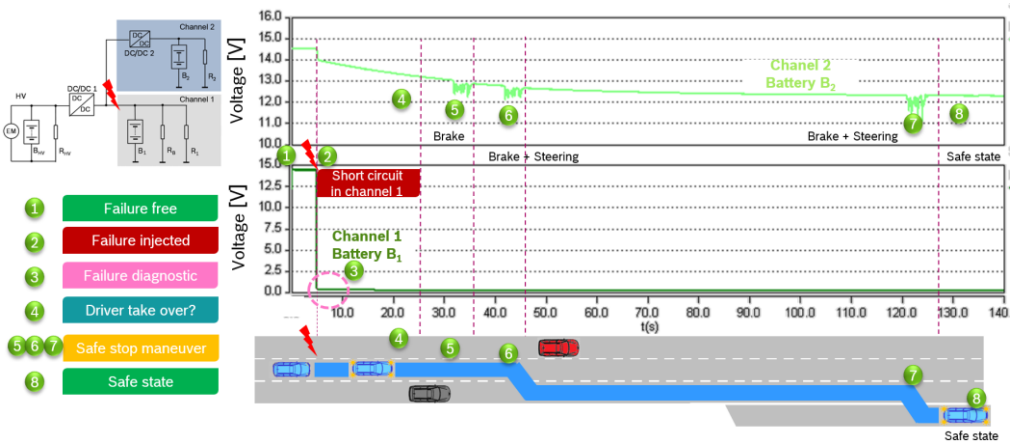


Figure 8: Failure simulation

failure free condition. At point 2, the failure is injected into the power net and the battery voltage in channel 1 immediately drops to 0V. It is assumed that the system needs several seconds to detect this failure. After detection of the failure at point 3, the automated driving system needs to be stopped. The system will request the driver to take over the vehicle control and wait for a defined period of time at point 4. If the driver does not take over the control, the automated driving system will then complete the safe stop maneuverer defined in the safety concept in the automated mode. In the example shown in Figure 8, the vehicle will change the lane twice and stop automatically at the emergency lane.

A fail operational power net should provide sufficient energy and power to the safety critical components required for transitioning the vehicle to a safe state. During the simulation, the functionality of the safety-related components is evaluated. If over- and/or undervoltage is detected in both channels during the simulation, the automated driving system is considered to be failed, since the safety critical components cannot be operated in the specified voltage range. An undetected short circuit to ground (single failure) for instance would discharge both low voltage batteries (B_B and B_2) and lead to a system breakdown. Also two independent failures occurring at the same time in different low voltage channels might lead to a system breakdown as well. In this case, the failure rate for the undetected single failure and for the double failures should be evaluated with the method described in Section 4.1. If the overall system failure rate estimated based on the simulation results is higher than required in accordance with ISO 26262:2011 [5], the design and/or the safety concept of the power net should be adapted. For example, additional safety mechanisms enhancing the failure diagnostic coverage could be applied for increasing the system reliability.

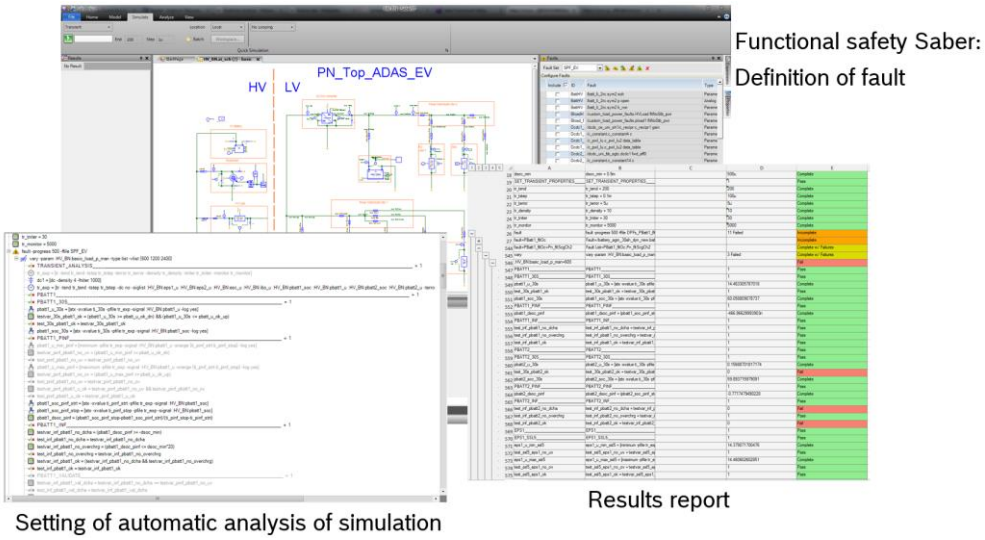


Figure 9: Overview of Saber functional safety toolbox

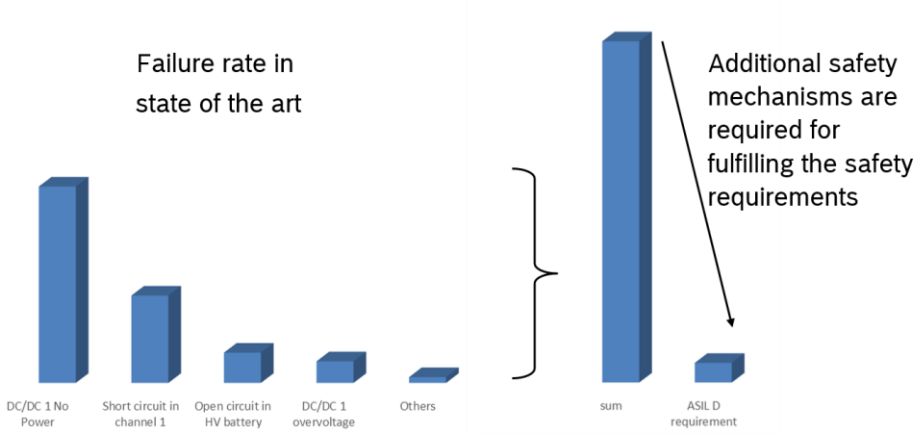


Figure 10: Failure rate of power net

According to the ISO 26262:2011 [5], the analysis of dual-point faults is sufficient. For simulating the dual-point faults, the combination of two failure classes must be injected in the simulation. In addition, different weather conditions lead to different energy demands of basic loads (heating and air conditioning). The probability of different energy demands should be taken into account. In this work, 30 failure classes leading to 900 failure combinations are evaluated. Due to the large number of simulations, only three different values for the energy demand of basic loads are considered, resulting in 2700 simulations in total. Using the Saber functional safety toolbox, a high number of simulations can be executed in automated mode and the simulation results can be exported as a report to Excel, simplifying the further evaluation. Figure 9 shows an overview of this toolbox.

After executing the fault injection simulations and evaluating the simulation results, most critical failures leading to the breakdown of the power net are identified. Figure 10 shows the estimated failure rates of the failure classes for the power net topology as depicted in Figure 1 by using state of the art components and safety mechanisms. The total power net failure rate (sum of all failure rates) exceeds the maximum allowed value defined by ISO 26262:2011 [5] for ASIL D, which is only 10 FIT (FIT= 10^9 device-hours of operation) over a typical life cycle of 15 years for a vehicle. In order to fulfil this requirement, additional mechanisms must be introduced to reduce the failure rate. This failure analysis shows us that the use of the state of the art components and safety mechanisms is not sufficient for fulfilling the safety requirements for automated driving. New features and functions reducing the failure rate should be implemented.

5 Deriving Component Requirements

In the previous sections, a new fail-operational power net topology for automated driving was briefly introduced. Regarding the new requirements for automated driving, a simulation-based method for dimensioning the power net components was presented. Three different simulations were used for analysing the system behaviour of the power net helping to find the optimal dimensioning for DC/DC converters and 12V batteries. Based on the results from the load balance simulations, the rated output power of DC/DC converters and minimum required capacity of 12V batteries can be derived. The required peak power of the DC/DC converters as well as the discharge ability of the batteries can be determined based on the simulation of the voltage stability. For estimating the reliability of the fail-operational power net, the failure analysis in accordance with ISO 26262:2011 [5] was performed. The behaviour of the power net in case of a failure was analysed and its ability to provide the required energy and power for the safety critical functions needed for executing the fall-back driving task was verified. After evaluating the most critical failures leading to the malfunctioning of the power net, new requirements for power net components in order to reduce the total system failure rate were identified.

6 Conclusion

It is shown that automated driving requires new power net designs for achieving reliable and robust power supply for safety-related functions. A new fail-operational power net topology for automated driving systems was briefly presented in this paper. Additionally, it was shown which new requirements for power net components arise and how this components can be dimensioned by using the simulation-based approach. The optimal dimensioning as well as the new requirements for the power net components were derived.

In the future work, the fail-operational concept presented in this paper will be evaluated in a test bench and in a vehicle.

References

[1] SAE International, J3016 SEP2016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, United States: SAE International, 2016.

[2] A. Kilic und W. Müller, „Fehlertolerante Bordnetze für autonomes Fahren," in *4. Internationaler Fachkongress Bordnetze im Automobil*, Ludwigsburg, 2016.

[3] J.-L. Augier, T. Huck, A. Kilic und W. Müller, „Efficient, Safe and Reliable Powernet for AD," in *Elektrik/Elektronik in Hybrid- und Elektrofahrzeugen und elektrisches Energiemanagement VII*, Renningen, expert verlag, 2016, pp. 398-411.

[4] United Nations Economic Commission for Europe, „Regulation No 13-H of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of passenger cars with regard to braking [2015/2364]," Official Journal of the European Union, European Union, 2010.

[5] ISO, ISO 26262-3:2011: Road vehicles - Functional safety - Part 3: Concept phase, ISO, 2011.

[6] UN/ECE, Regulation No. 79 UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARD TO STEERING EQUIPMENT, EU, 2005.

[7] H. Winner, S. Hakuli, F. Lotz und C. Singer, Handbuch Fahrerassistenzsysteme Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, Wiesbaden: Springer Vieweg, 2015.

[8] Synopsys, „Saber," Synopsys, [Online]. Available: https://www.synopsys.com/verification/virtual-prototyping/saber.html. [Zugriff am 19 6 2017].

[9] Vehico, "ISO Double Lane Change Test," [Online]. Available: http://www.vehico.com/index.php/en/applications/iso-lane-change-test. [Accessed 19 6 2017].

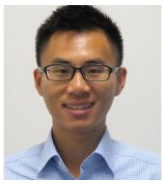
[10] Robert Bosch GmbH, "Bosch Mobility Solutions," Robert Bosch GmbH, [Online]. Available: http://products.bosch-mobility-solutions.com/en/de/_technik/component/SF_PC-CV_BS_Brake-Booster_SF_PC-CV_Brake-Systems_1987.html?compId=1135. [Accessed 21 6 2017].

[11] P. K. Kohler, Prädiktives Leistungsmanagement in Fahrzeugbordnetzen, Wiesbaden: Springer Vieweg, 2014.

[12] Siemens Standard, SIEMENS NORM SN29500, Munich and Erlangen: Siemens AG, 2004.

[13] U.S. MIL Specification, Military Handbook - Reliability Prediction of Electronic Equipment, USA, 1991.

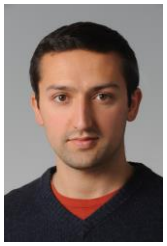
Authors



Tunan Shen was born in Hangzhou, China, in 1988. He received the B.Sc. degree in electrical engineering from the Tongji University, Shanghai, China, in 2011 and M.Sc. degree in electrical engineering from RWTH Aachen University, Aachen, Germany, in 2014.

In 2014, he joined the Robert Bosch GmbH in Corporate Sector Research and Advanced Engineering as a development engineer for powertrain and eMobility systems.

Dr. Ahmet Kilic was born in 1971, studied at the University Magdeburg. After his studies he started at Siemens VDO (Continental AG) as a Test Manager for hybrid vehicle. After 10 years he joined Mercedes Benz Tech and was responsible for the high voltage safety. He came to Bosch in 2012 and is a project manager for the power nets and powertrain in the Corporate Sector Research and Advanced Engineering of the Robert Bosch GmbH.



Kirill Gorelik was born in 1986 and received his diploma degree in electrical engineering from the University of Stuttgart, Germany. After his studies he joined the Robert Bosch GmbH as a hardware developer for transmission control unit. After 3 years he started to work on his dissertation as a Ph.D. student in the Corporate Sector Research and Advanced Engineering at the Robert Bosch GmbH.