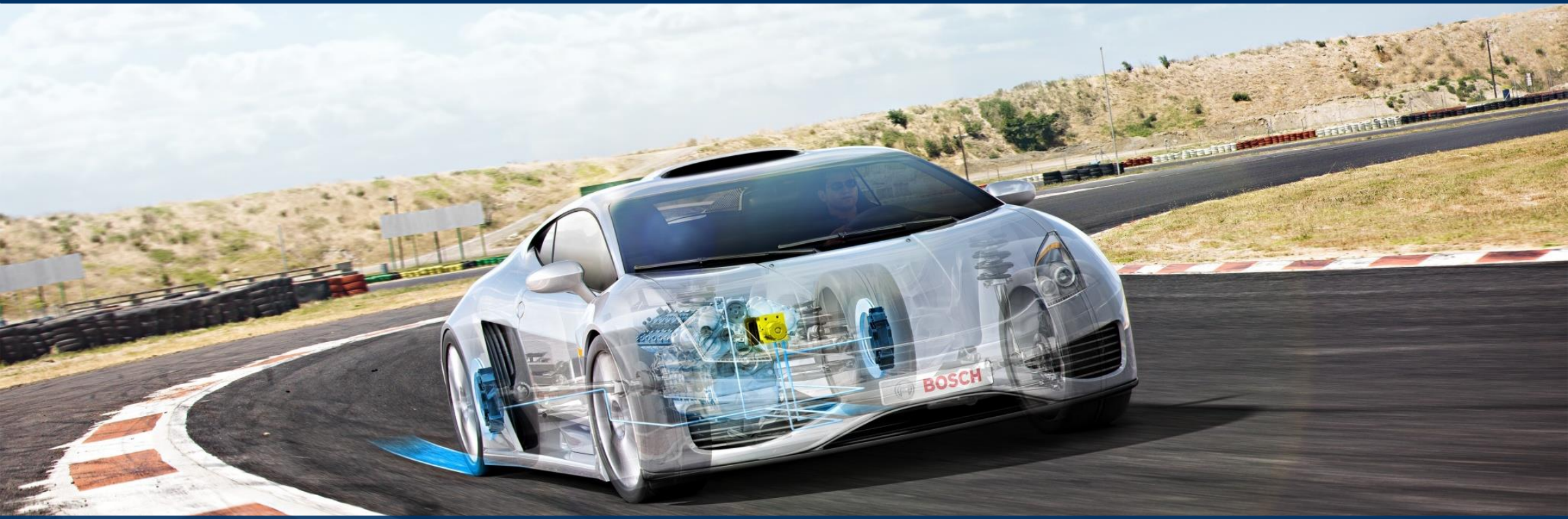


Simulation of Fault Tolerant Power Supply Networks for ADAS Vehicles with SaberRD

Automotive Electronics

BOSCH

Authors

Marco Beckmann
Robert Bosch GmbH, Leonberg, Germany
Automotive Electronics – Body Electronics
System and Architecture Engineering

- System Engineering Power Supply Networks
  - Coordination Modeling & Simulation

Dr. Jürgen Barthlott
Robert Bosch GmbH, Leonberg, Germany
Automotive Electronics – Body Electronics
System and Architecture Engineering

- System Engineering Power Supply Networks
  - Team Manager

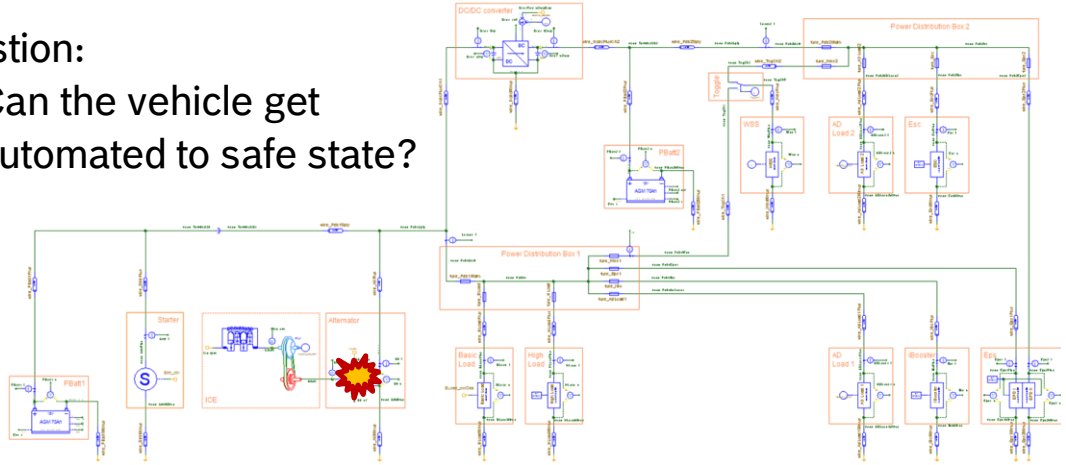
Fault Example: Alternator Breakdown

Situation:

- Alternator fails during running automated highway pilot

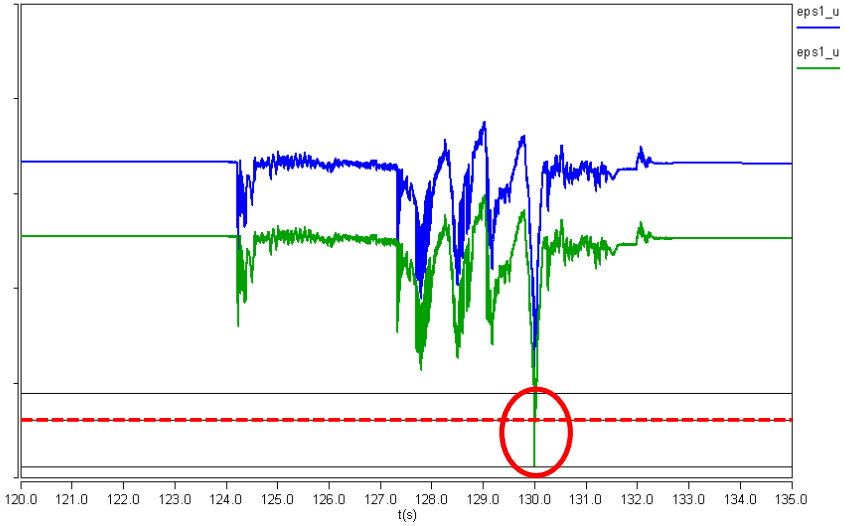
Question:

- Can the vehicle get automated to safe state?



Goal / Safe Stop Scenario:

- Stop at emergency lane



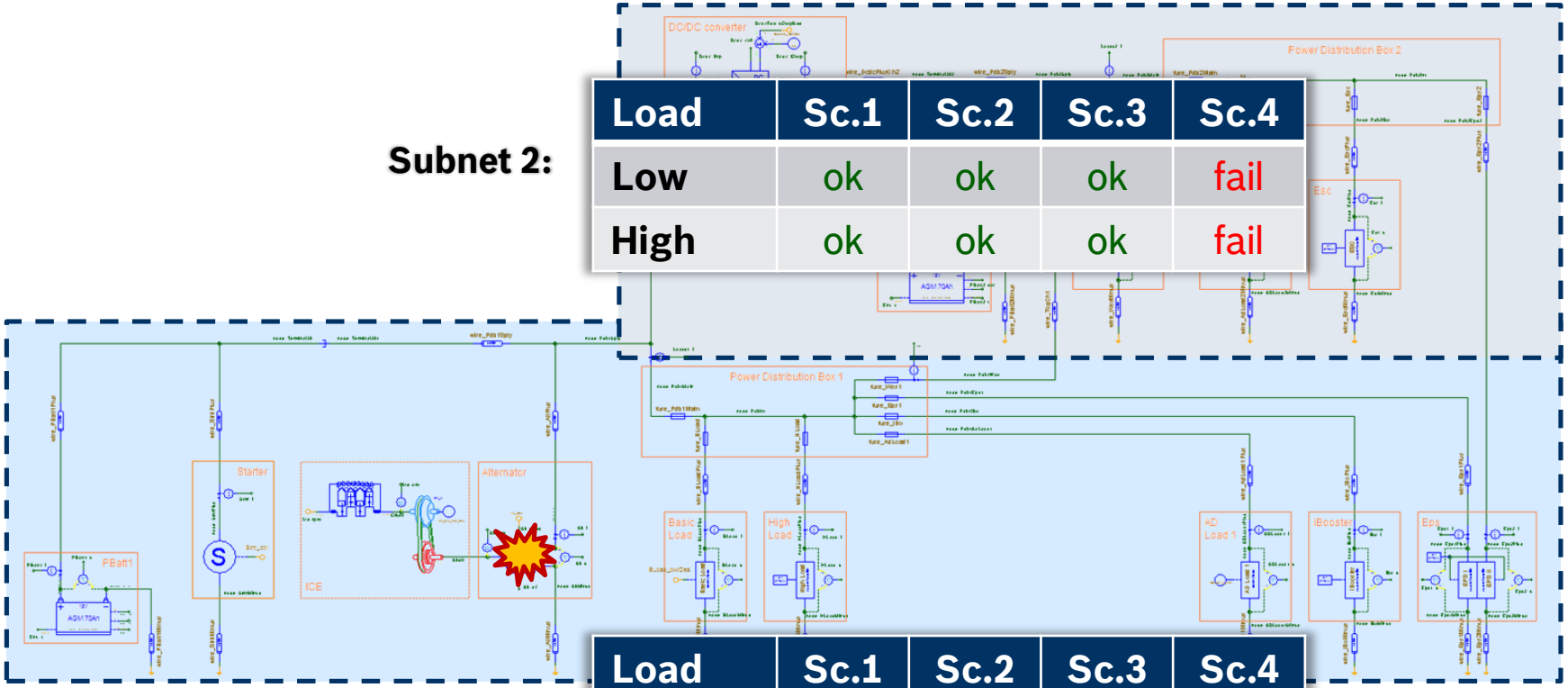
Simulations:

- Varying electric loads
- Different dynamic loads

Analysis & result:

- Voltage level falls below critical threshold
- Functional degrading of safety-relevant consumers → Scenario is not achievable if this fault happens

Scenario Variations



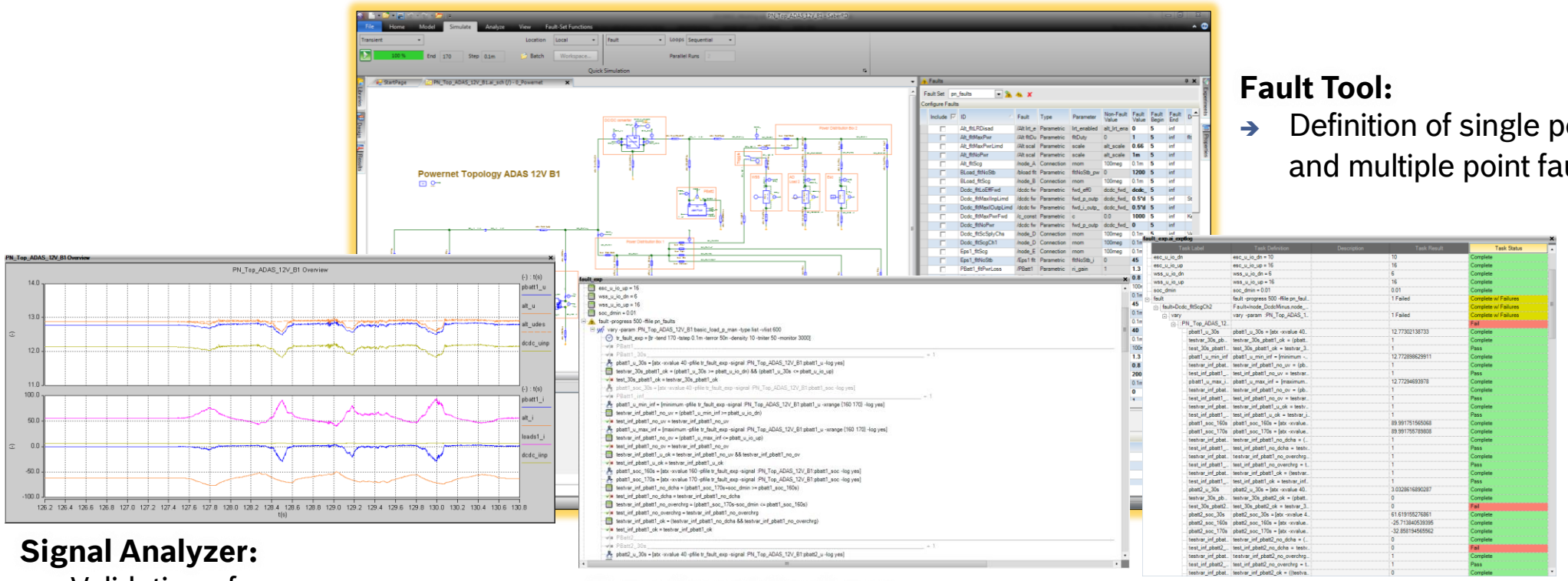
Subnet 2:

Load	Sc.1	Sc.2	Sc.3	Sc.4
Low	ok	ok	ok	fail
High	ok	ok	ok	fail

Subnet 1:

Load	Sc.1	Sc.2	Sc.3	Sc.4
Low	ok	ok	ok	fail
High	ok	ok	fail	fail

Using SaberRD



Fault Tool:

- Definition of single point faults and multiple point faults

Signal Analyzer:

- Validation of simulations

Experiment Analyzer:

- Variation of premises
- Variation of fault sets
- Automated analysis of the signal waveforms

Experiment Report:

- Review of the results
- Export to Excel

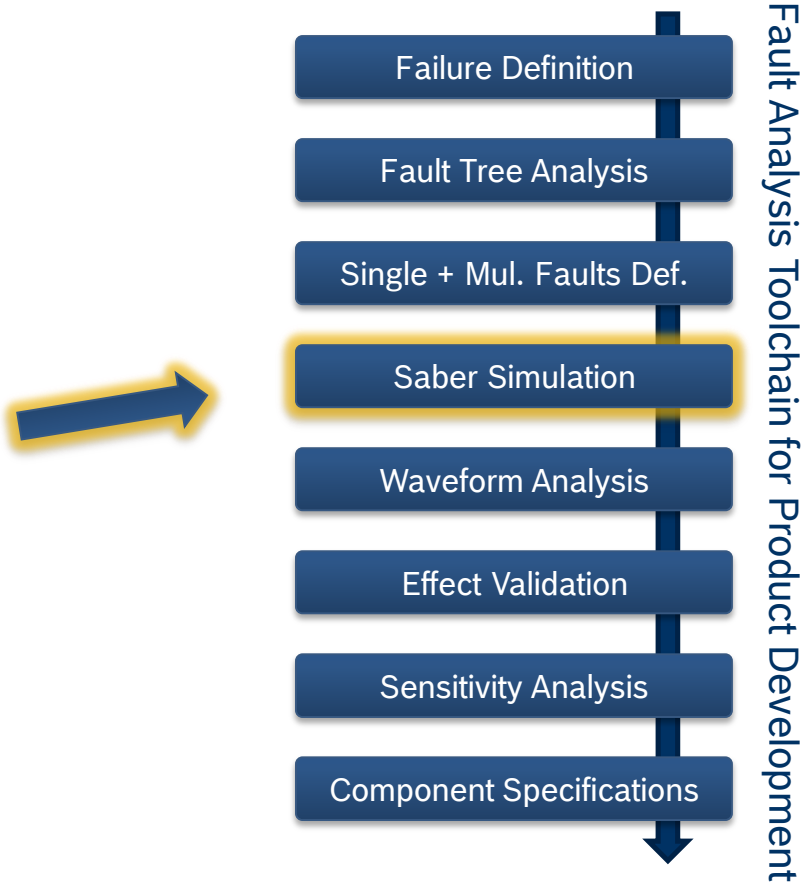
Complexity

- 3 load scenarios
- 2 ambient temperatures

- 10 power network components
  - 27 single point faults
  - 729 dual point faults

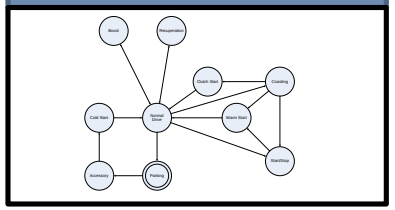
- 5000 simulations, approx. 7d calculation time

- 130 tests per simulation:
  - Extrema
  - Critical thresholds
  - Gradients

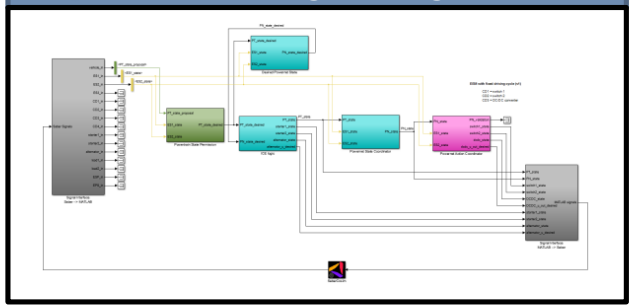


Architecture Design – Co-Simulation

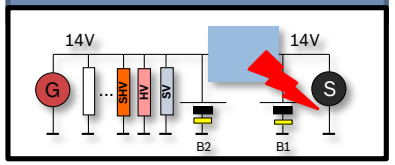
Operating strategy + components control



MATLAB
Electrical Energy Management

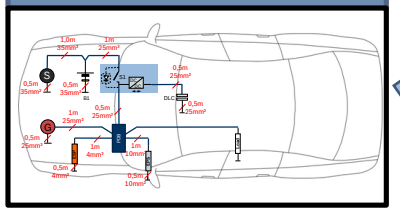


Fault injection

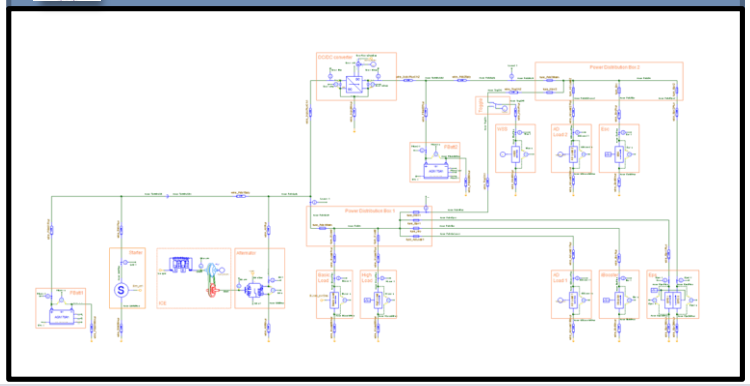


Co-Simulation

Wiring harness



SABER
Powernet Model



Nominal + Fault Analysis

- Voltage Stability
- Charge Balance

Conclusion

- Developing components for ADAS vehicles needs profound understanding of cause-effect relationships in power supply networks
- Classic method for analyzing fault effects are experiments on test vehicles, this would be
  - Expensive, time-consuming: Thousands of faults scenarios needs do be analyzed
  - Harmful: E.g. short cuts, component break-downs can cause dangerous effects
- Using simulations instead enables development regarding Functional Safety in an cost-efficient and flexible way
- Established toolchain with SaberRD:
  - Automatic execution of a very large number of fault simulations
  - Automatic analysis of signal waveforms
  - Exported report as input for succeeding process steps
- Effort: Robust simulation model must be developed for rated and failure operation mode
- Simulation allows:
  - Exploring many more failure scenarios that would have otherwise gone untested
  - Examining of current concepts and research on future concepts