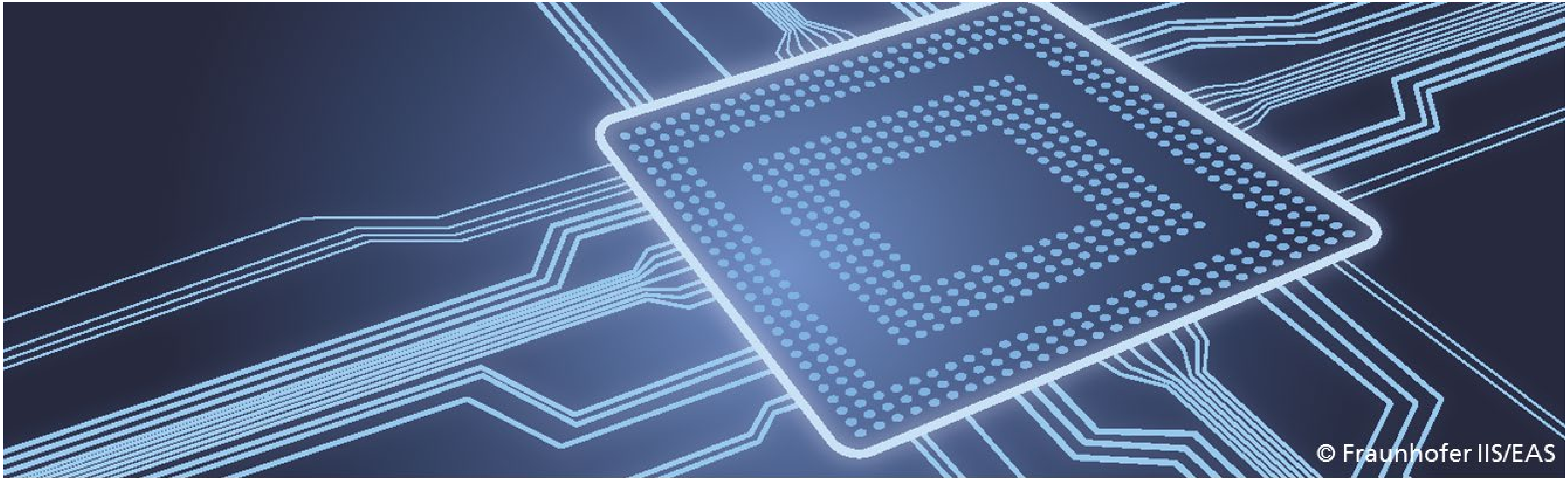
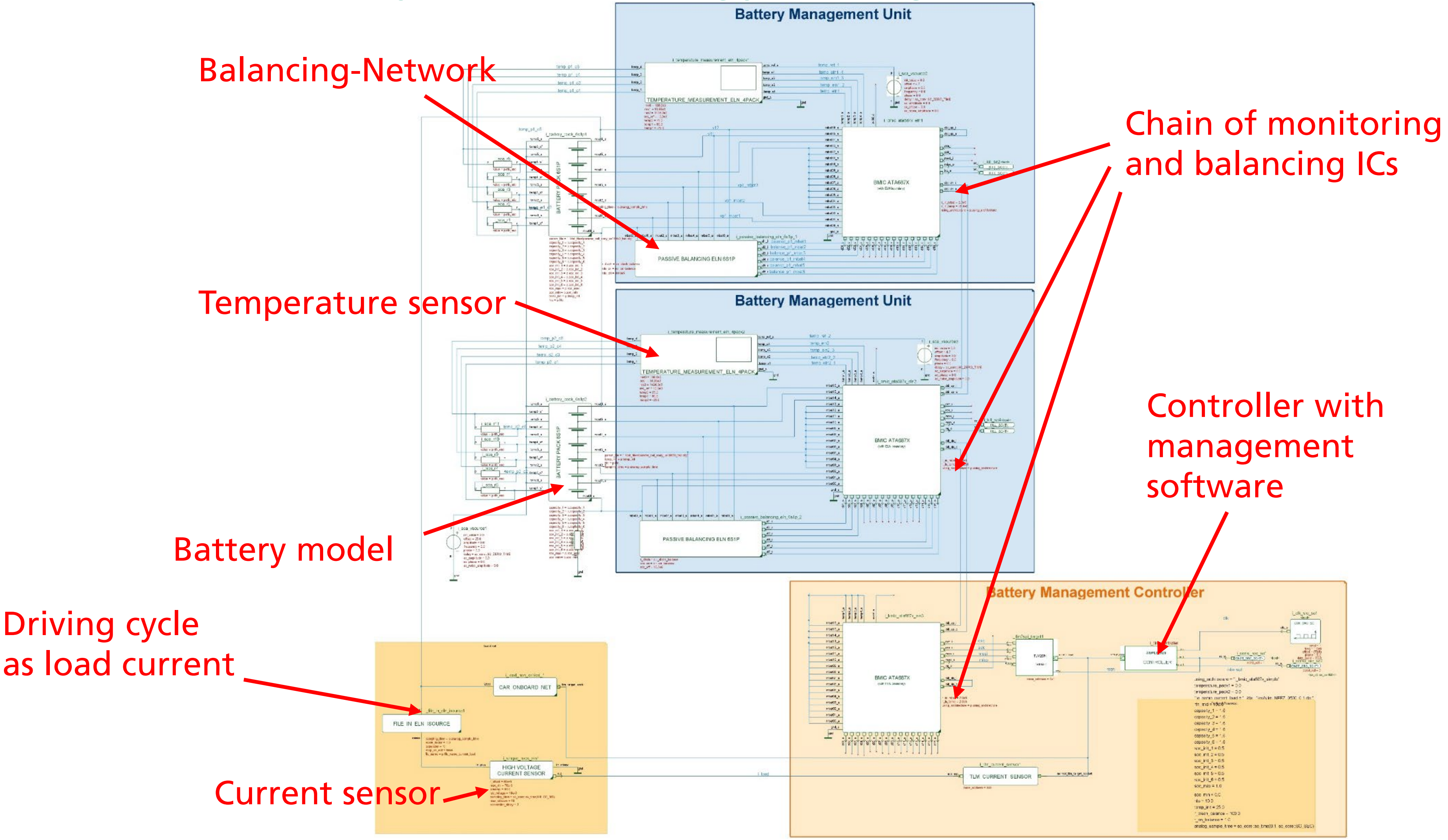
DYNAMIC FAULT INJECTION WITH SYSTEMC AMS FOR QUANTITATIVE SAFETY VERIFICATION

Fraunhofer Institute for Integrated Circuits IIS, Division Engineering of Adaptive Systems EAS
Department Design Methodology



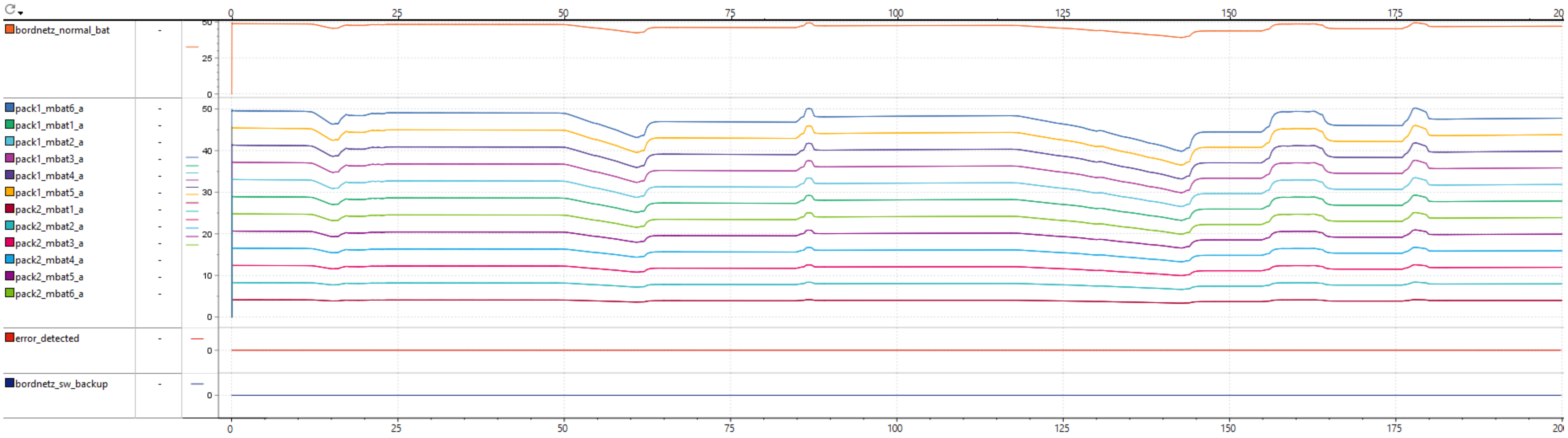
Fraunhofer
IIS

Battery management system (BMS)
As part of the safety critical energy storage item



Battery management system (BMS)
As part of the safety critical energy storage item

- Nominal simulation: based on driving cycle, provided by a project partner
  - No fault occurs
  - Battery cell voltages depend on SOC and load current



Fraunhofer IIS

Diagnostic Coverage Determination
FMEDA

- Investigations under Fusa aspects have to be done after functional verification

	Failure rate [FIT]	Safety Relevance Component	Failure Modes	Failure Mode Distribution D_{FMi} [%]	Failure Mode can Violate Safety Goal Directly	Failure Rate λ_i	Coverage by Safety Mechnism	Failure Mode Coverage K_{FMCi} [%]	Single Point Failure Rate $\lambda_{SPF,i}$ [FIT]	Residual Failure Rate $\lambda_{RF,i}$ [FIT]
Battery pack	10	x	Overvoltage	20	x	2	SM1	90	0	0,2
			Undervoltage	30	x	3	SM2	?	0	0
			Voltage changes too fast	10	x	1	SM3	99	0	0,01
			Temperature too low	20	x	2	SM4	95	0	0,1
			Temperature too high	20	x	2	SM4	95	0	0,1
Plug-Connector to main line	15	x	Open	30	x	4,5	SM5	99	0	0,045
			Short to ground	10	x	1,5	SM5	99	0	0,015
			Intermittend contact	60	x	9	SM5	99	0	0,09
Sum total [FIT]	123							Sum total [FIT]	2,2	6,085
Sum safety-relevant [FIT]	123							**SPFM [%]**	**93,3**	
Sum not-safety-relevant [FIT]	0									

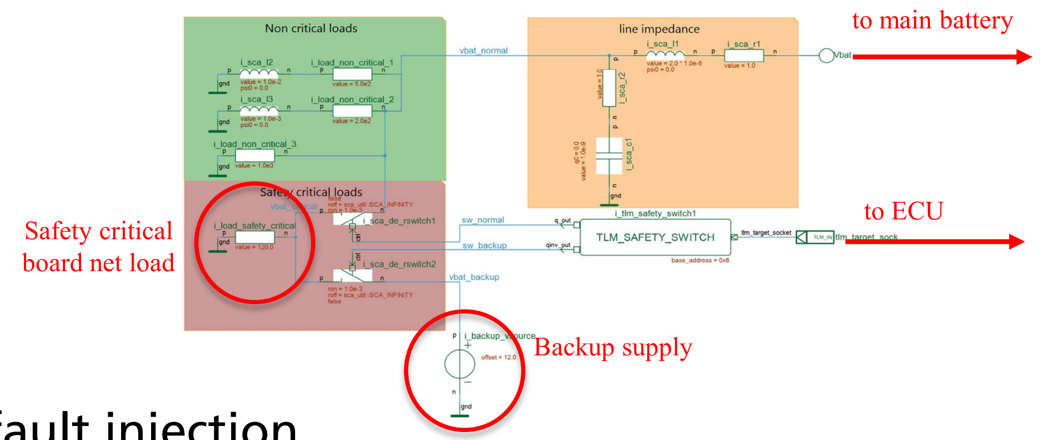
- Safety mechanism 2: Measure battery voltage and if a drop occurs connect redundant battery

Fraunhofer IIS

Battery management system (BMS)

Example board net with safety critical loads

- Goal:
  Assessment of safety concepts
  (e.g. supply of safety critical board net loads)
- Switch to backup voltage in case of under voltage



- Under-voltage condition provoked by dynamic fault injection
- ISO26262 compliance proved on time metrics

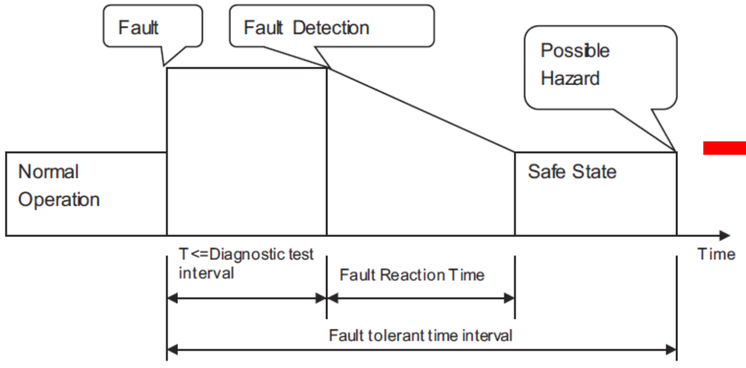
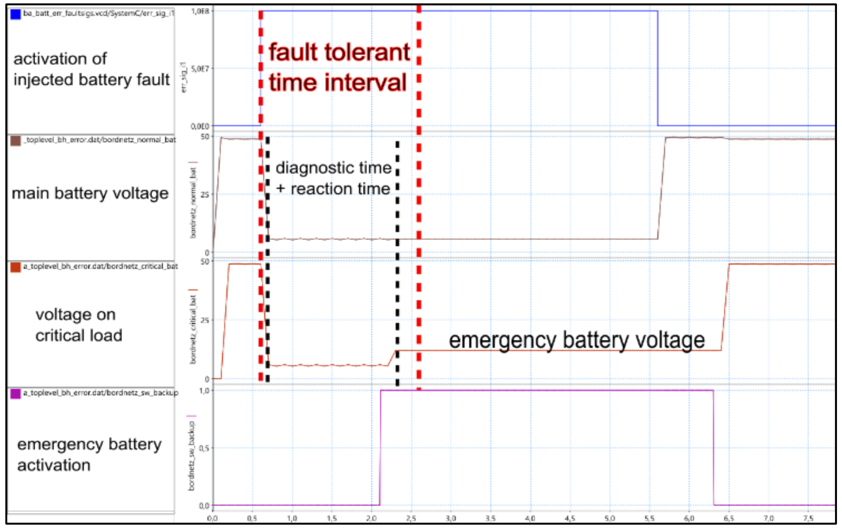
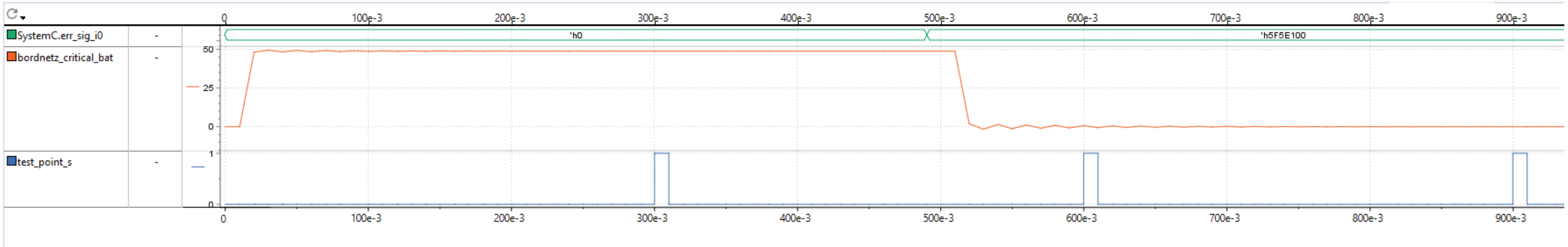


Figure 4 — Fault reaction time and fault tolerant time interval



Set up a fault injection scenario
Definition of the fault simulation scenario

- Scenario:

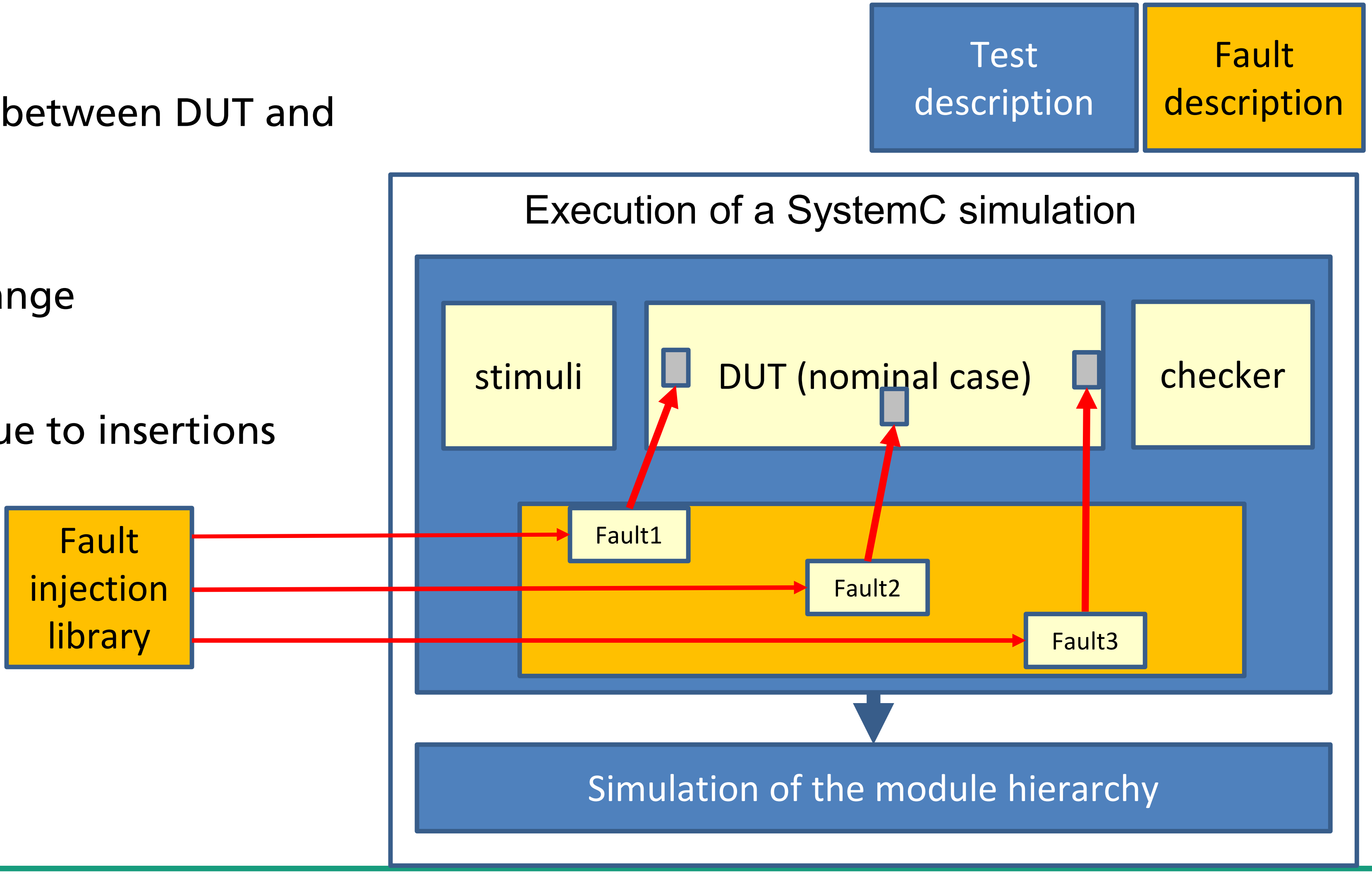


  - Suddenly, main battery cannot supply safety critical loads anymore
  - The provider defined a fault tolerant time interval
  - It has to be proven that safety mechanism is able to bring system in stability again fast enough
  - E.g. Check influence of fault occurrence time to this requirement

Fraunhofer IIS

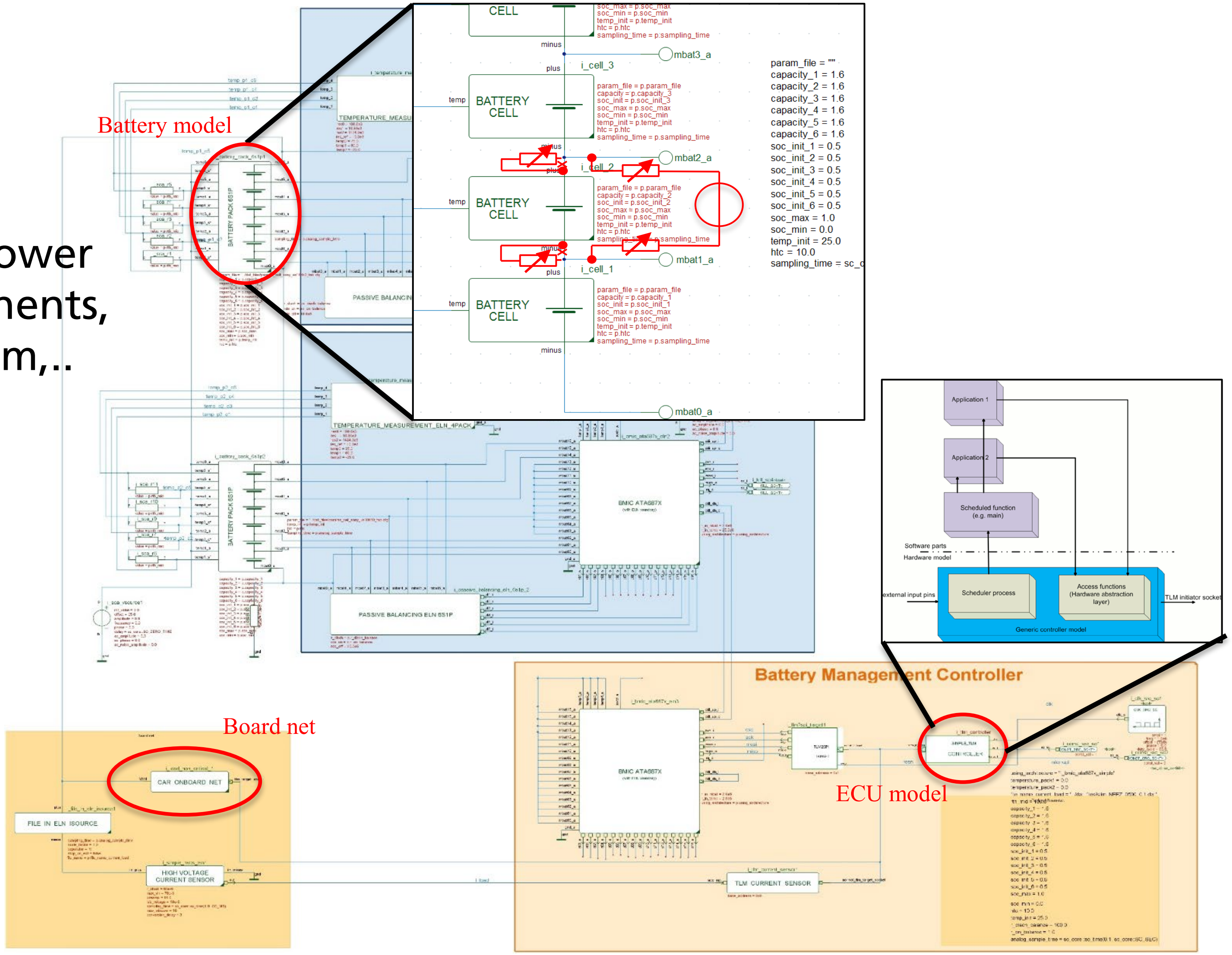
Fault injection approach for SystemC/ SystemC AMS
Principle of the dynamical fault injection

- Clear separation between DUT and test description
- No DUT code change
- Avoiding bugs due to insertions of test artifacts



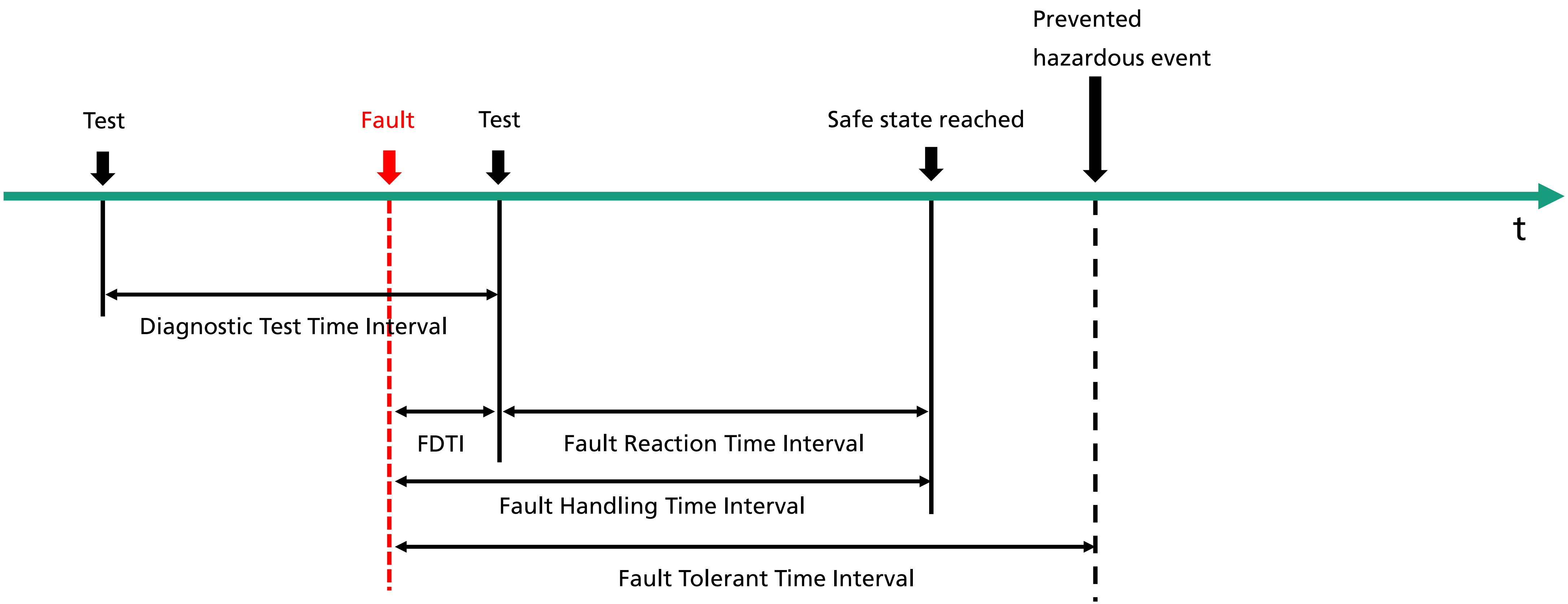
Battery management system (BMS)
Battery fault injection

- Board net as part of a safety-critical system
- Safety concept requires stabil power supply for safety critical components, e.g. ABS, Airbag, breaking system,..
- Safety mechanism is part of the software application

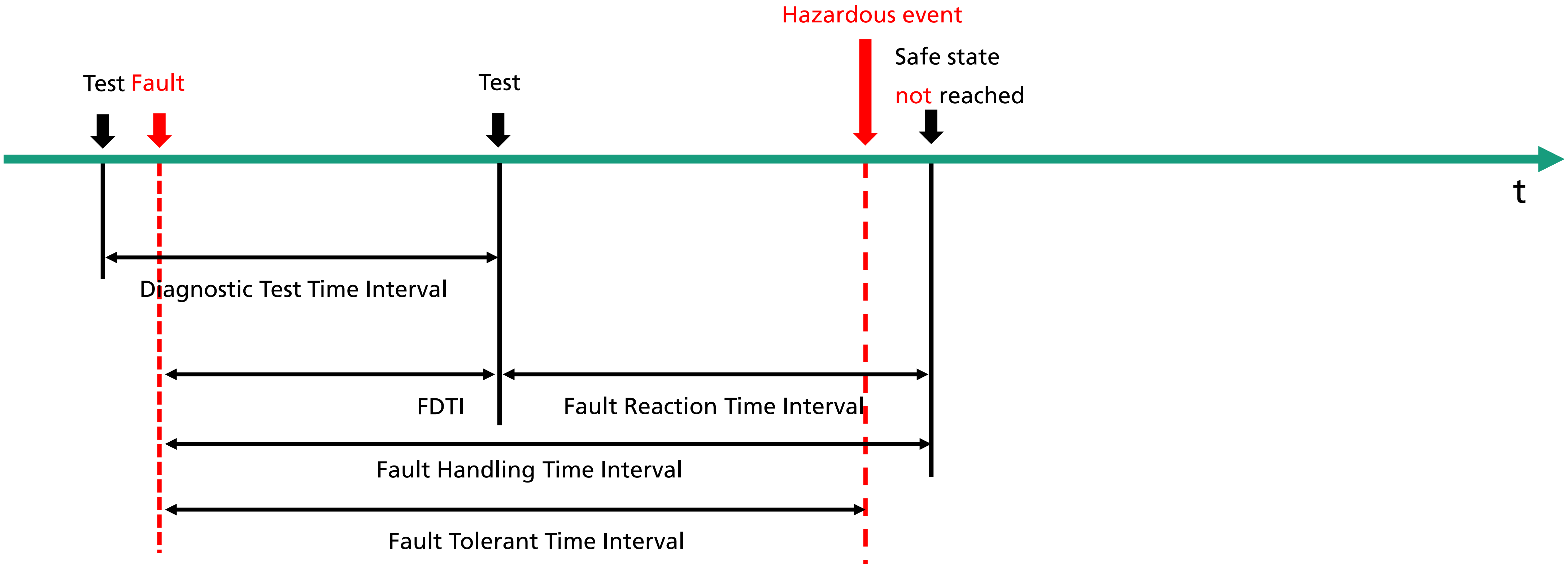


Fraunhofer IIS

Diagnostic Coverage Determination
Timing limitations for DC



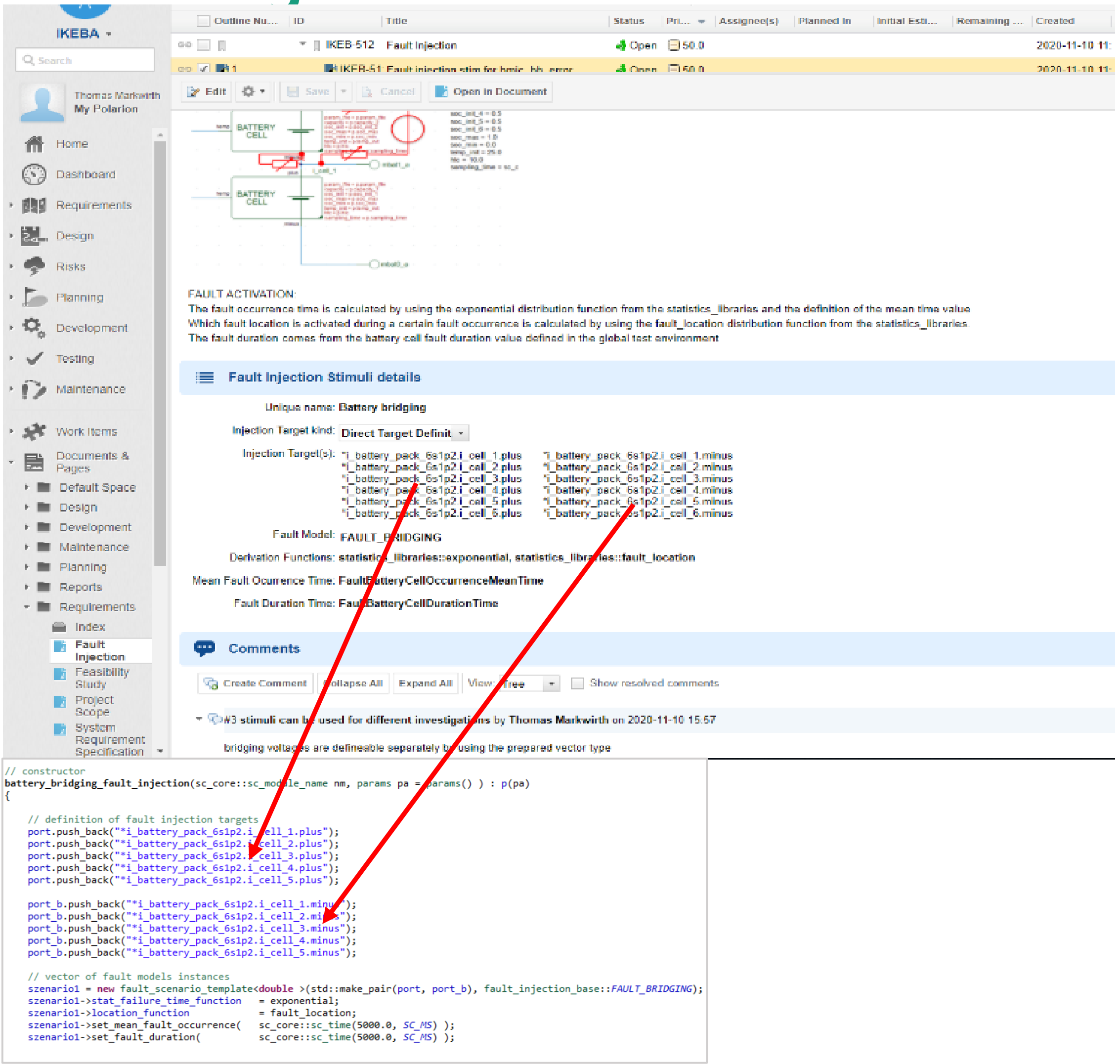
Diagnostic Coverage Determination
Timing limitations for DC



Battery management system (BMS)

Fault description embedded into structured generation flow

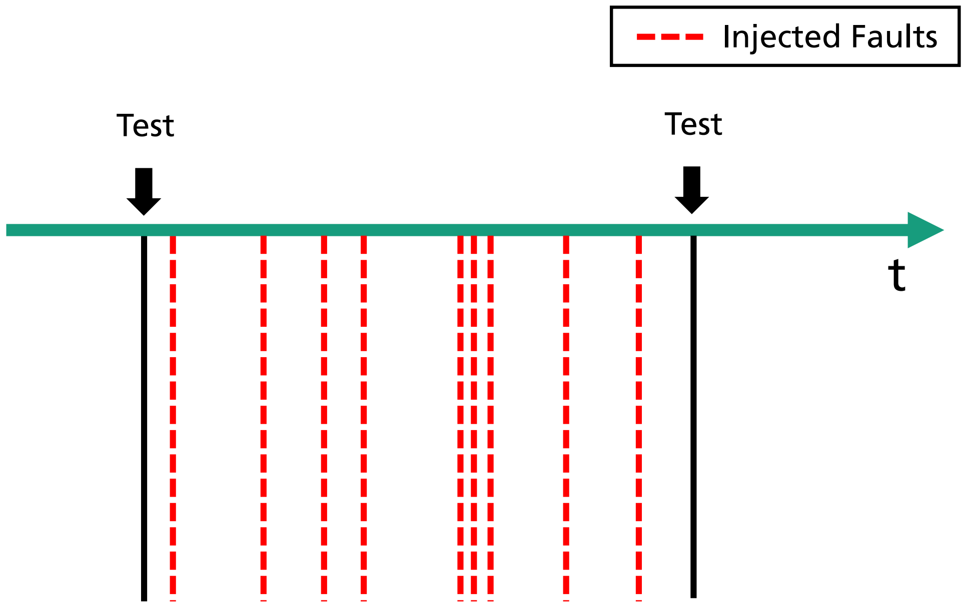
- Automated injection flow
  - Safety concept specified in requirement management tool
  - Requirement for fault simulation defined
  - Automated source code and testcase generation
  - Regression



Fraunhofer IIS

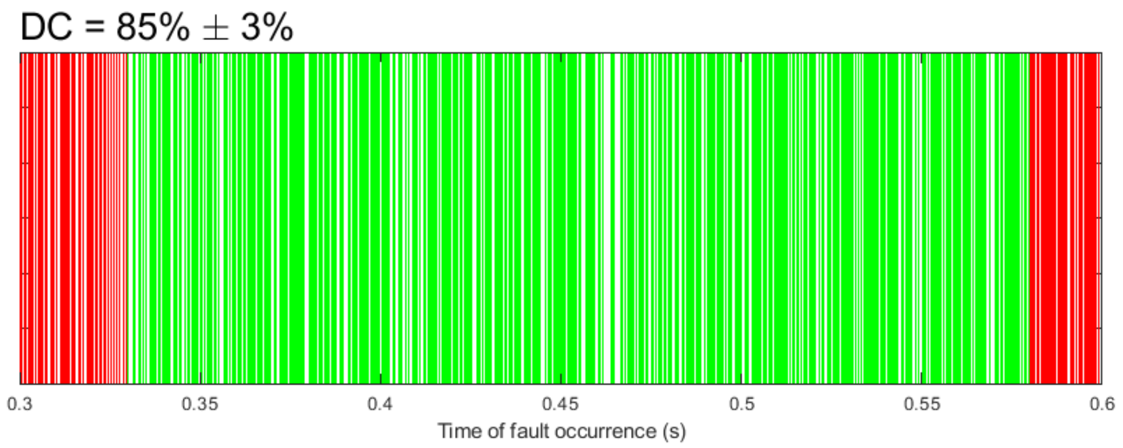
Diagnostic Coverage Determination
Monte-Carlo Simulations

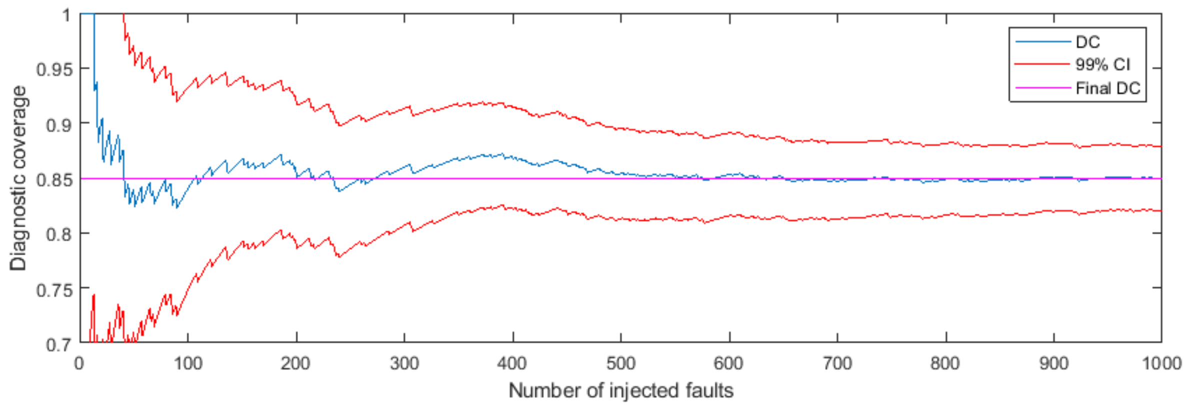
- Define parameter space(s) – e.g. DTTI
- Inject fault at random points
- Estimate DC from ratio of faults with prevented hazardous event to all injected faults
- Advantages:
  - Best efficiency for many parameter spaces
  - Can map whole parameter space
- Disadvantages:
  - Normally not sensible for one parameter space and required accuracy
  - Complicated to set up compared to other approaches



Example: 9 randomly injected faults – low accuracy

Diagnostic Coverage Determination
Monte-Carlo Simulations - Results





Fraunhofer IIS

Diagnostic Coverage Determination

FMEDA

	Failure rate [FIT]	Safety Relevance Component	Failure Modes	Failure Mode Distribution D_{FMi} [%]	Failure Mode can Violate Safety Goal Directly	Failure Rate λ_i	Coverage by Safety Mechnism	Failure Mode Coverage K_{FMCi} [%]	Single Point Failure Rate $\lambda_{SPF,i}$ [FIT]	Residual Failure Rate $\lambda_{RF,i}$ [FIT]
Battery pack	10	x	Overvoltage	20	x	2	SM1	90	0	0,2
			Undervoltage	30	x	3	SM2	85	0	0,45
			Voltage changes too fast	10	x	1	SM3	99	0	0,01
			Temperature too low	20	x	2	SM4	95	0	0,1
			Temperature too high	20	x	2	SM4	95	0	0,1
Plug-Connector to main line	15	x	Open	30	x	4,5	SM5	99	0	0,045
			Short to ground	10	x	1,5	SM5	99	0	0,015
			Intermittend contact	60	x	9	SM5	99	0	0,09
Sum total [FIT]	123							Sum total [FIT]	2,2	6,535
Sum safety-relevant [FIT]	123							SPFM [%]	92,9	
Sum not-safety-relevant [FIT]	0									

- Safety mechanism 2: Measure battery voltage and if a drop occurs connect redundant battery

Fraunhofer IIS

Diagnostic Coverage Determination
Sum up

- SystemC/ SystemC AMS is usable for a quantitative safety verification
- Could be demonstrated, that dynamic fault injection approach is very efficient for this task
- But…
  - No standardized interchange formats, e.g. for fault descriptions, metrics, … ,simulation results as e.g. FMEDA input
  - Mainly “own” libraries for fault injection, statistics, interfaces… used

THANK YOU FOR YOUR ATTENTION
YOUR CONTACT PARTNER

Thomas Markwirth

Group Virtual System Development

✉ thomas.markwirth@eas.iis.fraunhofer.de
☏ +49 351 45691 - 232

Christoph Sohrmann

Head of Group Virtual System Development

✉ christoph.sohrmann@eas.iis.fraunhofer.de
☏ +49 351 45691 - 230

Fraunhofer Institute for Integrated Circuits IIS
Division Engineering of Adaptive Systems EAS
Münchner Straße 16
01187 Dresden, Germany

www.eas.iis.fraunhofer.de/en

Fraunhofer
IIS

Copyright Permission

- A non-exclusive, irrevocable, royalty-free copyright permission is granted by **Fraunhofer IIS/EAS** to use this material in developing all future revisions and editions of the resulting draft and approved Accellera Systems Initiative **SystemC** standard, and in derivative works based on the standard.