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

- Balancing-Network
- Temperature sensor
- Battery model
- Driving cycle as load current
- Current sensor
- Chain of monitoring and balancing ICs
- Controller with management software
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
### Diagnostic Coverage Determination

**FMEDA**

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

<table>
<thead>
<tr>
<th>Failure rate [FIT]</th>
<th>Safety Relevance Component</th>
<th>Failure Modes</th>
<th>Failure Mode Distribution $D_{PMI}$ [%]</th>
<th>Failure Mode can Violate Safety Goal Directly</th>
<th>Failure Rate $\lambda_i$</th>
<th>Coverage by Safety Mechanism $K_{SMC[i]}$ [%]</th>
<th>Single Point Failure Rate $\lambda_{SPFMI}$ [FIT]</th>
<th>Residual Failure Rate $\lambda_{RDFMI}$ [FIT]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery pack</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>Undervoltage</td>
<td>20</td>
<td>x</td>
<td>2</td>
<td>SM1</td>
<td>0</td>
<td>0.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overvoltage</td>
<td>30</td>
<td>x</td>
<td>3</td>
<td>SM2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voltage changes too fast</td>
<td>10</td>
<td>x</td>
<td>1</td>
<td>SM3</td>
<td>99</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Temperature too low</td>
<td>20</td>
<td>x</td>
<td>2</td>
<td>SM4</td>
<td>95</td>
<td>0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Temperature too high</td>
<td>20</td>
<td>x</td>
<td>2</td>
<td>SM4</td>
<td>95</td>
<td>0.1</td>
</tr>
<tr>
<td>Plug-Connector to main line</td>
<td>15</td>
<td>Open</td>
<td>30</td>
<td>x</td>
<td>4.5</td>
<td>SM5</td>
<td>99</td>
<td>0.045</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Short to ground</td>
<td>10</td>
<td>x</td>
<td>1.5</td>
<td>SM5</td>
<td>99</td>
<td>0.015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intermittent contact</td>
<td>60</td>
<td>x</td>
<td>9</td>
<td>SM5</td>
<td>99</td>
<td>0.09</td>
</tr>
<tr>
<td>Sum total [FIT]</td>
<td>123</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sum total [FIT]</td>
<td>2.2</td>
</tr>
<tr>
<td>Sum not-safety-relevant [FIT]</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sum not-safety-relevant [FIT]</td>
<td></td>
</tr>
</tbody>
</table>

- **Safety mechanism 2**: Measure battery voltage and if a drop occurs connect redundant battery
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**
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
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
Diagnostic Coverage Determination

Timing limitations for DC

- Test
- Fault
- Test
- Safe state reached
- Prevented hazardous event

Diagnostic Test Time Interval
Fault Reaction Time Interval
Fault Handling Time Interval
Fault Tolerant Time Interval

FDTI
Diagnostic Coverage Determination

Timing limitations for DC

- Test Fault
- Test
- Hazardous event
- Safe state not reached

- Diagnostic Test Time Interval
- FDTI
- Fault Reaction Time Interval
- Fault Handling Time Interval
- Fault Tolerant Time Interval
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
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

DC = 85% ± 3%
Diagnostic Coverage Determination

**FMEDA**

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure Rate [FIT]</th>
<th>Safety Relevance</th>
<th>Failure Mode</th>
<th>Failure Mode Distribution $D_{IK}$ [%]</th>
<th>Failure Mode can Violate Safety Goal Directly</th>
<th>Failure Rate $\lambda_i$</th>
<th>Coverage by Safety Mechanism $K_{MGS}$ [%]</th>
<th>Single Point Failure Rate $\lambda_{MPS}$ [FIT]</th>
<th>Residual Failure Rate $\lambda_{Res}$ [FIT]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery pack</td>
<td>10</td>
<td>x</td>
<td>Overvoltage</td>
<td>20</td>
<td>x</td>
<td>2</td>
<td>SM1</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Undervoltage</td>
<td>30</td>
<td>x</td>
<td>3</td>
<td>SM2</td>
<td>0.85</td>
<td>0.45</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Voltage change too fast</td>
<td>10</td>
<td>x</td>
<td>1</td>
<td>SM3</td>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Temperature too low</td>
<td>20</td>
<td>x</td>
<td>2</td>
<td>SM4</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Temperature too high</td>
<td>20</td>
<td>x</td>
<td>2</td>
<td>SM5</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>Plug-Connector to main line</td>
<td>15</td>
<td>x</td>
<td>Open</td>
<td>30</td>
<td>x</td>
<td>4.5</td>
<td>SM5</td>
<td>0.045</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Short to ground</td>
<td>10</td>
<td>x</td>
<td>1.5</td>
<td>SM5</td>
<td>0.015</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Intermittent contact</td>
<td>60</td>
<td>x</td>
<td>9</td>
<td>SM5</td>
<td>0.09</td>
<td></td>
</tr>
</tbody>
</table>

Sum total [FIT]: 123
Sum safety-relevant [FIT]: 123
Sum not-safety-relevant [FIT]: 0

Sum total [FIT]: 123
SPPM [%]: 92.9
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

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

www.eas.iis.fraunhofer.de/en

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
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.