metaFMEA – A Framework for Reusable FMEAs
There is a gap between model-based development and dependability analysis

Current dependability analysis models cannot follow the increasing trend for model-based development.

<table>
<thead>
<tr>
<th>Model-based development is an increasing trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Systematic reuse of models or model elements</td>
</tr>
<tr>
<td>• Domain-specific model elements and languages</td>
</tr>
<tr>
<td>• Ability to include variation points</td>
</tr>
<tr>
<td>• Divide-and-Conquer strategy</td>
</tr>
<tr>
<td>• Shorter time-to-market</td>
</tr>
</tbody>
</table>

How do state-of-the-art dependability analysis methodologies relate to model-based development?

<table>
<thead>
<tr>
<th>Top down</th>
<th>Bottom up</th>
<th>Documentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Classic Fault Trees and Markov chains are widely used and compact, but are not integrated in the system model.</td>
<td>• FMEA is also well known, but becomes more and more unmanageable if the system complexity increases. Especially consistency is an issue if the system scales.</td>
<td>• Documentary diagrams for dependability arguments exist, but they need to show their efficiency in projects.</td>
</tr>
<tr>
<td>• Component Fault Trees are integrated in the system model, but automations and strategies are white spots.</td>
<td>• Excel is flexible.</td>
<td>• Generating documentation out of such diagrams is also white spot.</td>
</tr>
</tbody>
</table>

Unrestricted © Siemens AG 2014. All rights reserved
Central Business Use Cases are the Main Innovation Drivers for Methodologies and Tools

Establishing technology-driven innovations, business use cases are drivers to maintain a pull strategy.

### Central Use Cases

**Reuse**
- Repository with items.
- Compositional development strategy reusing existing items from the repository.
- Automated construction of the system, e.g. by code generation or circuit diagrams.
- Y integration approach for verification and validation.
- Automated certification.

**Impact**
- Change request.
- Changes are only applied to the affected components.
- Automated recertification.

### Methodologies and Tools

**Top down & documentary**
- Screening
- Scoping
- Business Case
- Development
- Test & Validation
- Rollout

**Bottom-up**
- Screening
- Scoping
- Business Case
- Development
- Test & Validation
- Rollout

Unrestricted © Siemens AG 2014. All rights reserved
A FMEDA analysis separates failure rates of electronic parts into classes to find out which are relevant.

**FMEA**  – Failure Mode and Effects Analysis

**FMEDA**  – Failure Mode, Effects and Diagnosis Analysis

- Quantified with failure rates.
- Mean Time Between Failures (MTBF)
- Additionally evaluates the safe failure fraction (SFF) according to IEC61508.

Failure rate of an element or a component in FIT (Failure In Time = 1 failure in $10^9$ operating hours or 114,000 years)

- Safe failures that do not result in a dangerous state
- Dangerous failures that do result in a dangerous state
- Dangerous failures that are Detected
- Dangerous failures that are Undetected

"Dangerous"
A manual list is hard to maintain and consistency is an issue

<table>
<thead>
<tr>
<th>Circuit ID</th>
<th>C101</th>
<th>R305</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Capacitor</td>
<td>Resistor</td>
</tr>
<tr>
<td>Part</td>
<td>100nF/120V</td>
<td>10kOhm</td>
</tr>
<tr>
<td>Function</td>
<td>smooth output</td>
<td>regulates amplification factor</td>
</tr>
<tr>
<td>Failure Mode</td>
<td>short circuit</td>
<td>open circuit</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Effect</td>
<td>amplification factor exceeds limitations</td>
<td>no effect</td>
</tr>
<tr>
<td>Classification Diagnosis</td>
<td>Dangerous pulsed test</td>
<td>Safe</td>
</tr>
<tr>
<td>Coverage</td>
<td>90</td>
<td>n/a</td>
</tr>
<tr>
<td>$\lambda_{du}$</td>
<td>1</td>
<td>n/a</td>
</tr>
<tr>
<td>$\lambda_{dd}$</td>
<td>9</td>
<td>n/a</td>
</tr>
</tbody>
</table>

1. **Consistency of failure effects.**
   Failures resulting in the same effect should be identifiable for analysis.

2. **Consistency of failure modes.**
   Each reused component should be analyzed for the same failure modes.

3. **Global effect analyses.**
   Global effects should be considered.

4. **Consistency of measures.**
   To enable a global effect analysis, identical measures should be identifiable.
Development Goal: Overcome Drawbacks of the Excel Template

Using a tool supported model-based approach overcomes the drawbacks of an excel-based analysis.

Benefits over Excel Templates

- To add a new evaluation method to an Excel sheet is a time intensive task and to add automations to existing analyses (reuse) is error prone.
- The visualization in Excel is constrained to one view. With .xml, multiple views can coexist at the same time.
- Adding a new failure mode can result in complex inconsistencies in an Excel-based FMEDA, e.g. if the analysis is comparatively large and has to be reviewed entirely.
- Reoccurring effects or diagnostic measures can result in a complex network of links in your Excel-based FMEDA. Using Database structures eases the process.
- Due to the database structure, fault trees can be generated out of FMEDA analyses.

Resulting Meta-Model for FMEDA

Unrestricted © Siemens AG 2014. All rights reserved
FMEDAexpress handles Local and Generic Effects

FMEDAexpress provides basic functionality for local and generic effects and is flexible and extendable.

**Characteristics**

- Handles .xml input and output.
- .xlst file allows customized view.
- SQL Database makes it easy to extend, e.g. to store additional information or to adapt different analyses.
- .NET 4 Framework application written in C Sharp
- Currently provides full FMEDA analyses with quantifications according to IEC61508.
- Handles local and generic effects.
- Implements a component-based approach for hardware components.
- Implements routines that solve specific problems during FMEDA.
FMEDAexpress provides vast improvements over Excel-based approaches

In a case study, we could measure a reduction over 90% of effort for some important use cases.

<table>
<thead>
<tr>
<th>Use case during the case study</th>
<th>Percent of the model affected</th>
<th>Number of manual actions in Excel</th>
<th>Number of manual actions in FMEDAexpress</th>
<th>Reduction of effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the failure model for comparators and amplifiers</td>
<td>12.00%</td>
<td>522</td>
<td>24</td>
<td>95%</td>
</tr>
<tr>
<td>Change the effectiveness of a diagnostic measure</td>
<td>5.50%</td>
<td>214</td>
<td>1</td>
<td>99%</td>
</tr>
<tr>
<td>Change the failure classification from &quot;VCC to ground&quot; from safe to dangerous</td>
<td>0.25%</td>
<td>11</td>
<td>1</td>
<td>90%</td>
</tr>
</tbody>
</table>

- These use cases are related to tasks from a compositional analysis. Composing a new analysis from existing data in a manual tool seems infeasible without a database solution.

- Having about 4'000 failure modes in this case study, a dedicated tool like FMEDAexpress pays off easily if new analyses are composed from existing data.
For further information, please do not hesitate to contact me directly via the following coordinates.

Dr.-Ing. Kai Höfig  
Model-based Reliability & Safety Engineering  
Corporate Technology  
Research & Technology Center  
CT RTC SYE DAM-DE

Otto-Hahn-Ring 6  
81739 München, Deutschland

E-mail:  
kai.hoefig@siemens.com  
siemens.com/innovation