SIEMENS

Kai Höfig & Marc Zeller, Siemens Corporate Technology, Lars Grunske, University of Stuttgart

metaFMEA – A Framework for Reusable FMEAs

There is a gap between model-based development and dependability analysis

SIEMENS

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

Model-based development is an increasing trend

- Systematic reuse of models or model elements
- Domain-specific model elements and languages
- Ability to include variation points
- Divide-and-Conquer strategy
- Shorter time-to-market

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

Top down

- Classic Fault Trees and Markov chains are widely used and compact, but are not integrated in the system model.
- Component Fault Trees are integrated in the system model, but automations and strategies are white spots.

Bottom up

- 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.
- Excel is flexible.

Documentary

- Documentary diagrams for dependability arguments exist, but they need to show their efficiency in projects.
- Generating documentation out of such diagrams is also white spot.

Central Business Use Cases are the Main Innovation Drivers for Methodologies and Tools

SIEMENS

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

Central Use Cases

Reuse

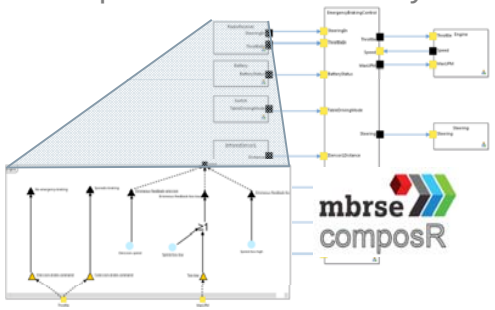
- Repository with items.
- Compositional development strategy reusing existing items from the repository.
- Automated construction of the system, e.g. by code generation or circuit diagrams.
- Y integration approach for verification and validation.
- Automated certification.

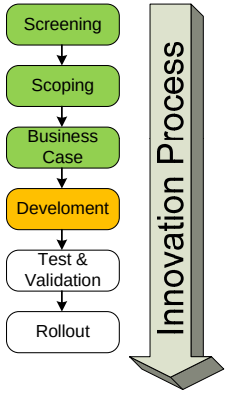
Impact

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

Methodologies and Tools

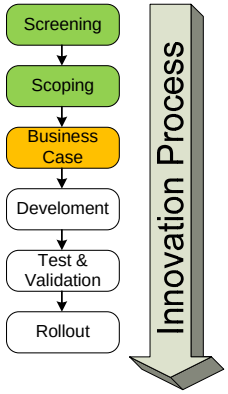
Top down & documentary





Bottom-up

Multi purpose



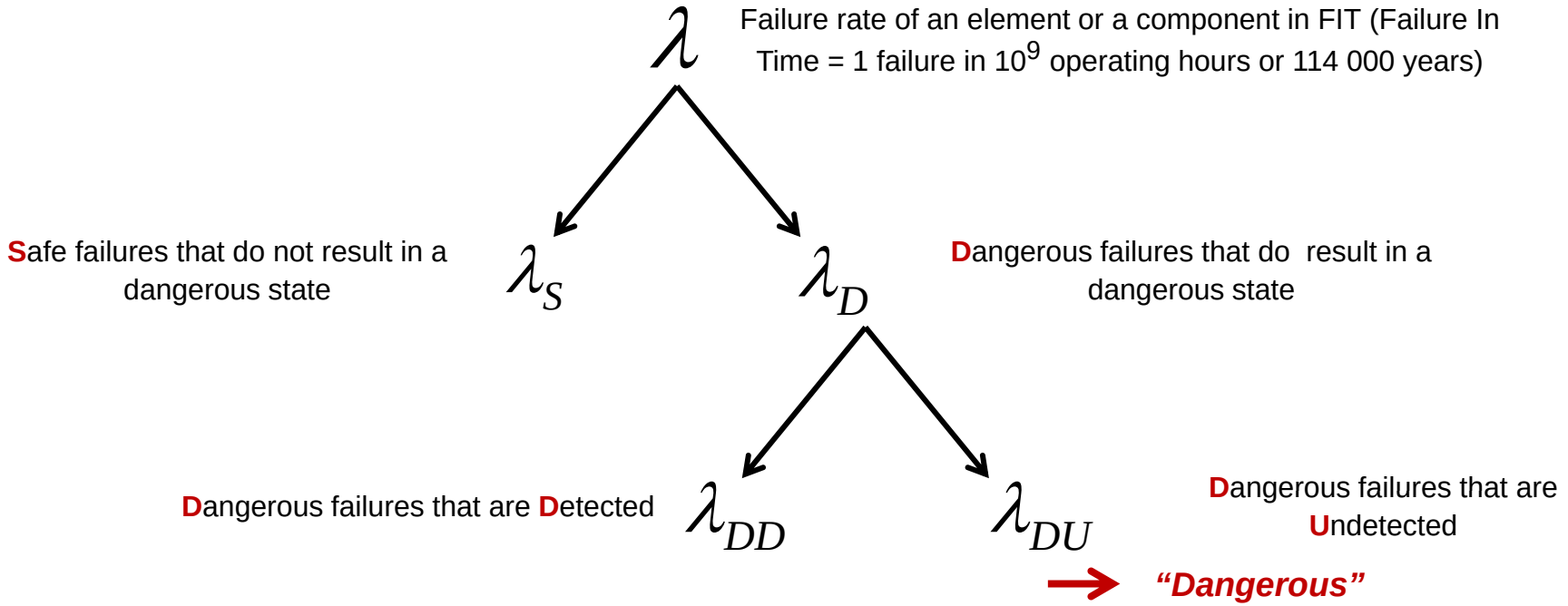
FMEDA Basic Principles

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.



FMEDA in Excel and Problems faced

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

Circuit ID	C101		R305	
Type	Capacitor		Resistor	
Part	100nF/120V		10kOhm	
Function	smooth output		regulates amplification factor	
Failure Mode	short circuit	open circuit	short circuit	open circuit
λ	10	10	20	20
Effect	amplification factor exceeds limitations	no effect	no effect	amplification factor exceeds limitations
Classification	Dangerous	Safe	Safe	Dangerous
Diagnosis	pulsed test	n/a	n/a	pulsed test
Coverage	90	n/a	n/a	90
λ_{du}	1	n/a	n/a	2
λ_{dd}	9	n/a	n/a	18

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

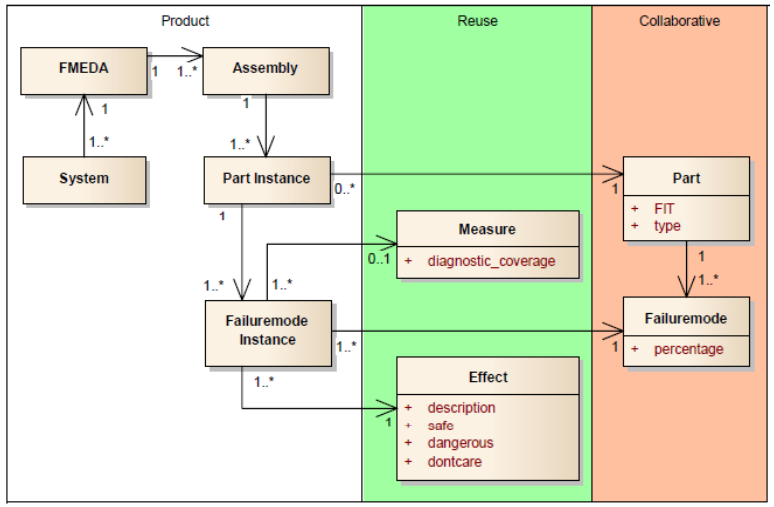
SIEMENS

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

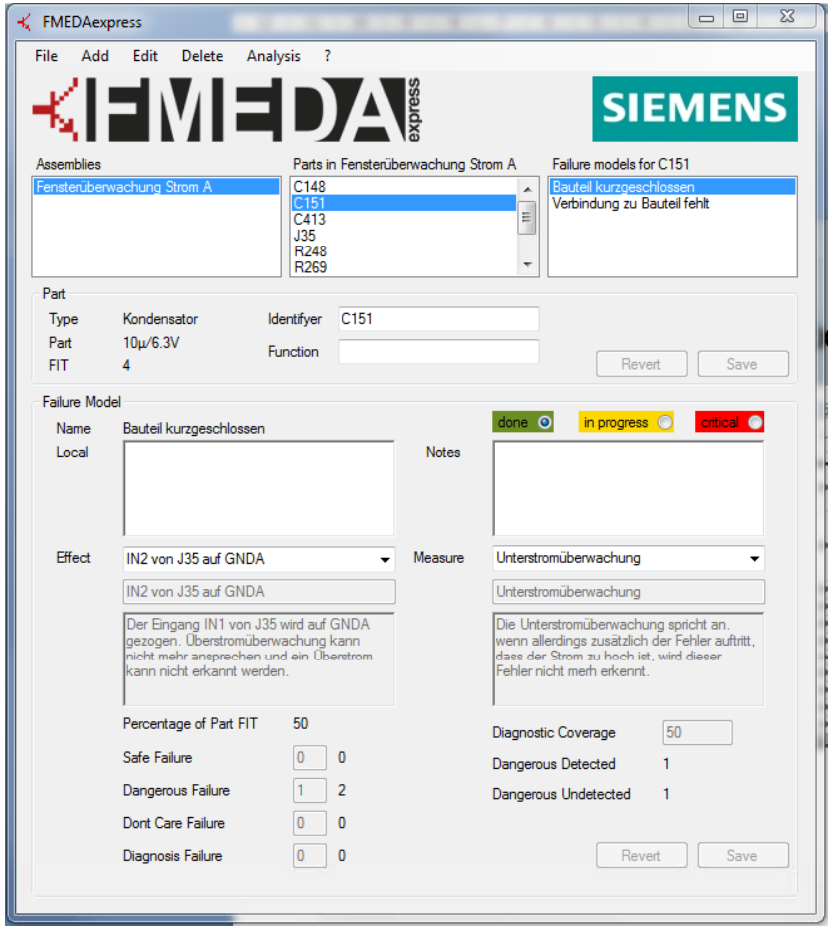


FMEDAexpress handles Local and Generic Effects

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

SIEMENS

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

Usecase during the case study	Percent of the model affected	Number of manual actions in Excel	Number of manual actions in FMEDAexpress	Reduction of effort
Change the failure model for comparators and amplifiers	12,00%	522	24	95%
Change the effectiveness of a diagnostic measure	5,50%	214	1	99%
Change the failure classification from "VCC to ground" from safe to dangerous	0,25%	11	1	90%

- 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.

Contact

✓ 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