Functional Safety Management with EA

Dr. Konrad Wieland, LieberLieber
Markus Schwarz, Vector

Stuttgart, 21.2.2017
My Background

• OOM & Model Engineering, TU Vienna
• 2011 PhD: Model Versioning, TU Vienna
• Sparx Trainer & Consultant
• LieberLieber Product Manager
Agenda

• „Safety needs models“
• Challenges for EA
  • Notation and Profiles
  • Tracability
  • Configuration & Change Management
• And how they are solved at Vector Informatik GmbH
Managing Complexity

We will target Companies manufacturing safety relevant Cyber Physical Systems
ISO 26262 Adaptation of IEC 61508

IEC 61508
Functional Safety for E/E/PES Safety Related Systems

IEC 61511
Process Industry

IEC 62061
Machinery

IEC 61513
Nuclear

ISO 26262
Road Vehicles

ISO 13849-1
Machine Safety

ISO 25119
Tractors...

ISO 26262 is “State of the Art” For Automotive
Developed with OEM
Complexity on the one Hand and Safety on the other

Growing Complexity of Environment and Solutions

Complex Processes, Distributed Teams

Safety in General and Safety Standards in Particular

• IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
• ISO 26262 - Road Vehicles Functional Safety
• IEC 62304 - Medical Device Software
• EUROCAE ED-12B European Airborne Flight Safety Systems
• IEC 61513 - Nuclear power plants
• IEC 62061 - Safety of machinery
• EN 50128, 50129 - Railway Industry
ISO 26262 Parts relevant for Modeling

Other Standards are similar

3 Concept phase

- Handles Hazard Analysis and Risk Assessment has impact on development process
- Tracking and Traceability of ASI-Level from requirements to tests is necessary

4 Product development at system level

4, 5, 6

- Nested V-Model process highly recommended
- Comprehensible and traceable documentation of all decisions
- Collaborative development of models necessary

5 Product development at hardware level

6 Product development at software level

7 Production and operation

8 Supporting Processes

8

- Configuration Management and Change Management for all artefacts relevant to development
From Concept to Solution as required by ISO 26262

<table>
<thead>
<tr>
<th>System Responsibility</th>
<th>Requirement Analysis</th>
<th>Architecture &amp; Design</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>normally OEM</td>
<td>3-7 safety goals</td>
<td>3-5 item definition</td>
<td>4-9 system safety validation</td>
</tr>
<tr>
<td></td>
<td>3-8 functional safety concept</td>
<td>3-8 preliminary architectural assumptions</td>
<td>4-8 vehicle integration testing</td>
</tr>
<tr>
<td></td>
<td>3-8 functional safety requirements</td>
<td>4-6 technical safety requirements</td>
<td>4-8 system integration testing</td>
</tr>
<tr>
<td></td>
<td>4-6 technical safety requirements</td>
<td>4-7 system design</td>
<td>6-10 software integration testing</td>
</tr>
<tr>
<td>Component Responsibility</td>
<td>6-6 software safety architectural level requirements</td>
<td>6-7 software architectural design</td>
<td>6-10 software safety verification</td>
</tr>
<tr>
<td>Normally Tier-1 Supplier</td>
<td>6-6 software safety unit level requirements</td>
<td>6-8 software unit design</td>
<td>6-9 software unit testing</td>
</tr>
</tbody>
</table>

How to Manage it?
Document-centric approach?

Variability Engineer: creates → System configuration/Variant definition

System Architect: creates → System architecture

FMEA Analyst: creates → FMEA

Requirements Engineer: writes → Requirement document

System tester: creates → Tests
From Concept to Solution as required by ISO 26262

<table>
<thead>
<tr>
<th>Requirement Analysis</th>
<th>Architecture &amp; Design</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Responsibility</strong></td>
<td><strong>Component Responsibility</strong></td>
<td></td>
</tr>
<tr>
<td>3-7 safety goals</td>
<td>3-8 preliminary architectural assumptions</td>
<td>4-9 system safety validation</td>
</tr>
<tr>
<td>3-8 functional safety requirements</td>
<td>3-5 item definition</td>
<td>4-8 vehicle integration testing</td>
</tr>
<tr>
<td><strong>3-8</strong> functional safety concept</td>
<td><strong>4-6/7</strong> technical safety concept</td>
<td><strong>4-8</strong> system integration testing</td>
</tr>
<tr>
<td><strong>4-6</strong> technical safety requirements</td>
<td><strong>4-7</strong></td>
<td><strong>6-10</strong> software safety verification</td>
</tr>
<tr>
<td>6-6 software safety architectural level requirements</td>
<td><strong>6-6</strong> software safety unit level requirements</td>
<td><strong>6-6</strong> software safety unit testing</td>
</tr>
<tr>
<td><strong>6-6</strong> software safety architectural level requirements</td>
<td><strong>Software unit design</strong></td>
<td><strong>Software unit testing</strong></td>
</tr>
<tr>
<td><strong>How to Manage it without Modeling Approach?</strong></td>
<td><strong>“Safety needs models”</strong></td>
<td></td>
</tr>
</tbody>
</table>
Model-based (Systems) Engineering

Basis: Graph-based Structure
→ Automation
→ Tool data integration
→ Model transformation

Processes

Model

Tools

Work Products

System Spec

«blockProperty»
«blockProperty»
«blockProperty»
Methodology is **your** Responsibility
we provide tools and consulting

**Notation (Language)**
- UML
- SySML
- C#
- etc.

**Tools**
- EA
- MS Office
- Doors
- etc.

**Development Process**
- Agile
- V-Process
- etc.

Roles, milestones, artifacts

**Methodology**
- Harmony
- FAS
- SYSMOD
- etc.

**Modeling Methodology**
- Modeling process
- Model structure
- UML Profile
- etc.
Time and Cost Reduction of MDE

- **C: +23%**
  - **T: +18%**
  - Requirement Analysis
  - Test Cases
  - System Tests

- **C: +10%**
  - **T: +6%**
  - System Architecture
  - Test Cases
  - Integration Tests

- **C: +37%**
  - **T: +25%**
  - Design
  - Test Cases
  - Module Tests

- **C: -9%**
  - **T: -12%**
  - Implementation

- **C: -46%**
  - **T: -45%**

**Challenges**

- More effort at the beginning - *positive effect later*
- Modeling qualification of employees is required
- Multiple Tools and Methods are required

**Sascha Kirstan:**
Modeling Methodology gives the Answers

- In what order to do what?
- What diagrams should I use for what purpose?
- Where to store what model elements?
- How to prevent redundancy in the Model?
- What does mean Traceability in term of UML model?
- Why SysML/UML does not help me to solve these problems?
- Why does everybody models differently?
Standards in Model-based Systems Engineering

• UML – Unified Modeling Language

• SysML – Systems Modeling Language

• AUTOSAR Virtual Function Bus modeling

• ReqIF – Requirements Interchange Format
What is SysML?

- The *Systems Modelling Language* (SysML) is a *standardized graphical* language to describe and specify technical systems of all kind, consisting of hardware and software components.

- SysML is based on the software modeling language UML (Unified Modeling Language) and reuses parts, but also extends and adds some new possibilities.

- With SysML you can specify:
  - the structure/the architecture
  - the behavior
  - the requirements

  of a system and bring them into relations to each other.

- SysML supports the concept of Systems Engineering.
Main Challenges for MBE for FSM

• Missing Methodology

• UML Profiles

• Traceability

• Configuration & Change Management
Tagging

UML and UML Profiles
SysML extensions for FSM/ISO 26262

Assignment of ASIL levels to components and ports

Coloring of Safety Mechanisms
AUTOSAR VFB Modeling with EA

• Tool extension enables AUTOSAR VFB modeling in EA
UML Profiles

Profile

Stereotype
- _image

TaggedValue
- name1: EnumerationTypes
- name2: Value

«metaclass»
Element

- EnumerationTypes
- literal1
- literal2
MDG Technologies

Define

• Profiles,

• Diagrams and

• Toolboxes

for central deployment
Tracability

... the models intelligence
How to ensure consistency?

Traceability-Tables?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 35</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 37</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 39</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test 40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The table represents traceability between various requirements and tests. Each cell with an 'X' indicates a direct relationship.
Traceability is the Model Intelligence

Disconnected Cells ➔ NOT INTELLIGENT
Disconnected Model ➔ NOT INTERPRETABLE

Traceability = Intelligence
Traceability in EA

- Connectors
- Different Traceability Views
- Relationship-Matrix
Model and View

- In case of graphical languages, it has to be distinguished between the model and various views.
- A view is a projection of a model that shows it from a specific perspective or position and omits objects that are not relevant for this perspective.
Navigierbarkeit einrichten
Configuration Management

Mit Auszug aus IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
IEC 61508 and Version Control

“Die Dokumentation oder der Informationssatz…”

“…muss einen Revisionsindex haben…”

“…effektive Maßnahmen für das Versionsmanagement…”
Configuration Management, Change Management and Collaborative Modeling

Working collaboratively on a model is hard

Versioning for EA Models is hard and error-prone

Tracking Changes in Models is very complex

RESULT → Modeling with EA is often used without Configuration Management → Third Party Tool?!
Versioning in EA

- File Copy
- Baselines
- XMI Export/Import
- Integration with VCS on package level (Lock/Modify/Lock)
• Fine-grained 3-way model diff is necessary
• Change tracking is essential
• Features of VCS are necessary for today’s challenges

“Generell fordern Normen wie IEC 61508 die Existenz eines Configuration Managements. Das bezieht sich auf alle Elemente, also auch auf die UML-Modelle. Der LieberLieber Model Versioner ist für uns dabei der Schlüssel dazu, ermitteln zu können, was in welcher Revision geändert wurde.”
Dipl.-Ing. (FH) Stefan Müller, HIMA Paul Hildebrandt GmbH
Safety-related automation solutions

“In general, standards such as IEC 61508 demand the application of configuration management. This refers to all artifacts, including UML models. Der LieberLieber Model Versioner is our key to revealing the changes that have been made to a revision,”
Dipl.-Ing. (FH) Stefan Müller, HIMA Paul Hildebrandt GmbH
Safety-related automation solutions
...and how it is solved by Vector

- Traceability
- Notation of safety-related elements
- Configuration management
Traceability

• Trace EA->EA
  • Trace Dependency

• Trace EA->X
  • Textually within notes

• Trace X->EA
  • Identifier
    • GUID
    • OwnIdentifier (DSGN-<Module><Id>)
      • Automatically calculated (based on EA ID)
      • Might be specifically defined by user (Alias)

\trace CREQ-1234, SPEC-5678

\trace {2C0069A7-1AEB-4a70-B166-091A3A75AC43}

\trace DSGN-EcuM1234, DSGN-EcuMINitInterface
Traceability

• Specification Overview

<table>
<thead>
<tr>
<th>SPEC</th>
<th>CREQ</th>
<th>CAD</th>
<th>CDD</th>
<th>TCASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPEC-17394</td>
<td>CREQ-1094</td>
<td>(Service)</td>
<td>SubModule LinSM_General</td>
<td>ServiceFunction LinSM_Init</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trigger LinSM_Init</td>
<td>ServiceFunction LinSM_InitMemory</td>
</tr>
<tr>
<td>SPEC-17364</td>
<td>CREQ-1056</td>
<td>(Service)</td>
<td>SubModule LinSM_General</td>
<td>ServiceFunction LinSM_GetVersionInfo</td>
</tr>
<tr>
<td>SPEC-17366</td>
<td>CREQ-1098</td>
<td>(Service)</td>
<td>DesignFeature Mode Request Confirmation Timeout Handling</td>
<td>SubModule LinSM_RequestComMode(FULL_COM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DesignFeature Mode Request Handling</td>
<td>SubModule LinSM_RequestComMode(NO_COM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trigger LinSM_RequestComMode(FULL_COM)</td>
<td>TCASE-5072 (CREQ-based)</td>
</tr>
<tr>
<td>SPEC-10425</td>
<td>CREQ-1100</td>
<td>(Service)</td>
<td>SubModule LinSM_ModeRequest Handler</td>
<td>ServiceFunction LinSM_GetCurrentComMode</td>
</tr>
<tr>
<td>SPEC-52068</td>
<td>CREQ-1251</td>
<td>(Service)</td>
<td>DesignFeature Full Communication Mode Request Repetition</td>
<td>TCASE-2043 (CAD-based)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCASE-2044 (CAD-based)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCASE-2045 (CAD-based)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCASE-2046 (CAD-based)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TCASE-5069 (CAD-based)</td>
</tr>
</tbody>
</table>
Safety Notation

• Where?
  • Functionality (TSR, CREQ)
  • Module
  • Function

• How?
  • SafetyLevel as Property (TaggedValue)

• Additional
  • ShapeScripts Overlay
Safety Notation

• Why?
  • Identify elements for safety analysis.

<table>
<thead>
<tr>
<th>Failure Cause</th>
<th>Failure Mode</th>
<th>Failure Effect</th>
<th>Prob. of Occurrence</th>
<th>Prob. of Detection</th>
<th>Severity</th>
<th>Rationale</th>
<th>Risk</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown</td>
<td>EcuM_AL_Reset</td>
<td>(ASIL D)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invalid input</td>
<td>Unintended behavior</td>
<td>Reset is performed in a wrong way.</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>ResetMode is wrong handled in callout because wrong passed parameter.</td>
<td></td>
<td>SMI-145</td>
</tr>
<tr>
<td>Invalid input</td>
<td>Unintended behavior</td>
<td>Reset is not performed.</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>ResetMode is not handled in callout implementation</td>
<td></td>
<td>SMI-145</td>
</tr>
<tr>
<td>Wrong caller</td>
<td>Unintended behavior</td>
<td>Unintended reset is performed.</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td>SMI-4</td>
</tr>
<tr>
<td>Inconsistent configuration</td>
<td>Unintended behavior</td>
<td>Reset is potentially not performed.</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>ResetMode is not handled in configuration</td>
<td></td>
<td>SMI-145</td>
</tr>
</tbody>
</table>
Configuration Management

• What are the changes? (e.g. relevant for review, impact analysis)

• EA mechanism
  • Audit
  • Baseline

• Simple mechanisms
  • Create/Modify date

• Extended mechanisms
  • Create/Modify version
  • DesignLog/SafetyLog

• Export & Compare
  • Focus on „relevant“ data.
Conclusion

• Model-based development uses a central model repository to integrate all relevant development data.

• You can create relations between all the model elements and so fulfill the process requirements for traceability and consistency.

• Tool data integration enables the reuse of existing data as basis for further tools in the development tool chain (e.g. FMEA-tool).

• Model-based development with SysML in a context of ISO26262 helps to ensure the process requirements and leads to consistent system and safety specifications at the end of the day and a improved time-saving workflow.
Contact

lieberlieber.com
blog.lieberlieber.com

konrad.wieland@lieberlieber.com