On Traceability of Informal Specifications for Model-Based Verification

27th of October 2014

Marco Filax
• DIN EN 61508
  • Recommends formal verification for different safety integrity levels

• Definition
  • Formal verification requires an abstract model in a language with defined mathematical semantics.

• How to apply formal methods correctly?
• Direct transformation of informal system specification

Informal System Specification  --  Formal Model

Domain Knowledge?  \(\rightarrow\)  Traceability?
Proposed Three Phased Methodology

• Distinguish three Sub-Processes

Informal Phase  Semi-Formal Phase  Formal Phase

• → Goal: *Preserve traceability through all stages*
• Goal
  • Structuring Requirements

• Naive
  • Indexing using IBM Doors
  • Problem: Significance of requirements unclear

• Proposed
  • Structuring requirement using different generic categories
  • Identified 8 different categories
    • Adopted from Cimatti et. al.
<table>
<thead>
<tr>
<th>Text Fragment</th>
<th>Semi-Formal Artefacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Requirement</td>
<td>Use Case Diagram</td>
</tr>
<tr>
<td>Glossary Fragment</td>
<td>Component Diagram</td>
</tr>
<tr>
<td>Architecture Fragment</td>
<td>Component Diagram</td>
</tr>
<tr>
<td>Property Requirement</td>
<td>Class Diagram</td>
</tr>
<tr>
<td>Communication Requirement</td>
<td>Sequence Chart</td>
</tr>
<tr>
<td>Functional Requirement</td>
<td>- (formal)</td>
</tr>
<tr>
<td>Safety Requirement</td>
<td>- (formal)</td>
</tr>
<tr>
<td>Annotation</td>
<td>-</td>
</tr>
</tbody>
</table>

- **All Fragments:**
  - Requirement Diagrams
template Schranke

...  

formula bool istGeschlossen;

formula bool istGeschlossen_return;

endtemplate
NUSMVSPEC EF((EF((EF((istGeschlossen = true) & (istGeschlossen return = true)))&((schliee = true)))&((schlieeSchranke = true)))&(((istGeschlossen = true)& (istGeschlossen return = false))));
- Completing Partial Formal Model
  - Functional requirements
  - Add requirement links

- Validating the Consistency
  - Using automatic generated formal specifications

- Developing CTL & LTL specifications
  - Safety requirements
  - Add requirement links
Detailed Three Phases Methodology

- Reducing required domain knowledge
- Preserving traceability
  - Structured approach
  - Requirements & links consistent through all stages

- Precise instructions from first system specification until last verification
THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?

• Deutsche Kommission Elektrotechnik Elektronik Informationstechnik: DIN EN 61508, 2011