Improving Consistency Checks between Safety Concepts and View-based Architecture Design

PSAM12 - Probabilistic Safety Assessment and Management
22-27 June 2014, Honolulu, Hawaii

Pablo Oliveira Antonino (Pablo.Antonino@iese.fraunhofer.de)
Mario Trapp (Mario.Trapp@iese.fraunhofer.de)
View-based Architecture Design
Analogy – Views on a Building

http://www.planungswerkstatt-bau.de
Analogy – Views on a Building
View-based Architecture design

System

Runtime

Devtime

Data

Functions

Deployment

Activities

Technologies

Software

Environment
Safety Concepts
Safety Concepts

- Safety concepts are requirements with a strong emphasis on the architectural elements that compose the measures to be used to prevent safety-critical failures.

ISO 26262 – Road vehicles -- Functional safety
“For the 34 (safety) incidents analyzed, 44% had inadequate specification as their primary cause.”

Health and Safety Executive (HSE), Out of Control: Why Control Systems Go Wrong and How to Prevent Failure, 2005.

“Almost all accidents related to software components in the past 20 years can be traced to flaws in the requirements specifications, such as unhandled cases.”

Safeware Engineering, 2005.
Multitude of artifacts
ISO 26262 – Road vehicles -- Functional safety

Safety requirements shall be traceable to (i) each source of a safety requirement at the upper hierarchical level, (ii) each derived safety requirement at a lower hierarchical level, i.e. realization in the design, and (iii) the specification of verification.

DO-254, DO-178C, ARP 4754, ARP 4761 – Aerospace

“software developers must be able to demonstrate traceability of design against requirements.”
ANSI/AAMI/IEC 62304:2006 – Medical Devices

“Traceability between requirements, software system test, and risk control measures implemented in the software.”

FDA – Medical Devices

“Traceability analysis must be used to verify that the software design of a medical device implements the specified software requirements, that all aspects of the design are traceable to software requirements, and that all code is linked to established specifications and test procedures.”
Traceability among hazards, safety requirements, and architecture of equipments submitted to FDA are usually incomplete, incorrect, and conflicting.


Creating and documenting traceability immediately prior to certification is a common proceeding.

Mäder et al., 2014.

“None of the existing traceability approaches described in the literature are appropriate to meet this demand of the safety-critical domain.”

CoEST - Center of Excellence for Software Traceability, 2012.
Hill Holder Controller
Safety Requirements Specification

Architecture Specification

Diagram of a system with components labeled HHC, BT, Flag, and Brake Torque Controller.
Safety Requirements Specification

Hazard
Self-Braking

Safety Goal
No unintended self-braking

Assumption
HHC only passively holds brake pressure that has been created by the driver.

Strategy
Brake Torque Controller should provide an interface that ensures that only pressure created by the driver is held.

Architecture Specification

HHC

Brake Torque Controller

BT
Flag
Causes

- Multitude of textual documents to specify safety requirements;
- Different understanding of underlying concepts and terminologies.

Consequences

- Ambiguous, incomplete, and inconsistent safety requirements;
- Decrease the efficiency of safety assurance.
Our Approach
CORE

Improving completeness and consistency of safety requirements with respect to architecture design and failure propagation models

Identifying inconsistent and incomplete safety requirements specifications

Consistency and Completeness Checks

Specifying complete and consistent safety requirements with respect to architecture design and failure propagation models

Safety Requirements Decomposition Pattern

Parameterized Safety Requirements templates
Tool support
Why Enterprise Architect?

Source: IIBA UK Business Analysis Survey 2012 (http://uk.theiiba.org/images/reports/basurvey2012_final_v1_0s.pdf)
Why Enterprise Architect?

Source: IIBA UK Business Analysis Survey 2012 (http://uk.theiiba.org/images/reports/basurvey2012_final_v1_0s.pdf)
Improving Consistency Checks between Safety Concepts and View Based Architecture Design

PSAM12 - Probabilistic Safety Assessment and Management
22-27 June 2014, Honolulu, Hawaii

Pablo Oliveira Antonino (Pablo.Antonino@iese.fraunhofer.de)
Mario Trapp (Mario.Trapp@iese.fraunhofer.de)
Linked Slides
Safety Requirements Decomposition Pattern
Hazard Analysis and Risk Assessment

Top-level Safety Requirement

Refinements (n)

Refined Safety Requirements

Usage Context
System Behaviour Specification

Engineering Artifacts that realize behaviour (e.g. Components and Deployment units)
Safety Requirements Decomposition Pattern
Safety Requirements Decomposition Pattern
Linked Slides
Parameterized Safety Requirements Templates
Safety Concepts Decomposition Pattern (2/2)

<table>
<thead>
<tr>
<th>Safety Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>[System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical Safety Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Component Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Component Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under Development</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fault Tolerance Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect and Handle [type of violation] violation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detection Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>It should be detected if [artifact affected by action] is not [action performed - past tense] [threshold of measurement] [Value Constraint] [Timing Constraint]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Containment Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>[artifact affected by action] shall be handled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safety Patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various templates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fault Avoidance/Removal Requirement</th>
</tr>
</thead>
</table>