Requirements Specification Tool for Safety Critical Systems based upon Linked Data

Adj. Prof. Mattias Nyberg
Dept. Sys. Architecture and Tools, Scania R&D
Dept. Mechatronics, KTH

FFI:Espresso+ITEA3:ASSUME+ITEA3:REVaMP
• 40000 employees
• Company in VW Group (Heavy Vehicles)

• In-house development
• Embedded systems development: 500+

• The product: a “truck” in many versions and configurations

• Continuous development and integration

• Agile and lean
The Current Challenges

• Complexity
  – More functions
  – Connectivity
  – ADAS and Autonomous Vehicles
  – Variants

• Competition
  – Faster
  – More efficient development

• Functional safety standard ISO 26262
Specification of requirements is a cornerstone in ISO26262, …but one of the most challenging tasks!

**ESPRESSO**

Project (KTH + Scania):

- How can we build a tool that
- …gives maximum support to the user, when
- …writing requirements specifications according to ISO26262?
Digitalization Vision

Digitalized Development
- automatized generation of ”safety case”
- automatized generation of single artefacts, e.g. FMEA, sequence charts
- automatized checks/verification
- efficient information/documentation management

- increased product quality
- increased development speed
- less engineering hours
- ability to change the product!

Survival!

2017
From Informal Documents to Machine Readable and Integrated Data

- emails
- Microsoft Word
- Microsoft Excel
- JIRA

Traceability!
SESAMM Specifier - Key Capabilities

- focus on the task of requirements specification
- support agile and dynamic working environments => user friendly

- formal references to any Linked Data object
- whole range of requirements notation: informal, semi-formal, formal
- contracts based requirements traceability
- detailed variability
- automatic verification with live feedback
- automated fill-in
Contents

Intro

- ISO26262 and Requirements Engineering
- Linked Data
- Contracts Theory (= Requirements Specification Theory)
- Variability

- SESAMM Specifier (our tool!)
- Demo
ISO 26262 and Requirements Engineering
The Core of ISO26262

Hazard identification

Requirements

Architecture

Requirements

Architecture

Design

ASIL (Automotive Safety Integrity Level) is an attribute of requirements!
Requirements Engineering in ISO26262

- … is the core,
- but ISO26262 introduces new concepts:
  - main role of requirements is to identify safety critical properties
    ⇒ requirements are safety critical artefacts!
  - ASIL – violation of requirements is accepted
  - requirements breakdown – traceability (four levels!)
  - tight interplay between requirements and architecture
  - semi-formal notation for ASIL C and D requirements
# Requirements Notation and Verification according to ISO26262

## Table 1 — Specifying safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Informal notations for requirements specification (^a, b)</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>1b Semi-formal notations for requirements specification (^a, b, c, d)</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1c Formal notations for requirements specification (^a)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

## Table 2 — Methods for the verification of safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Verification by walk-through</td>
<td>++</td>
<td>+</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1b Verification by inspection</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1c Semi-formal verification (^a)</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1d Formal verification</td>
<td>0</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
State-of-Practice of Requirements Engineering in Automotive Electrical Systems Development

- Maturity is in general low
- Quality of requirements is in general bad
- …and is accepted to be bad
- Engineers (and managers) are not very enthusiastic about writing requirements

- Traceability is often not applied
- …since in house-development of components is not as common,
- …and is considered to be one-of or the (!) biggest challenge with ISO26262

- Good tool chains are rare
- Increased interest in formal specification and verification of requirements
Linked Data

Semantic Web

Scania
Tool Chain Architecture based on Linked Data Data

- Test Management System
- JIRA Issue Tracking
- PSM Configuration DB
- SESAMM Tool CAN DB
- OAS PDM System
- Source Code Architecture Model
- SESAMM Specifier Requirements Specification Editor
- Architecture Visualizer
- LD Search and Browse

Linked Data Cloud
Linked Data Schemas = Structural Constraints
Linked Data for Tool Interoperability

- Standardized in OSLC from OASIS
- Used by IBM since 2007 in the Jazz platform (their ALM product suite)
- Used by major companies to integrate tools, e.g. Ericsson, VW
- Direction for PTC, Siemens, …
Contracts Theory

(= Requirements Specification and Traceability Theory)
Contracts Theory

- Structure requirements into Assumptions and Guarantees
- Allocate requirements to elements in the Architecture

- “Design by Contract” Introduced by Meyer (≈1990)
- Specifications for software components
  - Assume-Guarantee reasoning (60’s)
- EU-project SPEEDS: Extension to cyber physical systems
Requirements Tracing as "Contracts"
Requirements are relations between "ports" in the architecture.

The indicated fuel volume must equal the actual fuel volume.
Requirements are relations between properties in the architecture.

The indicated fuel volume must equal the actual fuel volume.

\[ \text{indicatedFuelVolume} \text{ must equal } \text{actualFuelVolume}. \]
Variability
SESAMM Specifier

Linked Data Cloud

Other Tool

Other Tool

Other Tool

SESAMM Specifier
LD Adapter

SESAMM Specifier
Authoring Tool

Perforce .DITA

Other Tool

Other Tool

Other Tool

Other Tool
Demo of SESAMM Specifier

Also during lunch by PhD Jonas Westman (KTH/Scania).
Summary

• **Functional Safety (ISO26262)** is a major challenge for automotive industry.

• **Safety requirements** is the core of ISO26262,

• but maturity is low and

• better tools are needed.

• Espresso project (KTH+Scania) has developed a **requirements specification tool**, with

• unique features:
  – strong integration with Linked Data
  – support for all three requirements notations
  – automatic verification with live feedback
  – detailed variability
  – ...