5th Scandinavian Conference on Systems & Software Safety

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

SCANIA

VINNOVA

KTH VETENSKAP OCH KONST

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

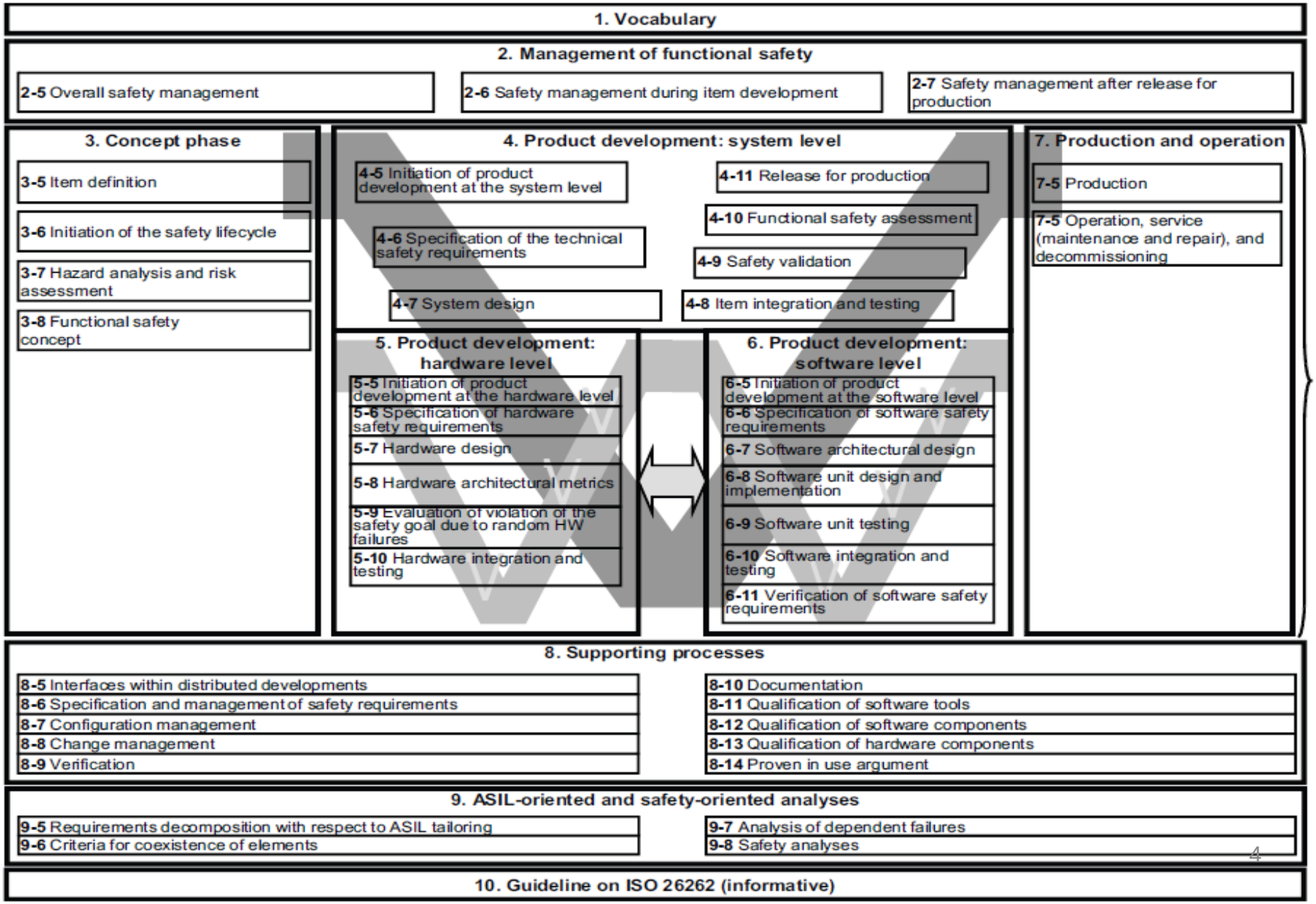
- Continuous development and integration

- 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

ISO26262 Road Vehicles Functional Safety



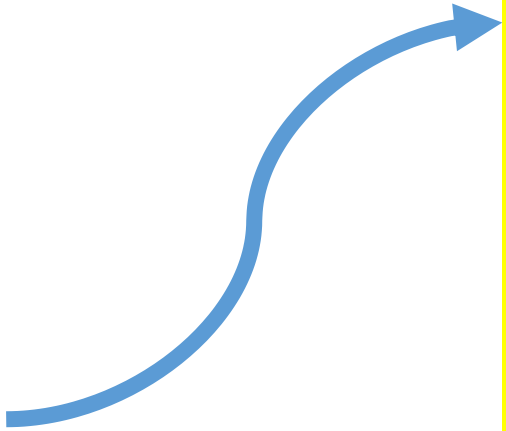
- Specification of requirements is a cornerstone in ISO26262,
- …but one of the most challenging tasks!

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

SCANIA
2017



Digitalized Development

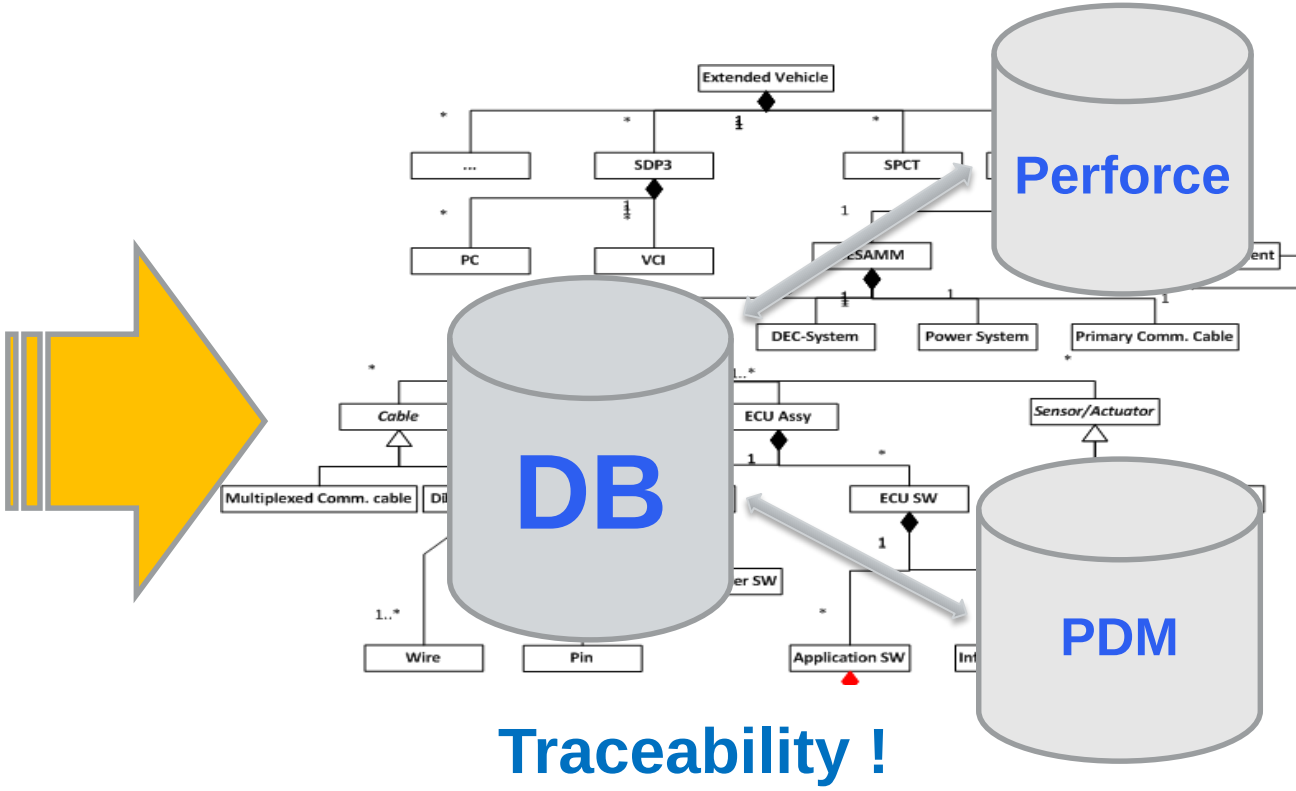
- automatized generation of ”safety case”
- automatized generation of single artefacts, e.g. FMEA, sequence charts
- automatized checks/verification
- efficient information/documentation management

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

Survival!

From Informal Documents to Machine Readable and Integrated Data

- emails
- Microsoft Word
- Microsoft Excel
- JIRA



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

Unique features

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
    $\Rightarrow$ requirements are safety critical artefacts!
  - ASIL – violation of requirements is accepted
  - requirements brakedown – 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

Methods		ASIL			
		A	B	C	D
1a	Informal notations for requirements specification [a, b]	++	++	+	+
1b	Semi-formal notations for requirements specification [a, b, c, d]	+	+	++	++
1c	Formal notations for requirements specification [a]	+	+	+	+

Table 2 — Methods for the verification of safety requirements

Methods		ASIL			
		A	B	C	D
1a	Verification by walk-through	++	+	o	o
1b	Verification by inspection	+	++	++	++
1c	Semi-formal verification [a]	+	+	++	++
1d	Formal verification	o	+	+	+

State-of-Practice of Requirements Engineering in Automotive Electrical Systems Development

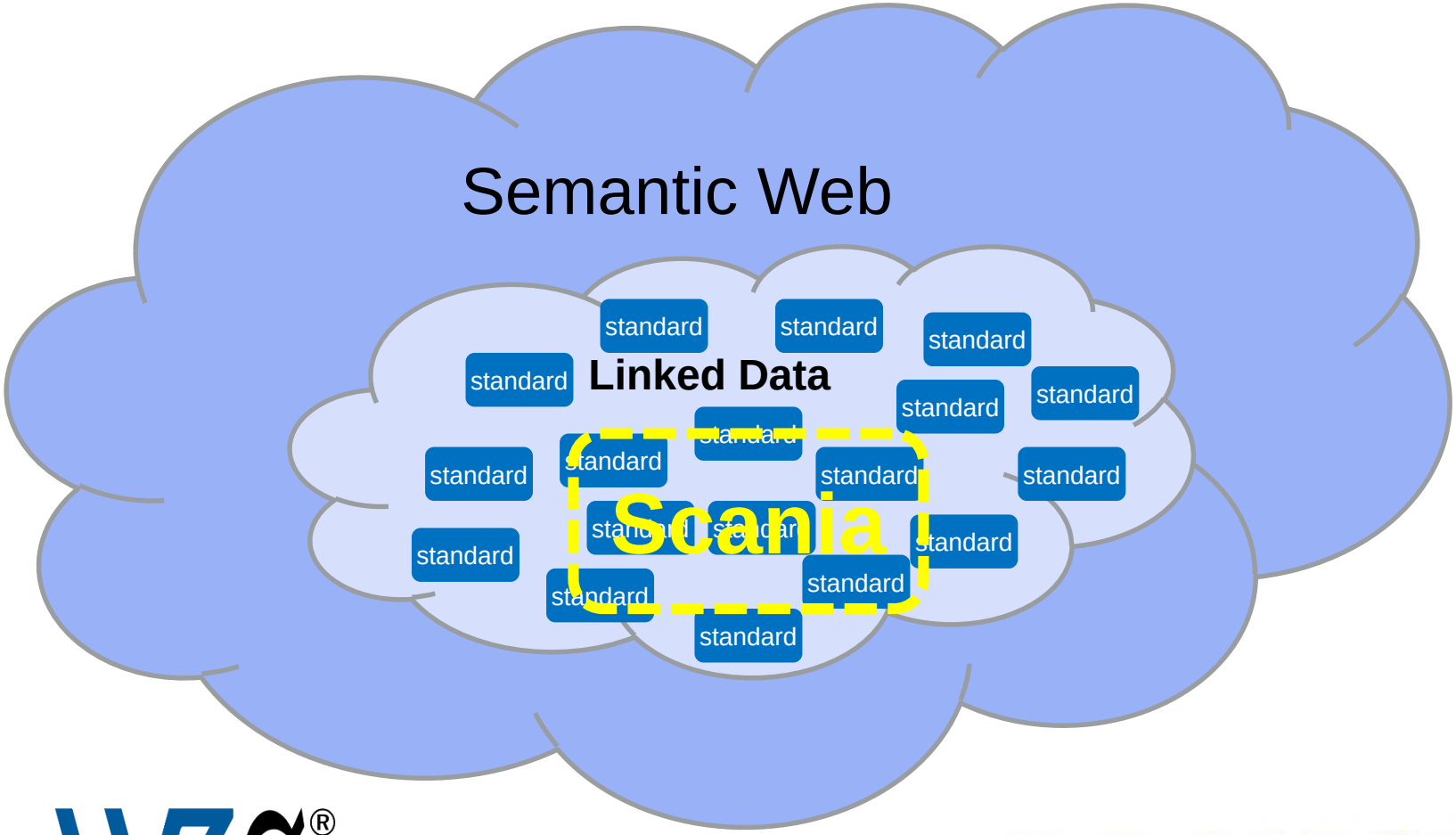
- Maturity is in general low
- Quality of requirements is in general bad
- …and is accepted to be bad
- Engineers (and managers) are not very enthuiastic about writing requirements

- 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

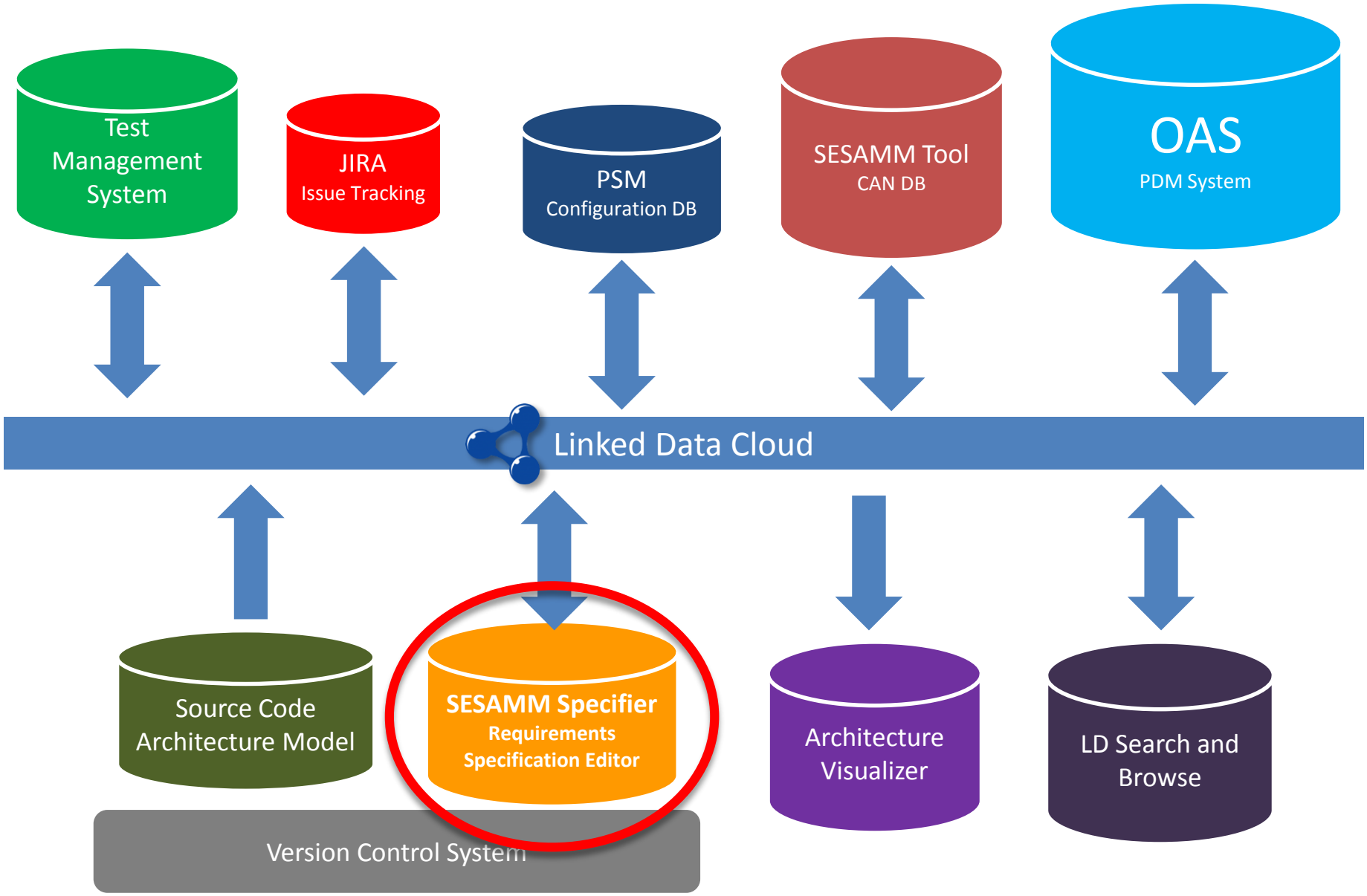
- Good tool chains are rare
- Increased interest in formal specification and verification of requirements

Linked Data

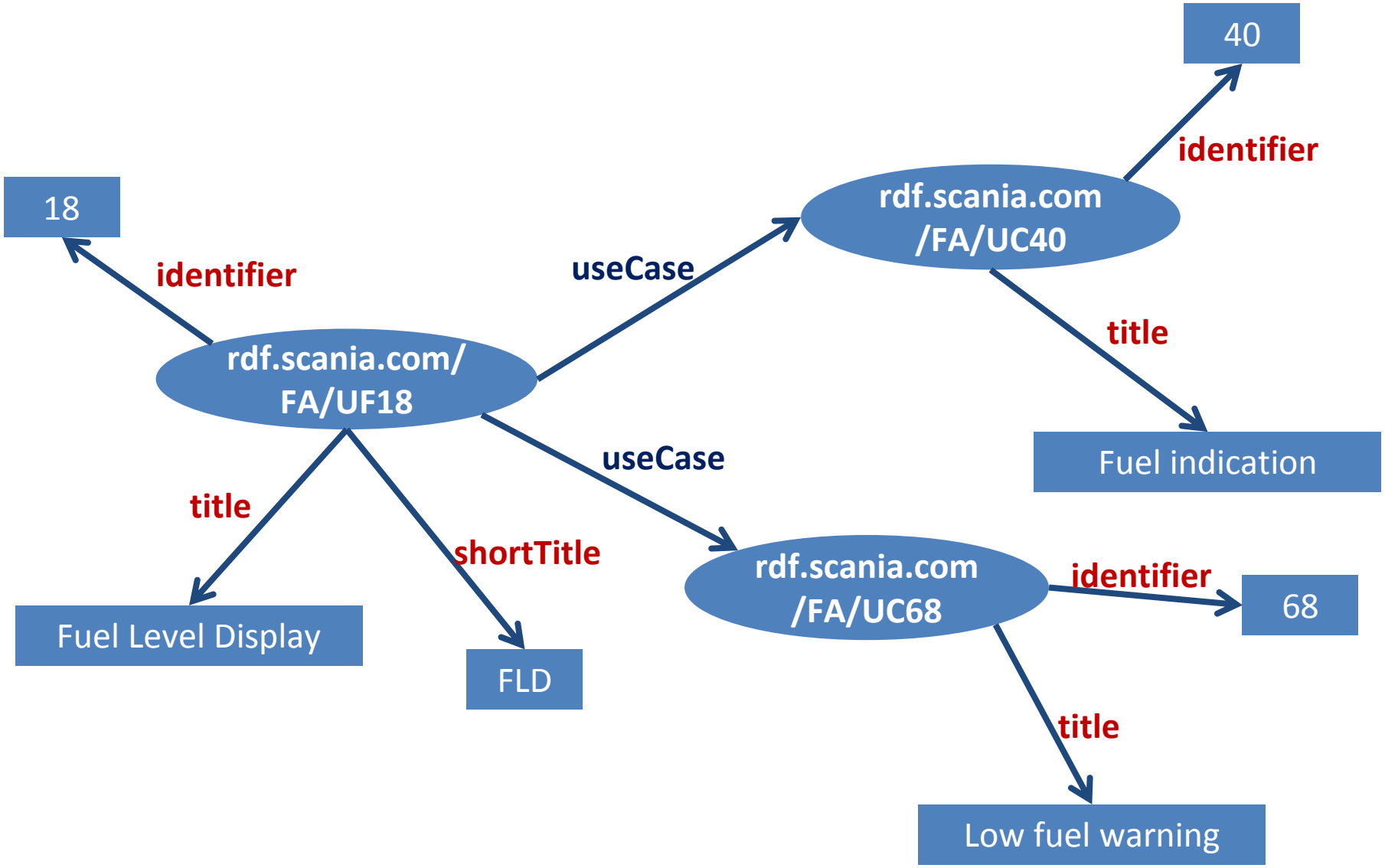
Linked Data



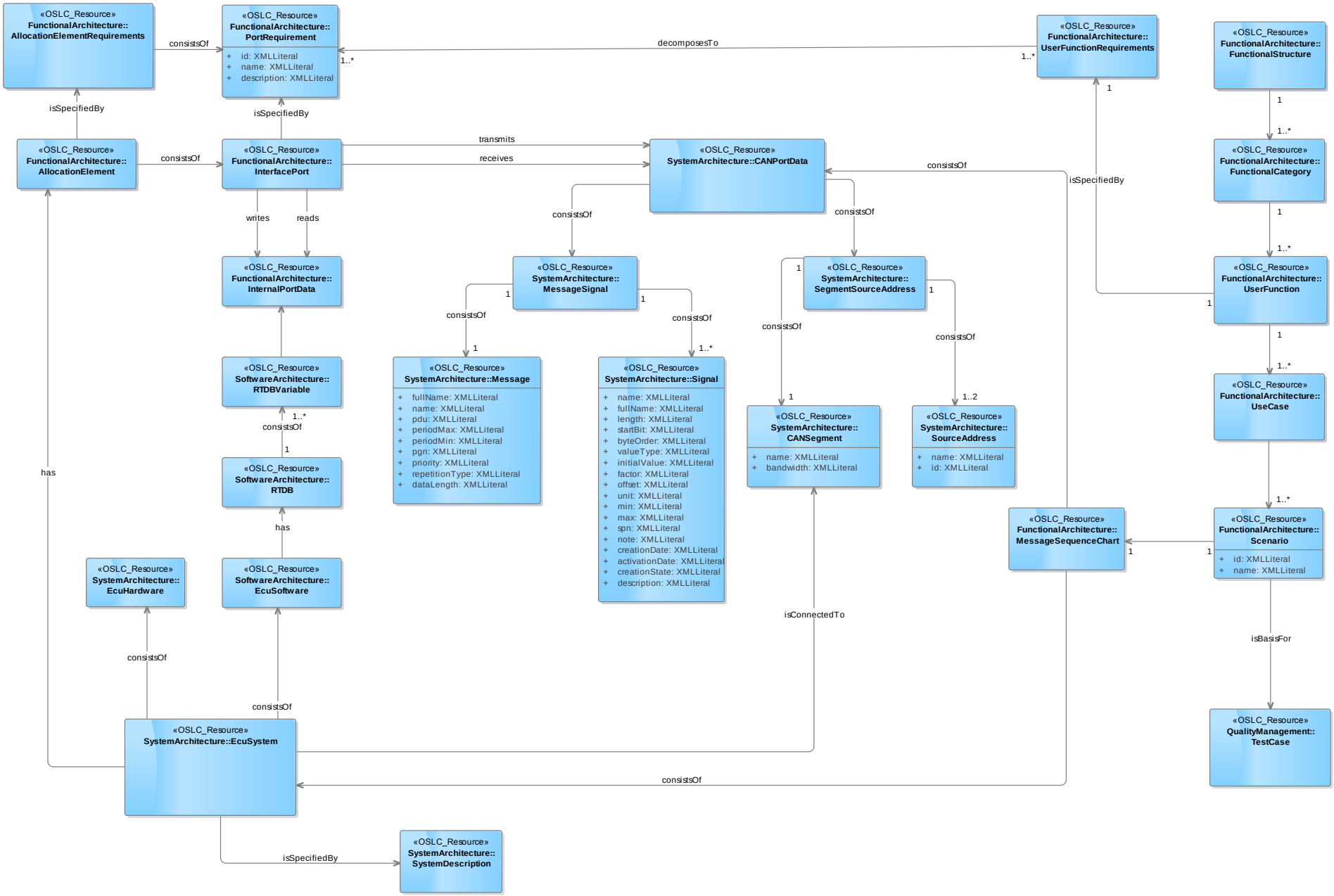
Tool Chain Architecture based on Linked Data



Linked Data


40
identifier
18
rdf.scania.com
/FA/UC40
identifier
useCase
title
rdf.scania.com/
FA/UF18
Fuel indication
useCase
title
shortTitle
rdf.scania.com
/FA/UC68
identifier
68
Fuel Level Display
FLD
title
Low fuel warning

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

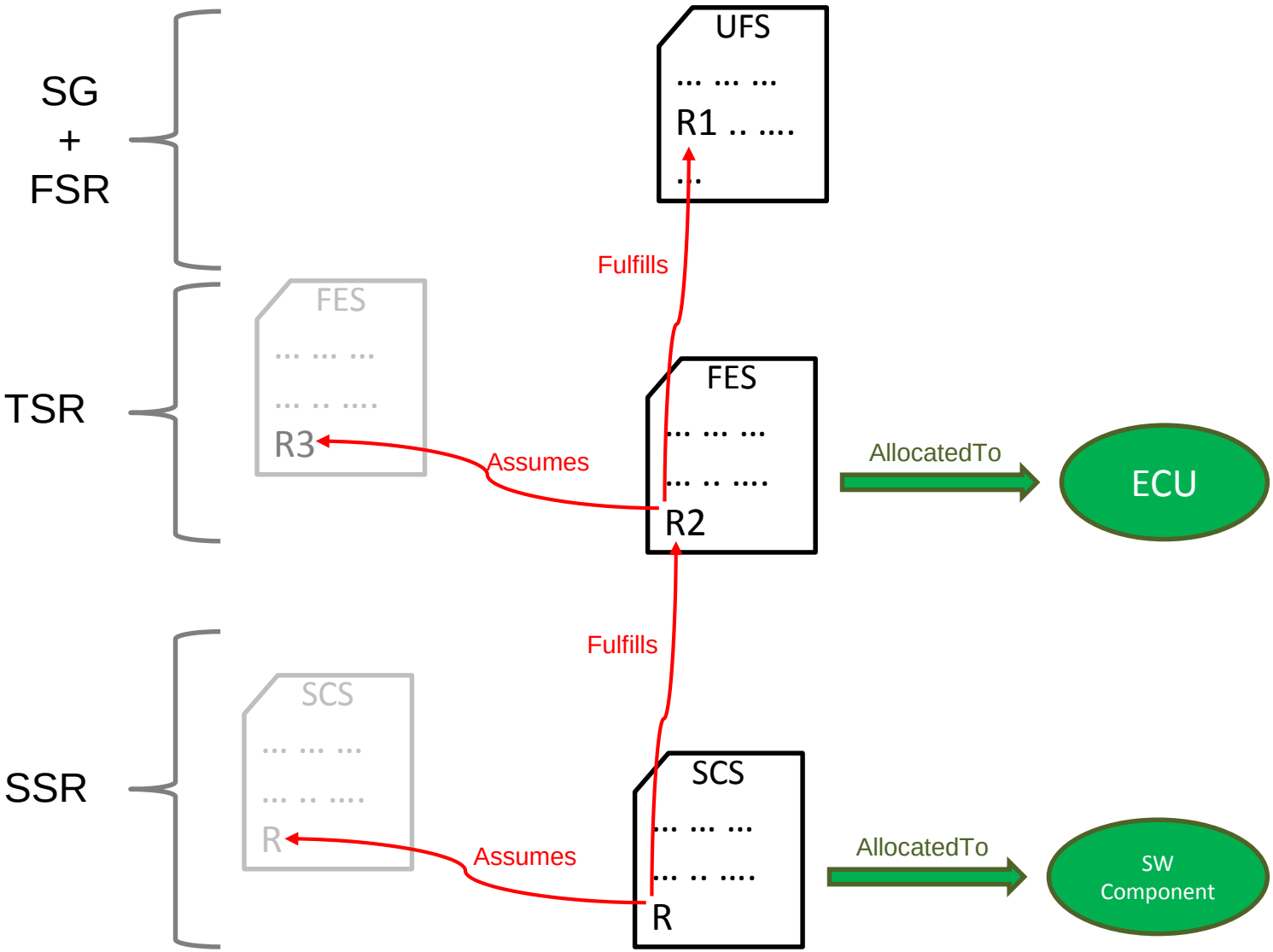
(= Requirements Specification and Traceability Theory)

Contracts Theory

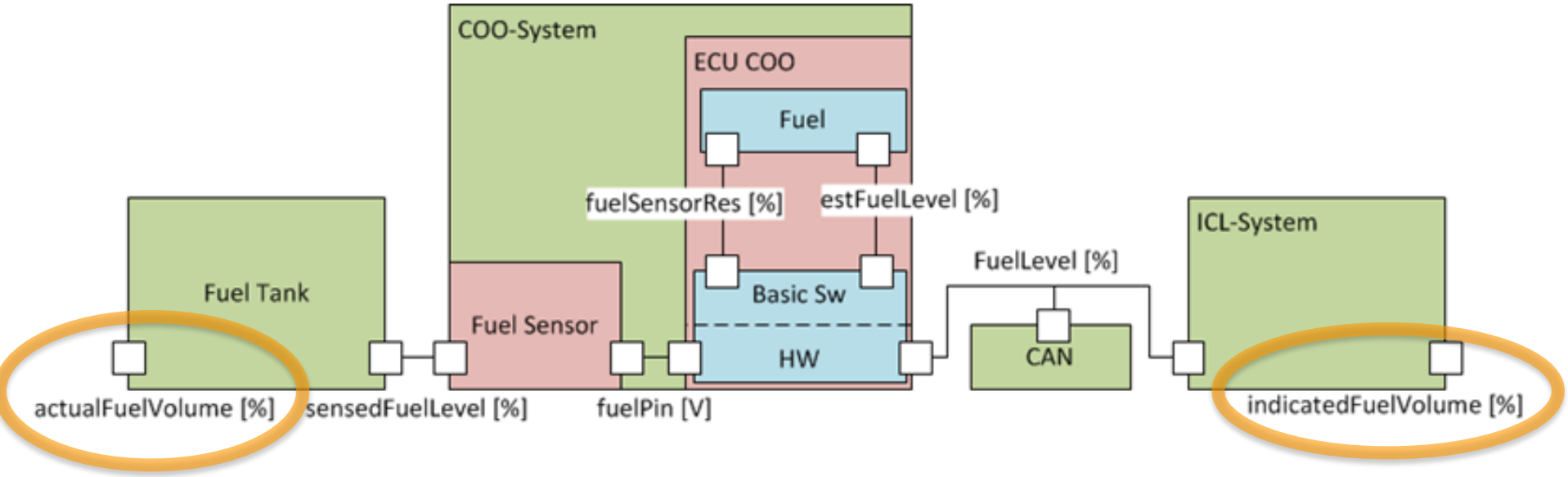
- Structure requirements into **Assumptions** and **Guarantees**
- Allocate requirements to elements in the **Architecture**

- “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”

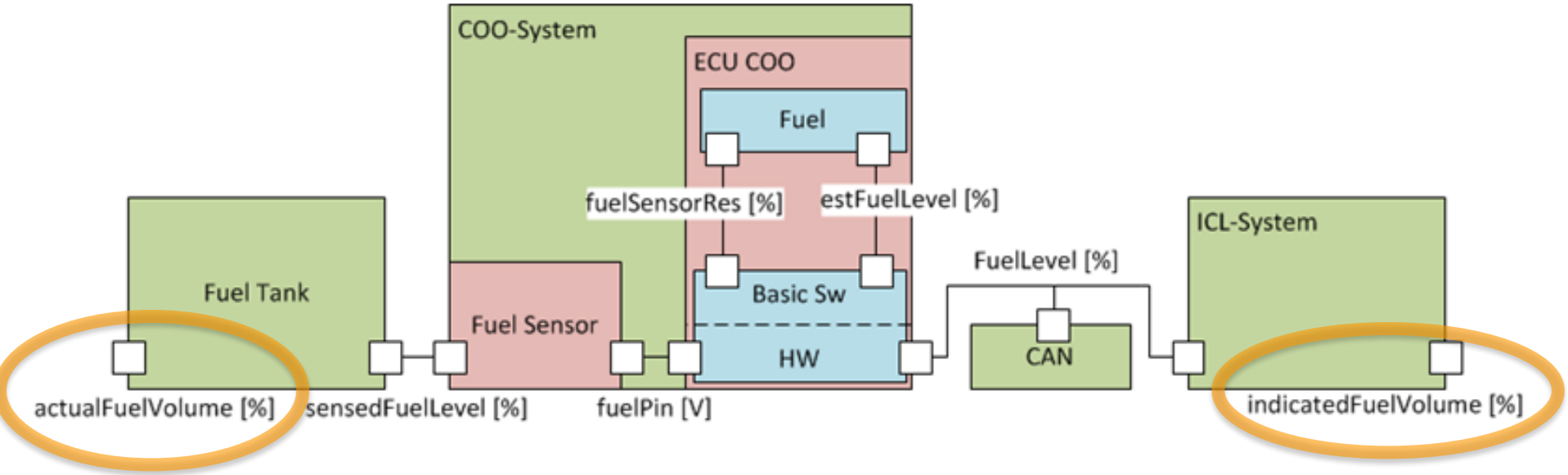


Requirements are relations between ”ports” in the architecture



The indicated fuel volume must equal the actual fuel volume.

Requirements are relations between properties in the architecture



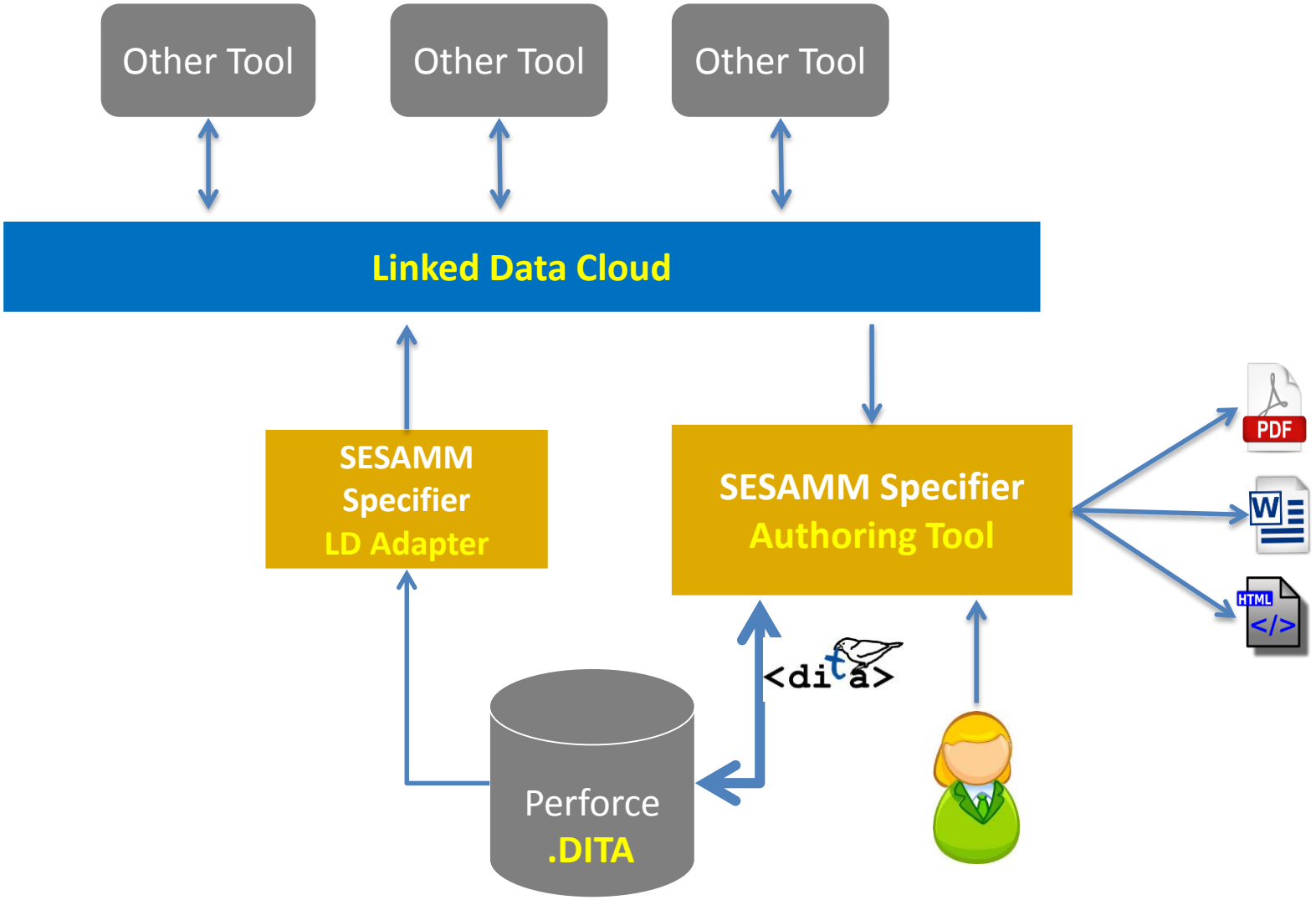
The indicated fuel volume must equal the actual fuel volume.

⇓

`indicatedFuelVolume` must equal `actualFuelVolume`.

Variability

SESAMM Specifier



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
  - …