Towards an ISO 26262-compliant OSLC-based Tool Chain Enabling Continuous Self-assessment

Barbara Gallina[1]
with contribution from and Mattias Nyberg[2]
1 Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se
2 Scania AB, Södertälje, Sweden
mattias.nyberg@scania.com

Work supported by the **Swedish Foundation for Strategic Research** via the **SSF Gen&ReuseSafetyCases project**

23rd May 2017, **5th Scandinavian Conference System and Software Safety (SCSSS)**

MÄLARDALEN UNIVERSITY
SWEDEN

AMASS ESPRESSO2

Barbara Gallina, *Associate Professor*

E-mail: barbara.gallina@mdh.se
Room: U1-068
Phone: +46(0)21-101631
Division: Division of Computer Science and Software Engineering
Research groups: Dependable Software Engineering
Safety-Critical Engineering
Web: Linkedin page

Biography | Research | Publications | Projects | PhD students | MSc theses

Barbara Gallina is Associate Professor of Dependable Software Engineering at Mälardalen University. Currently, she is Vice-chair of the security subgourp within EWICS. Within AMASS, a large EU-ECSEL funded project, she is playing various roles: technical manager at the global level, work package leader, task leader, and land coordinator. She was also the leader of the dependability-related work packages in the EU-Artemis funded SafeCer and CONCERTO projects. She has been visiting researcher at Scania AB, via the SSF-SM14-0013 grant. She has been member of several program committees related to dependability such as SafeComp, ISSRE, EDCC, COMPSAC, QUORS, WoSoCER, SASSUR, ReSACI, ISSA.

She got a M.Sc. in Computer Engineering and a II-level Master in IT, both from Politecnico di Milano (Italy). She got her PhD in Computer Science from the University of Luxembourg (Luxembourg).

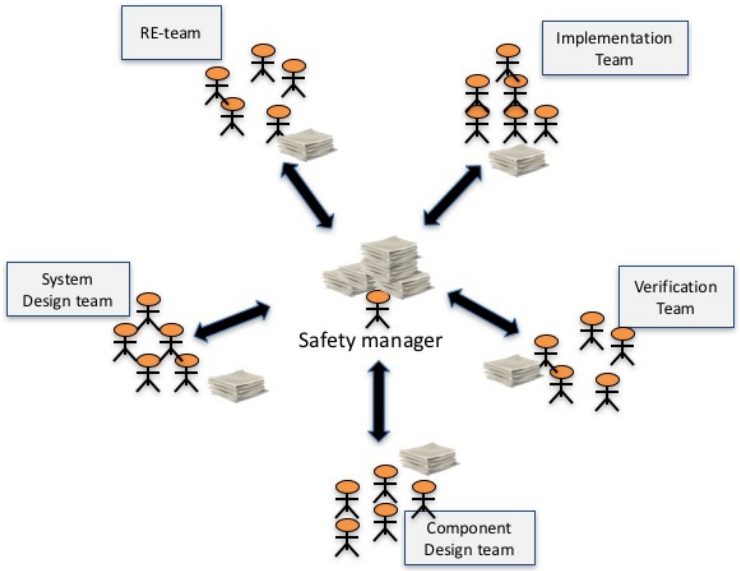
Recent Bio

- **Associate Professor** at MDH, working on Dependability
  - **Dependability modelling and analysis**
  - **ISO 26262-compliant safety case building**
  - **Systematic reuse of (Relaxed) ACID-based transactional artifacts**
  - **Systematic reuse of product-related certification artifacts**
  - **(Safety-critical) Software Development as a Service (SDaaS)**
  - **Systematic reuse of process-related certification artifact**

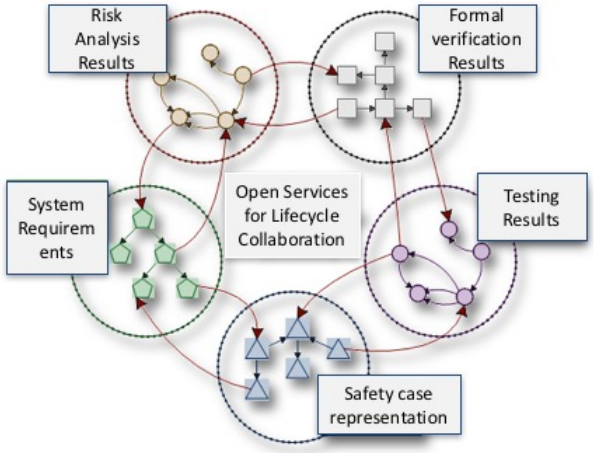
- Research Projects
  - EU ECSEL AMASS: Technical manager, WP/Task-leader
  - EU ARTEMIS CHESS, CONCERTO, p/nSafeCer: (co)WP/Task-leader
  - SSF SYNOPSIS, Gen&ReuseSafetyCases, strategic mobility grant
  - …

Context, motivation, and vision

Current Safety Documentation at Scania (word/excel based)



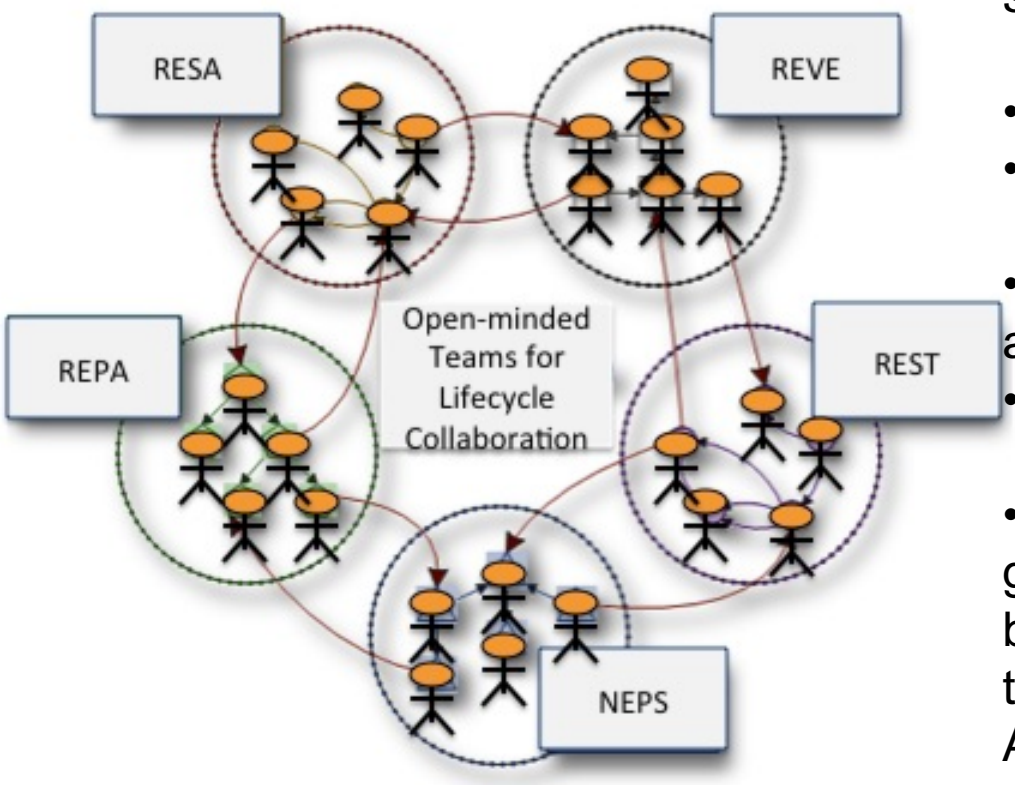
Future Safety Case Creation at Scania OSLC-based



[Gallina et al. 2015]

Safety Case-Argument that the safety requirements for an item are complete and satisfied by evidence **compiled from work products of the safety activities during development**.
ISO 26262- Part 1, Definition 1.106

Soft solution: Open-minded Teams for Lifecycle Collaboration



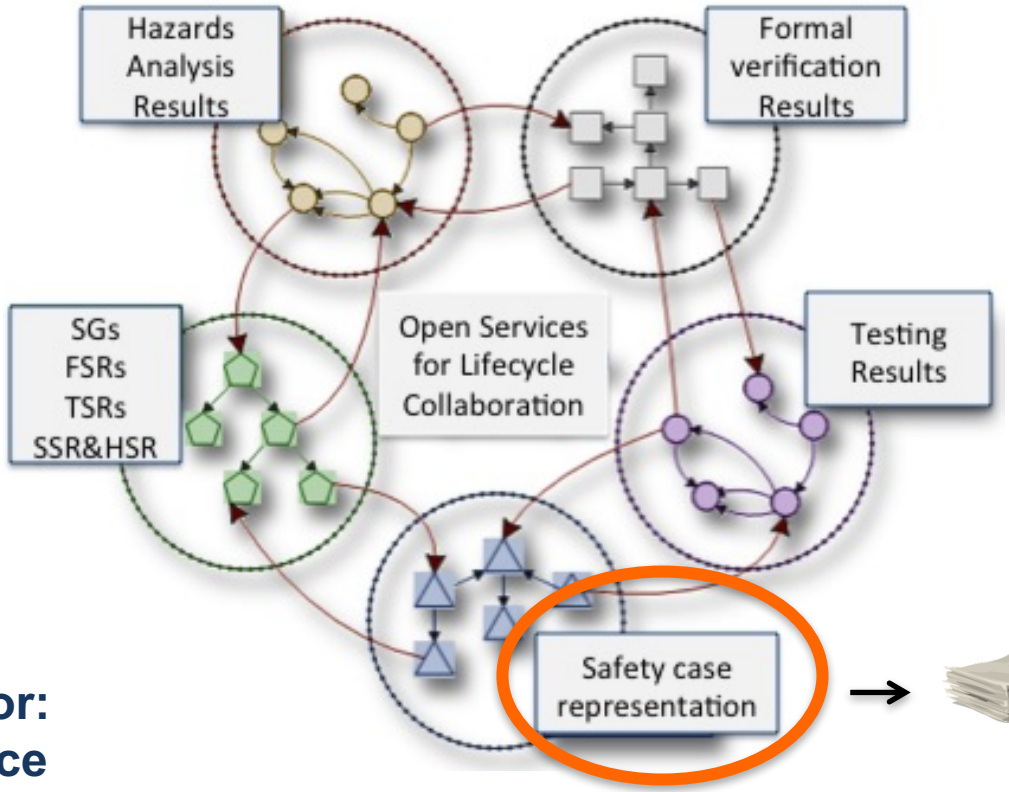
Adapted from the original OSLC figure

ISO26262:
safety manager can delegate tasks!

- Work performed by the different teams
- Replace safety manager by a safety case generator
- Avoid the introduction of additional hierarchical roles
- Flat hierarchy is preserved

•A safety manager should be appointed to guarantee the continuous integration of best practices, which should be suggested to the various teams
A safety manager should be mindful and vigilant

Hard solution: OSLC-based interoperable tools

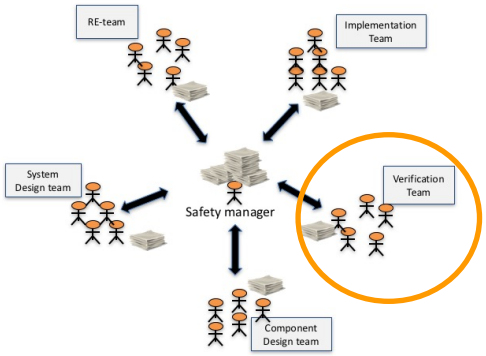


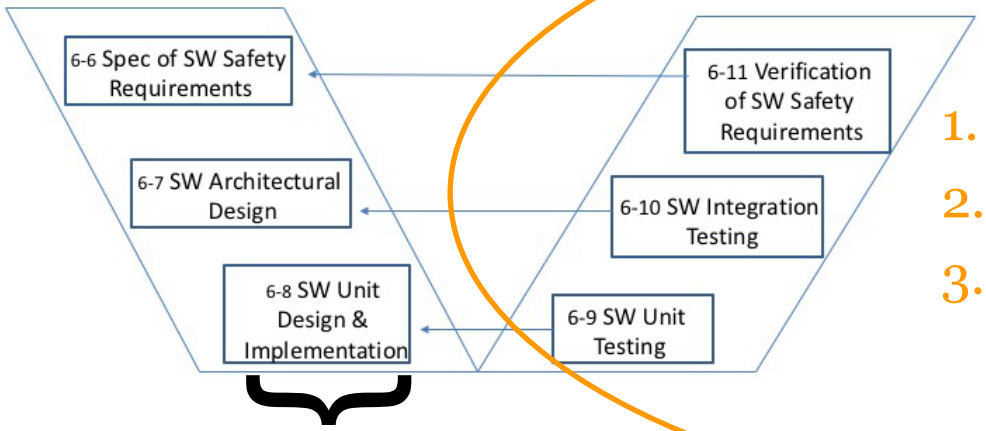
Safety-case generator:
Consumer of evidence
Producer of evidence-supported composable argument-fragments,
contributing to showing that the product is acceptable safe

Talk outline

- Background
  - ISO 26262 (focus on Part 6, clause 8-9)
  - OSLC (Open Services for Lifecycle Collaboration)
  - CSM (Chassis Management System) 1
- Core
- Related work
- Conclusion and future work

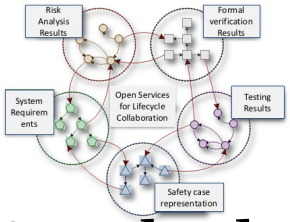
ISO 26262





1. Software verification plan
2. Software verification specification
3. Software verification report

[Gallina et al. 2016, CARS-2016]



OSLC

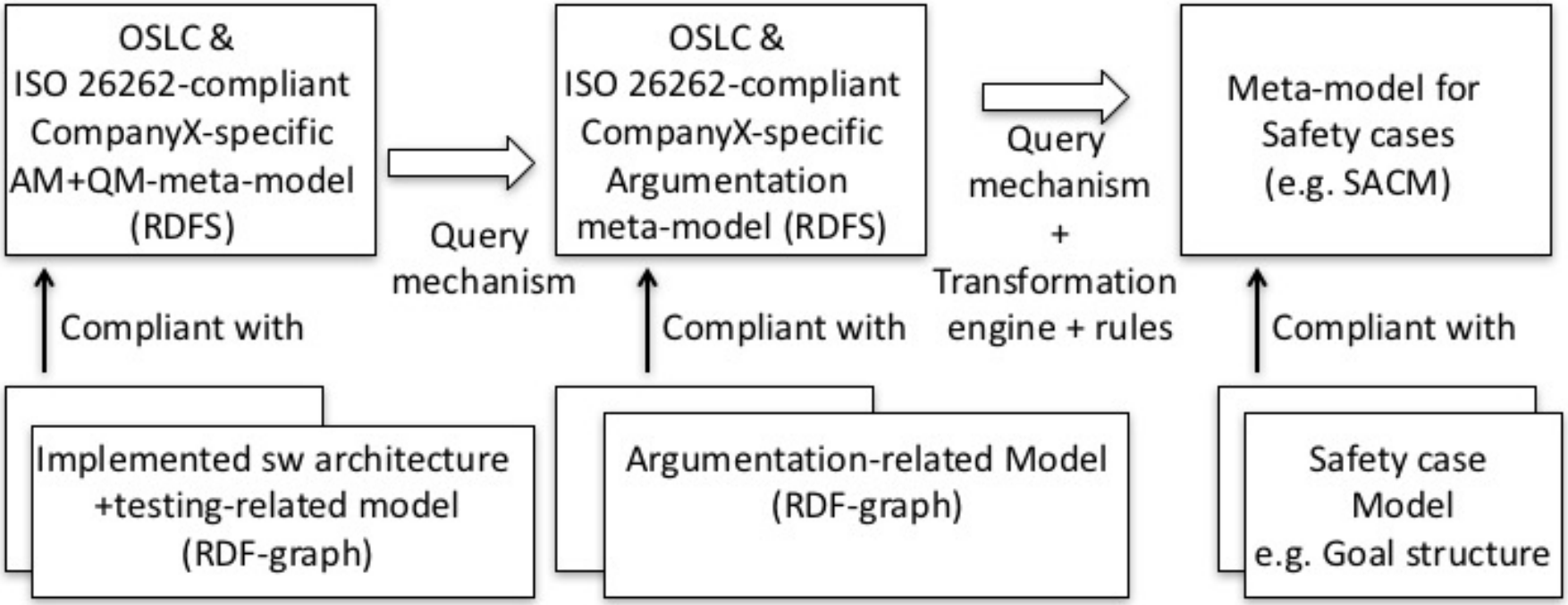
Open Services for Lifecycle Collaboration

- Standard aimed at enabling life cycles tools interoperability
  - Various extensible specifications are at disposal
    - Predefined OSLC domains, including QM (quality management) and AM (Architecture Management)
      - QM defines QM resources (Test Plan, Test Case, Test Script, Test Execution Record, and Test Result)
  - builds on top of:
    - Linked Data
    - Resource Description Framework (RDF)
    - RDF Schema
    - HTTP protocol
    - SPARQL

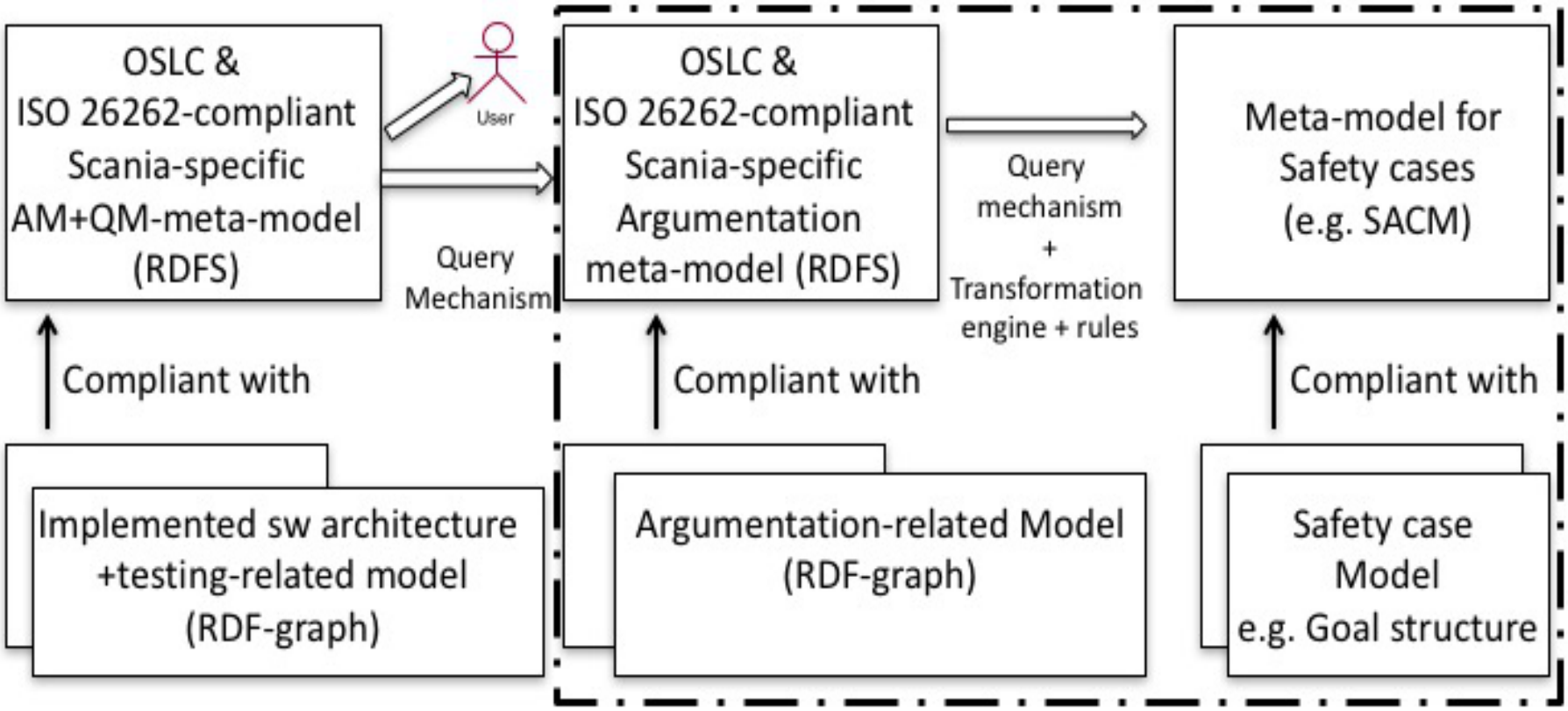
CMS (Chassis Management System)1

- is an ECU (Electronic Control Unit) used for realising the Fuel Level Estimation and Display System functionality within Scania products.
- is responsible for calculating the total fuel level.

Continuous self-assessment: technical solution



Continuous self-assessment: technical solution



Creating ISO 26262-compliant OSLC domains

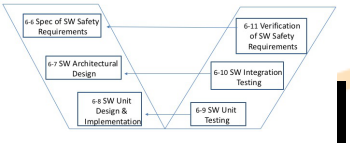
- First, we create a metamodel in compliance with a UML-profile for OSLC

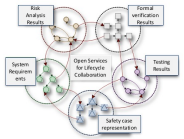
9.5 Work products

9.5.1 **Software verification plan (refined)** resulting from requirements 9.4.2 to 9.4.6.

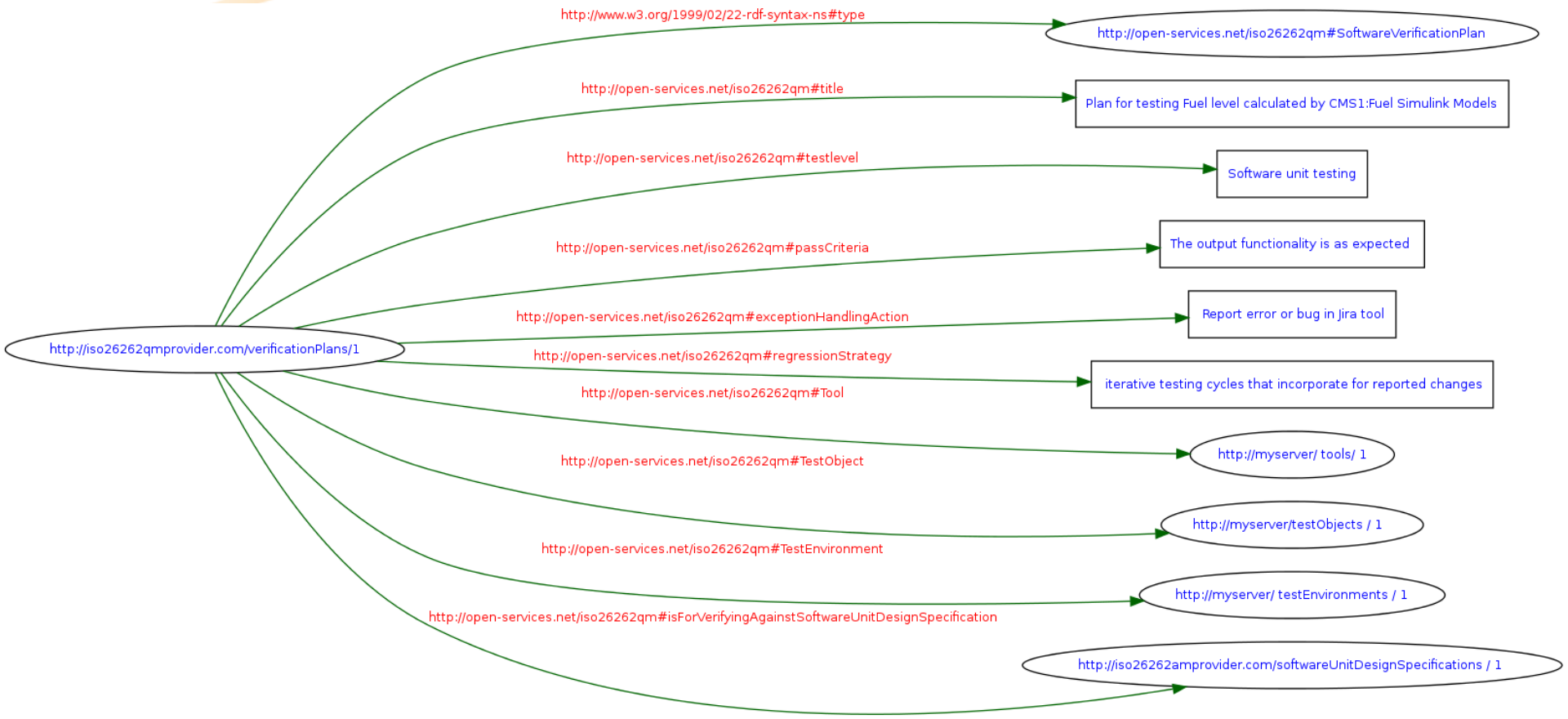
9.5.2 **Software verification specification** resulting from requirements 9.4.2 and 9.4.4 to 9.4.6.

9.5.3 **Software verification report (refined)** resulting from requirement 9.4.2.





ISO 26262-compliant QM extension


http://iso26262qmprovider.com/verificationPlans/1
http://www.w3.org/1999/02/22-rdf-syntax-ns#type
http://open-services.net/iso26262qm#SoftwareVerificationPlan
http://open-services.net/iso26262qm#title
Plan for testing Fuel level calculated by CMS1:Fuel Simulink Models
http://open-services.net/iso26262qm#testlevel
Software unit testing
http://open-services.net/iso26262qm#passCriteria
The output functionality is as expected
http://open-services.net/iso26262qm#exceptionHandlingAction
Report error or bug in Jira tool
http://open-services.net/iso26262qm#regressionStrategy
iterative testing cycles that incorporate for reported changes
http://open-services.net/iso26262qm#Tool
http://myserver/ tools/ 1
http://open-services.net/iso26262qm#TestObject
http://myserver/testObjects / 1
http://open-services.net/iso26262qm#TestEnvironment
http://myserver/ testEnvironments / 1
http://open-services.net/iso26262qm#isForVerifyingAgainstSoftwareUnitDesignSpecification
http://iso26262amprovider.com/softwareUnitDesignSpecifications / 1

Validation

- We performed empirical validation
  - Questionnaire-based validation
    - traceability, confirmability and abstraction
  - →positive feedback from the respondents

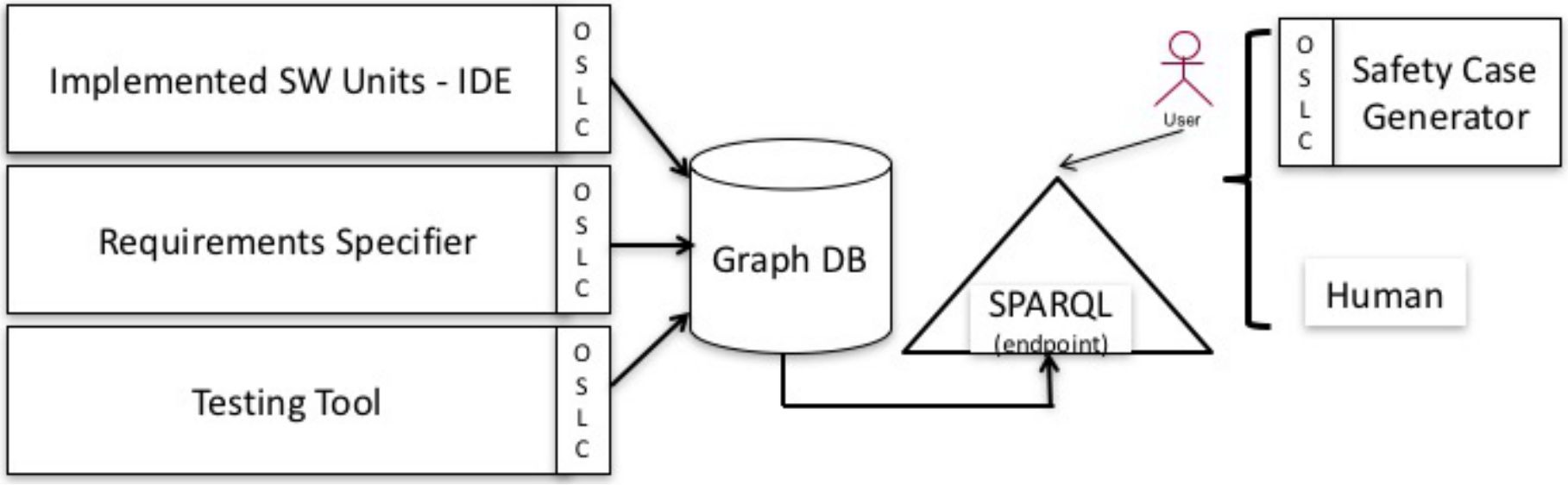
Continuous self-assessment

- The generation of the safety case can be done continuously allowing for monitoring of its progress: from a preliminary and skeleton-oriented version to a complete and operational one.

HOW?

Continuous self-assessment

- Via SPARQL queries



Continuous self-assessment

```
PREFIX oslc_iso26262am: <http://open-services.net/ns/oslc_iso26262am#>
PREFIX oslc_iso26262qm: <http://open-services.net/ns/oslc_iso26262qm#>
ASK{
  { ?subject oslc_iso26262qm:passResult ?o
    FILTER(xsd:integer(?o="1"))}
}
```

Claim 1: CMS1:Fuel was successfully tested.
Context 1: Definition of successfully tested via coverage criteria.
Claim 1.1: All critical test cases passed
Context 2: Definition of critical test cases.
Strategy 1.1: Argument over test case TC1
*Claim 1.1.1: Test case TC1 ("*http://open-services.net/ns/oslc_iso26262qm*/testCases/1") passed*
Evidence: Test Execution Log (rdf:resource= http://open-services.net/ns/oslc_iso26262qm/ *testExecutionLogs/1);*

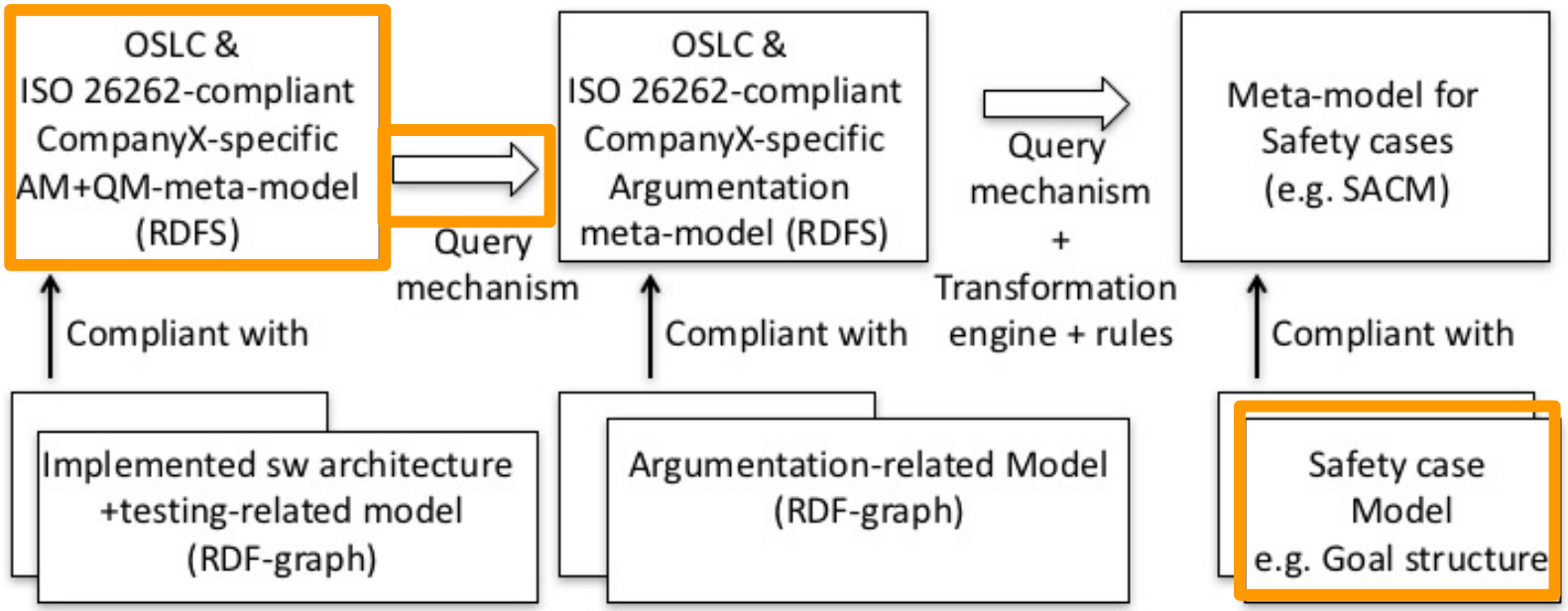
Related work

- [Alvarez-Rodriguez et al. 2015] authors propose an OSLC Knowledge Management specification and a mapping between RDF and RelationSHiP to enable N-ary relationships representations.

- [Regan et al. 2015] authors propose a Process Assessment Model based on ISO 15504. Authors envision the possibility to automate the generation of a safety case via the exploitation of the OSLC specifications. The vision is discussed but no concrete step is carried out.

Conclusion and future work

- First step towards an ISO 26262-compliant OSLC-based tool chain enabling continuous self-assessment –technical solution



References

- [Alvarez-Rodriguez et al. 2015] J. L. Jose Mara Alvarez-Rodrgiuez, Manuela Alejandres and J. Fuentes. OSLC-KM: A knowledge management specification for OSLC-based resources. *25th Annual INCOSE International Symposium (IS) Seattle*, 25(1):16–34, 2015.
- [Regan et al. 2015] G. Regan, M. Biro, D. Flood, and F. McCaffery. Assessing traceability practical experiences and lessons learned. *Journal of Software: Evolution and Process*, 27(8):591–601, 2015.
- [Gallina et al. 2015] B. Gallina and M. Nyberg. Reconciling the ISO 26262-compliant and the Agile Documentation Management in the Swedish Context. In *Critical Automotive applications: Robustness & Safety (CARS), Matthieu Roy, Paris, France, HAL*, September 2015.
- [Gallina et al. 2016a] B. Gallina, J. P. Castellanos Ardila, and M. Nyberg. Towards Shaping ISO 26262-compliant Resources for OSLC-based Safety Case Creation. In *Critical Automotive applications: Robustness & Safety (CARS), Gteborg, Sweden, HAL*, September 2016.
- [Gallina et al. 2016b] B. Gallina, K. Padira, M. Nyberg. Towards an ISO 26262-compliant OSLC-based Tool Chain Enabling Continuous Self-assessment. 10th International Conference on the Quality of Information and Communications Technology- Track: Quality Aspects in Safety Critical Systems (QUATIC), Lisbon, Portugal, 6-9 September, 2016.

Thank you for your attention!

Discussion time…and advertisement:

SAFECOMP´18: Conference on Computer Safety Reliability & Security

Speaker: Barbara Gallina

Type: Conference

Start time: 2018-09-18 09:00

End time: 2018-09-21 16:00

Location: Aros Congress Center, Västerås, Sweden

Contact person: Barbara Gallina

Barbara Gallina,

Email: barbara.gallina@mdh.se

INTERESTED in JOINING as EXHIBITOR? Contact me..