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

Barbara Gallina
with contribution from and Mattias Nyberg
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)
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

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

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

[23rd May 2017, 5th Scandinavian Conference System and Software Safety (SCSSS)]
Soft solution: Open-minded Teams for Lifecycle Collaboration

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

Adapted from the original OSLC figure
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

17th March 16, SCSSS
Talk outline

• Background
  – ISO 26262 (focus on Part 6, clause 8-9)
  – OSLC (Open Services for Lifecycle Collaboration)
  – CSM (Chassis Management System)

• 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

Subject \( \rightarrow \) Predicate \( \rightarrow \) Object
CMS (Chassis Management System)

- 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

**Diagram:**

- **OSLC & ISO 26262-compliant CompanyX-specific AM+QM-meta-model (RDFS)**
  - Compliant with
  - Implemented sw architecture + testing-related model (RDF-graph)

- **OSLC & ISO 26262-compliant CompanyX-specific Argumentation meta-model (RDFS)**
  - Compliant with
  - Argumentation-related Model (RDF-graph)

- **Meta-model for Safety cases (e.g. SACM)**
  - Compliant with
  - Safety case Model e.g. Goal structure

---

23rd May 2017, 5th Scandinavian Conference System and Software Safety (SCSSS)
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 Software unit testing ............................................................................................................................................. 19
9.1 Objectives ......................................................................................................................................................... 19
9.2 General .......................................................................................................................................................... 19
9.3 Inputs to this clause ........................................................................................................................................ 19
9.4 Requirements and recommendations ........................................................................................................... 19
9.5 Work products ................................................................................................................................................. 21

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.
In this section, we provide essential information concerning Part 6 of the ISO 26262 standard, which is related to the software V-model. The clauses 6-8 in Part 6 are related to the right side of the software V-model, as depicted in Fig. 1 adapted from [9]. In this paper, we limit our attention to a subset of clauses (9-11) of Part 6 that are imposed based on the assigned ASIL. In this paper, we focus on the work products that are to be generated. Notes are also included to show the domain instantiation.

**A. ISO 26262**

ISO 26262 regulates all phases of the entire lifecycle of the product (item), starting from the management and requirements specification phases up to the production release. The standard recommends the usage of a V-model at item level as well as at element (software and hardware) level. ISO 26262 consists of 9 normative parts, each of which is structured into clauses. These clauses are:

- Verification of Software safety requirements
- Software integration and testing
- Software unit testing

The main objective of this clause is to verify that the developed software is as per the software architectural design and the embedded software and to verify that the embedded software satisfies all the software safety requirements defined in Part 6, clause 6.

**B. OSLC**

In this section, we present the background information concerning OSLC. OSLC [13] is an industrial standard that targets tools used for requirements engineering, design, implementation, verification, etc. are expected to interoperate in a traceable manner i.e. traceability between the respective work products can be easily retrieved and shown. To enable interoperability, different specifications, called domains, need to be provided. More precisely, an OSLC Domain is one ALM (Application Lifecycle Management) or one Product Lifecycle Management (PLM) topic area such as Quality Management (QM), Architecture Management (AM), Requirements Management (RM). Each OSLC Domain has its own OSLC specification that complies with this core specification. OSLC builds on top of Linked Data [12], Resource Description Framework (RDF) [15], RDF Schema [16], and HTTP protocol. Each tool can provide a list of work products that is to be represented.

In case of a justified and well defined rationale, recommendations and requirements to be fulfilled and finally implemented in a traceable manner can be applied to omit the generation of some work products. The standard recommends best practices for achieving functional safety by recommending the generation of hundreds of work products: software verification report (SVR), software verification plan (SVP), software verification specification (SVS), and software verification plan (SVP). For sake of completeness, it should be mentioned that the standard recommends best practices for achieving functional safety by recommending the generation of hundreds of work products: software verification report (SVR), software verification plan (SVP), software verification specification (SVS), and software verification plan (SVP).

In Section II-B we provide an overview of OSLC and its core structure of linked data, presented in form of RDF-graphs, abstract syntax of RDF as well as its formal semantics. The core of OSLC is described. RDF Schema provides a data-modelling vocabulary based on directed graphs to facilitate the linking of the resources to be manipulated via HTTP methods (i.e., GET, POST, etc.). To interoperate via a Uniform Resource Identifier (URI). Work products are described as an HTTP resource, identified by URI. RDF provides a standard representation for data as triples. Each tool can provide a list of work products that is to be represented. In Section II-C we provide essential information about Part 6-product development at the software domain level. In Section II-B we provide an overview of OSLC and its companion documents which describe the basic concepts and RDF vocabulary. RDF Schema is complemented by several extensions for RDF data. RDF Schema is an extension of the basic RDF vocabulary. RDF Schema provides a data-modelling vocabulary based on directed graphs to facilitate the linking of the resources to be manipulated via HTTP methods (i.e., GET, POST, etc.). To interoperate via a Uniform Resource Identifier (URI). Work products are described as an HTTP resource, identified by URI. RDF provides a standard representation for data as triples. Each tool can provide a list of work products that is to be represented.

**C. CMS (Chassis Management System)**

In Section II-C we provide essential information concerning Part 6 of the ISO 26262 standard, which is related to the software V-model. The clauses 6-8 in Part 6 are related to the right side of the software V-model, as depicted in Fig. 1 adapted from [9]. In this paper, we limit our attention to a subset of clauses (9-11) of Part 6 that are imposed based on the assigned ASIL. In this paper, we focus on the work products that are to be generated. Notes are also included to show the domain instantiation.

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

**ISO 26262-compliant QM extension**

**ISO26262_RM**

- **SoftwareSafetyRequirements**
  - Title: XMLLiteral
  - Identifier: XMLLiteral

**ISO26262_AM**

- **Architecture Design Specification**
  - Title: XMLLiteral
  - Identifier: XMLLiteral
  - TestLevel: softwareTestLevels

**ISO26262_QM**

- **SoftwareVerificationSpecification**
  - TestEnvironment
    - Title: XMLLiteral
    - Identifier: XMLLiteral
    - methodName: targetEnvironment

- **SoftwareVerificationPlan**
  - TestObject
    - Title: XMLLiteral
    - Identifier: XMLLiteral
    - version: XMLLiteral

- **SoftwareVerificationReport**
  - SoftwareVerificationPlan
    - TestObject
      - Title: XMLLiteral
      - Identifier: XMLLiteral
      - version: XMLLiteral
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

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

INTERESTED in JOINING as EXHIBITOR? Contact me..