How to increase efficiency with the certification of process compliance

Barbara Gallina
School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se
Talk outline

• Recent Bio
• Preliminary concepts
  – Certification, process-based certification, etc.
  – Certification crisis
  – Certification framework
• Context and motivation
• Background
• THRUST/MDSafeCer
• Proof-of-concept prototype
• Conclusion and future work
Recent bio - research

- **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
  - ...

2017 March 27th, Malaga University
Recent bio - education

- Education
  - DVA321-Safety-critical systems engineering
  - DVA433-Functional safety, PROMPT initiative
  - New course on certification (to be developed)
  - Contribution to the discussion related to the *Manifesto on Software Process Education, Training and Professionalism*
    - Constructive Alignment extension for safety critical systems
Preliminary concepts

• Certification
  – from Latin, certify --> make certain
  – in common use: attestation by someone trustworthy that a certain statement is true to the best of his/her knowledge

• Why Safety Certification?
  “Safety certification assures society at large that deployment of a given system does not pose an unacceptable risk of harm. There are several ways of organizing and conducting certification, but all are conceptually based on scrutiny of an argument that certain claims about safety are justified by evidence about the system.”

Taken from J. Rushby, Substantially revised version; original appears in Proceedings of the Ninth ACM International Conference On Embedded Software (EMSOFT), pp. 211–218, Taipei, Taiwan, October 2011.
Preliminary concepts

• What can be certified in the context of safety-critical systems?
  – Processes
  – Products
  – Tools used during the development of products
    • Tool qualification processes
  – ...

2017 March 27th, Malaga University
Why process-based certification?

- We have no real consensus on absolutely essential metrics for products.

- It is widely accepted that testing software products completely is not possible. One of the major differences between software products and more traditional, physical products, is that the principle of continuity does not apply to software products. Since software engineers felt that even a huge number of test cases could not guarantee the quality of the product, we turned to supportive evidence, hoping that layers of evidence will add up to more tangible proof of quality/dependability.

Process and process-based certification

- Processes are not useful
- Documentation is not useful

Self-fulfilling prophecy\(^1\)

[Parnas et al 1986] A RATIONAL DESIGN PROCESS: HOW AND WHY TO FAKE IT

\(^1\)A prediction that directly or indirectly causes itself to become true, by the very terms of the prophecy itself, due to positive feedback between belief and behavior
On the statement: processes are not useful

For process-inspiration, consider: https://en.wikibooks.org/wiki/Cookbook:Fried_Eggs

2017 March 27th, Malaga University
On the statement: processes are not useful

Time wasted! Moreover, in the meantime, I might burn the eggs, I might eat cancerogenic substances.
Process-based certification

- Which is the danger?
  - “box ticking” mentality (checklist of deliverables)

- We need product assurance instead of compliance with standards. Compliance with standards is a necessary but not a sufficient condition!

- Why is not sufficient?
  - efficacy of development approaches (UNKNOWN)
  - benefits of certification schemes (UNKNOWN)
Those seeking to reduce costs argue that some of the DO-178B objectives or activities are unnecessary and could be eliminated. The danger is that, if we don’t know why DO-178B works, we could stop doing something that really matters, which could lead to an accident.” Taken from D. Daniels “The Efficacy of DO-178B ”

“never-enough-studied process-product relationship”
Taken from M. Fusani & G. Lami “On the efficacy of safety-related software standards”

Planning the Unplanned Experiment:
Certification crisis!!!

Why?

(Increasingly, many researchers and practitioners are questioning themselves about the value of the current certification processes.)
The framework accommodates all approaches to certification, from current in-use standards based approaches to our own vision for software certification. In fact, there is no reason that the framework could not be applied to any setting in which evaluation takes place.

The framework decomposes any certification scheme into four aspects, indicated by the italicized words in the simplified approach above: evidence, confidence, determination, and certification. The remainder of this section is devoted to discussing each of the aspects in detail. For each, we give its philosophical basis, explain what it is meant to include and to exclude, give examples of the kinds of things that it indicates, and provide a (provisional) further decomposition into useful sub-categories. Figure 1 presents the decomposition in graphical form.

3.1 Evidence

Evidence embodies the empirical part of the certification effort. It consists of the things under consideration: the real-world objects and documents that form the informational foundation of evaluation. Examples of evidence specific to the software setting include source code, requirements, specifications, machine executables, models, test results, proofs of correctness, real-world trial results, etc. Evidence can also include things like personnel qualifications/certifications and documented adherence to development processes.

When we discuss evidence in isolation from the other aspects, we are discussing how to identify, observe, measure, classify and organize items of interest. We are not talking about their trustworthiness, accuracy, relevance, adequacy, or any other such interpretation: these issues are epistemic and therefore fall into the confidence aspect. We are also not talking about the actual performance of any observations or measurements, as this is a pragmatic consideration which is...
Let’s look at reality...
The original **DO-178** had sixty-seven pages. Today's engineers working on a modern Integrated Modular Avionic (IMA) platform have to be familiar with (and in many cases comply to) over a thousand pages of official RTCA publications supported by hundreds of pages of regulatory guidance. The **DO-178C** family of documents alone weighs in at over six hundred pages.

Taken from “**Assuring Avionics – Updating the Approach for the 21st Century**” by T. Ferrell and U. Ferrell, SASSUR, 2014

<table>
<thead>
<tr>
<th>Objective-based</th>
<th>Prescriptive, triple V model + tailoring rules</th>
<th>Prescriptive, V model</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DO-178B</td>
<td>ISO 26262-2011</td>
<td>BS EN 50128:2001</td>
</tr>
<tr>
<td>• DO-178C</td>
<td>ISO 26262-2018</td>
<td>BS EN 50128:2011</td>
</tr>
<tr>
<td>• ...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Motivation

Proliferation of standards → thousands of pages!
→ increasing complexity
→ intellectual unmanageability
→ (re)certification is inefficient (time consuming and expensive!)

IEC 61508
ISO 26262
ASPICE
EN 5012x
DO 178B/C
DO 330
DO-326A

...
How the proliferation of standards could be faced?

- How complexity could be mastered?
- How can we speed up (re)certification?
- How can we enable intra/cross domain reuse?
- How can we enable process-related systematic reuse?
- What varies from one criticality level to another?
- What varies from one version to another?
- What remains unchanged?
- What can be reused?
- What can be generated?
Talk outline

• Preliminary concepts
• Context and motivation
• Background
  – Product lines engineering
  – Safety-oriented process line engineering (SoPLE)
  – Safety-oriented process line modeling
  – Process compliance
  – Process compliance documentation
  – Model-driven Engineering/Certification
• THRUST/MDSafeCer
• Proof-of-concept prototype
• Conclusion and future work
Concurrent engineering of a set of products

- Why? To reuse systematically
  - To reduce time and cost, while increasing quality

Product lines engineering

P1 P2 P3 P4
Product lines engineering

- 2-phase method

**Commonalities**
- Shape

**Variabilities**
- Size
- What else?

**PRODUCT LINE ENGINEERING**
Focus on the product line

**DOMAIN ENGINEERING**
Focus on the product line

**APPLICATION ENGINEERING**
Focus on the product
Product lines engineering
(modelling support)

P4={big, emoticon}
Safety-oriented process line engineering-SoPLE

• Concurrent engineering of a set of safety-oriented processes
  – Why? To reuse systematically!

• Which consists of:
  – Scoping
  – Domain engineering (full and partial commonalities, variabilities)
  – Process engineering

Gallina et al 2012
(SEW Workshop)

Gallina et al 2014
(QUORS Workshop)

Gallina et al 2014
(DEVVARTS Workshop)
Safety-oriented process lines modeling

- **S-TunExSPEM** (SPEM2.0 extension)

<table>
<thead>
<tr>
<th>Task</th>
<th>Role</th>
<th>Tool</th>
<th>Work product</th>
<th>Guidance</th>
<th>Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
</tbody>
</table>

Gallina et al 2014 (SEERA Conference)

- **vSPEM** (SPEM2.0 extension)

<table>
<thead>
<tr>
<th>Concept</th>
<th>Variation point</th>
<th>Variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
</tr>
</tbody>
</table>

2017 March 27\textsuperscript{th}, Malaga University
Process compliance

• To be compliant, a company has two alternatives:
  – strict and almost literal implementation of the process
    • identification and assignment of roles;
    • execution of all the activities according a specific order (if any) and/or grouping (if any);
    • consumption/provision of all the required work products;
    • application of specific guidance (if any);
    • usage of specific tools (if any).

  – execution of a tailored process
Process compliance documentation

- Textual languages (plain natural language)
- Graphical notations
  - CAE
  - GSN

SACM (Structured Assurance Case Metamodel) 2.0
Model-driven Engineering

- MDE: Model-centric software engineering method
  - Model transformations from **source to target space**
    - Vertical transformations aimed at generating code
    - Horizontal transformation aimed at analyzing properties
Talk outline

- **Background**
- **THRUST/MDSafeCer**
  - Overview
  - Process
  - Applications
  - Take home message
- **Proof-of-concept prototype**
- **Conclusion and future work**
THRUSt

SoPL

Process compliance
Argumentation Line

+ model-driven principles…

Gallina et al 2014
(DASC Conference)
THRUST

- Method for speeding up the creation of process-based artefacts via:
  - Systematic reuse
    - safety-oriented process lines
    - safety argumentation lines
  - Semi-automatic generation
    - model driven certification
THRUST

In this section we present our proposal, called THRUST. THRUST is a method that allows users to speed up the creation of process-related deliverables by combining safety-oriented process line engineering, process-based argumentation line engineering and model driven certification. Figure 2 provides an overview of THRUST given by using S-TunExSPEM.

As Figure 2 shows, THRUST consists of four phases: two process-centered phases and two process-based argumentation-centered phases. The red hat is meant to highlight that THRUST is highly critical. THRUST is expected to provide support for efficient creation and management of process-related deliverables compliant with the most stringent development assurance level, A, of DO-178B/C.

Figure 2. THRUST Overview

As Figure 3 shows, these phases can be partially ordered logically. Various executions are possible since concurrent phases can be serialized in various ways. At the end, however, the deliverables of both branches (left and right) have to be available to satisfy the certification authorities.

Figure 3. THRUST - high-level Activity Diagram

Process-centered phases

In this subsection, we focus on the left-hand branch of the activity diagram, shown in Figure 3, and we reveal the tasks that are embraced by the phases. As Figure 4 shows, the Domain (Process-elements) Engineering phase consists of three tasks, which can be iterated if needed. The first task consists of the interpretation of the set of standards according to S-TunExSPEM, i.e., identification of tasks, safety tasks, etc. Then, common and variable process elements are identified. Finally the process line is modeled by using S-TunExSPEM extension.

Figure 4. Focus on the Process-related Phases

Once the safety-oriented process line model is at disposal, single processes can be derived from it by selecting and composing the required process elements. This derivation is performed during the Process Engineering Phase.

MDSafeCer (Gallina 2014, ASSURE Workshop)
In the context of safety certification, it is required to collect and structure the evidence that a system is acceptably safe. Generally, this requires the provision of process as well as product-based arguments. A safety case should be constituted of two branches (one devoted to process-based argumentation and the other to product-based argumentation). These branches could be developed in parallel and be inter-related. In some safety standards, these branches can be provided separately.

As recalled in the introduction, within ISO 26262, the process-based argumentation is provided separately to be evaluated and documented within the Safety Functional Audit work-product. In this section, we focus on the process-based branch and we present a method to generate and reuse process-based arguments. In particular, in Section III-A we give an overview of our model-driven safety certification method. In Section III-A, we provide the conceptual mapping between SPEM 2.0 and ARM/SACM. Then, in Section III-C, we sketch in natural language the meaningful steps of the algorithm that should be executed to automatically generate process-based arguments from process models.

A. Model-driven Safety Certification

To generate certification artifacts, we propose to use MDE principles and apply them in the context of certification. The idea is to pioneer a Model-Driven Safety Certification (MDSafeCer) method enabling automatic generation of argumentation models from process models. The goal is not the creation of novel goal structures, but the generation of goal structure that have successful stories and a proven compelling power. Thus, reuse of experience is crucial to provide adequate transformation rules allowing for the generation of easy-to-maintain and easy-to-review arguments.

Fig. 2. MDSafeCer overview specified in SPEM 2.0.

As Fig. 2 shows, MDSafeCer is constituted of three chained iterative tasks. The first task, called "Safety process modeling" is detailed in Fig. 3. This first task shows that a process engineer is responsible of modeling a safety process according to the best practices in process modeling as well as according to the standard(s). To model a process, a modeling tool is used. As shown in Fig. 4, once the model is available the process engineer generates a process-based argument by using a model transformation implemented within a transformation engine.

As shown in Fig. 5, this argument, which can be considered a "raw" or better defeasible argument, is then checked and eventually corrected (if fallacies are detected) and/or completed by a safety argumentation expert. Checking and completion is an iterative task, which takes in input also the feedback provided by external assessors. If the transformation engine or the safety argumentation expert detect problems related to the process-based argument due to e.g. missing/wrong information in the process model, new iterations of the first task are required.

Fig. 4. Process-based argument generation.

Fig. 5. Process-based argument Check&Completion.

To perform the generation of the process-based argument via model transformation, no constraint on the source and target meta-models exists. However, by considering the current state of the art in terms of standardization, tool-support and active research community, we choose SPEM 2.0 for the source space and ARM/SACM for the target space. Fig. 6 shows the M2M intended transformation. In case of more appropriate future alternatives, our general approach remains valid. As recalled in Section II, both SPEM 2.0 and ARM/SACM are two domain-specific meta-models and in the context of this paper they represent a possibility towards the realization of our MDSafeCer method, allowing for the generation of ARM/SACM-compliant argumentation models from SPEM 2.0-compliant process models.

Fig. 6. M2M tranformation.

As we discussed in [15] and as it was mentioned in [16], the goal of automation is not to replace human reasoning, but to focus it on areas where they are best used. Similarly, in this work we are not aiming at eliminating human reasoning.
Automotive Safety oriented Process Line Engineering
Focus on development processes

STEP 1 (A) SPICE

ISO 26262

IEC 61508

STEP 2 (A)SPICE

STEP 3 ISO 26262

STEP 4 - 6

STEP 7 Proj. Spec. Process

STEP 8 EXPORT HTML

STEP 9 EXPORT XML

Guideline

Work in cooperation with Virtual Vehicle Research Center

2017 March 27th, Malaga University
Concerning process compliance, in ISO 26262 we can read:

– The organization shall institute, execute and maintain organization-specific rules and processes to comply with the requirements of ISO 26262 (Part 2, 5.4.2.2).

– Organization-specific rules and processes for functional safety is a specific work-product that must be provided (Part 2, 5.5.1).

– A functional safety audit shall be carried out for items, where the highest ASIL of the item’s safety goals is ASIL (B), C, or D, in accordance with 6.4.7, 6.4.3.5 i) and 6.4.8.2. (Part 2, 6.4.8.1), where a functional safety audit is a work-product aimed at evaluating the process implementation.

– The organization may tailor the safety lifecycle (Part 2, 5.4.5.1) and tailoring rules are then detailed.

Thus, for certification purposes, it is crucial to provide work-products aimed at showing that either process activities have been performed according to the ISO 26262 safety life-cycle or they have been tailored appropriately according to the tailoring rules provided within ISO 26262.
Applying MDSafeCer - ISO 26262

1. Glossary

2. Management of functional safety
   - 2.5 Project-independent safety management
   - 2.6 Project-dependent Safety management
   - 2.7 Safety management activities after SOP

3. Concept phase
   - 3.5 Item definition
   - 3.6 Initiation of safety lifecycle
   - 3.7 Hazard analysis and Risk assessment
   - 3.8 Functional safety concept

4. Product development system
   - 4.5 Initiation of product development system
   - 4.6 Specification of technical safety concept
   - 4.7 System design
   - 4.8 Integration and testing
   - 4.12 Product release
   - 4.10 Functional safety assessment
   - 4.9 Safety validation

5. Product development hardware
   - 5.5 Initiation of product development at HW level
   - 5.6 Specification of HW safety requirements
   - 5.7 HW design
   - 5.8 HW architectural metrics
   - 5.9 Evaluation of violation of safety goal due to HW random failure
   - 5.10 HW integration and testing

6. Product development software
   - 6.5 Initiation of product development at SW level
   - 6.6 Specification of SW safety requirements
   - 6.7 SW architectural design
   - 6.8 SW unit design and implementation
   - 6.9 SW unit testing
   - 6.10 SW integration and testing
   - 6.11 Verification of SW safety requirements

7. Production and operation
   - 7.5 Production
   - 7.6 Operation, service and decommissioning

8. Supporting processes
   - 8.5 Interfaces within distributed developments
   - 8.6 Overall management of safety requirements
   - 8.7 Configuration management
   - 8.8 Change management
   - 8.9 Verification
   - 8.10 Documentation
   - 8.11 Qualification of software tools
   - 8.12 Qualification of software components
   - 8.13 Qualification of hardware components
   - 8.14 Proven in use argumentation

9. ASIL – oriented and safety – oriented analyses
   - 9.5 Requirements decomposition with respect to ASIL tailoring
   - 9.6 Criteria for coexistence of elements
   - 9.7 Analysis of dependent failures
   - 9.8 Safety Analyses

10. Guidelines on ISO 26262 (Informative)
Applying MDSafeCer - ISO 26262

1. Create the top-level goal ID:G1 and statement: “The task \( t_a \) has been carried out”. Create the context to be associated to G1. Context ID:C1 and statement: “Standard \( \{x\} \)”, where \( x \) is a variable. Create an inContextOf link to relate G1 and C1.

Develop the goal G1 further by creating four strategies and for each strategy a set of sub-goals.

(a) S1: “Argument over roles \( R \)”.

(b) S2: “Argument over work products \( W \)”.

(c) S3: “Argument over tools \( T \)”.

(d) S4: “Argument over guidance \( G \)”. 
Applying MDSafeCer - ISO 26262  
(towards a process-based argumentation pattern)
Proof-of-concept prototype

- Implementation within AIT-WEFACT-tool
  
  Work in cooperation with:
  
  Austrian Institute of Technology (AIT)
  Virtual Vehicle Research Center (ViF)


- Implementation within the SDaaS-prototype architecture
Take home message

• SoPLE+MDSafeCer may contribute in increasing efficiency

• More efficiency in process certification →
  More time for product-based evidence provision!!
  → e.g., verification results

• SoPLE may contribute in:
  – Re-establishing a balance between the “odd couple” (discipline and creativity)
  – Enabling a transition “from rigid compliance to smart convergence”
  – Enabling a transition from non rationalized standards to rationalized standards

Conclusion

- **THRUST/MDSafeCer:**
  - Novel model-driven approaches for time and cost reduction
    - Mapping of (ideally reusable) process structures (patterns) onto (ideally reusable) argumentation structures (patterns)

- **Manual application on various small-sized sub-processes**
  - Automotive
  - Rail
  - Avionics
  - Space

- **Prototype tool support – proof of concepts**
  - Initial validation
Future work

• Provision of a fully defined pattern for process compliance
• Contribution to provision of adequate metamodels
• Experimental validation on more complex case-studies

• Towards Anti-Sisyphus: combination of
  – safety-oriented process lines,
  – safety-critical product lines,
  – safety case lines
Safety case
(core arguments)

System X is acceptably safe

Context of system X

Process is "safe/compliant" (process-based argument)

Product is acceptably safe (product-based argument)

Evaluated via a safety audit

Fragment of a goal structure, safety argument given in GSN (Goal Structuring Notation)

2017 March 27th, Malaga University
Anti-Sisyphus


Then, integrated within AMASS (http://www.amass-ecsel.eu), see AMASS newsletter 1.

2017 March 27th, Malaga University
Thank you for your attention!

Discussion time…
Publications

International Peer-reviewed Journals

1. **B. Gallina**, E. Gómez-Martínez, C. Benac Earle. Promoting MBA in the Rail Sector by Deriving Process-related Evidence via MDsafeCer. Computer Standards & Interfaces -SPICE-2016 Special Issue (CSI SPICE-2016), [http://dx.doi.org/10.1016/j.csi.2016.11.007](http://dx.doi.org/10.1016/j.csi.2016.11.007);

Publications

International Peer-reviewed Conferences


Publications

International Peer-reviewed Conferences


Publications

International Peer-reviewed Conferences


International Peer-reviewed Workshops


2017 March 27th, Malaga University
Publications

International Peer-reviewed Workshops


