THRUST: A Method for Speeding up the Creation of Process-related Deliverables

Barbara Gallina [1], Kristina Lundqvist [1], and Kristina Forsberg [1,2]
1 School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
name.surname@mdh.se

2 Saab AB, Jönköping, Sweden
name.surname@saabgroup.com

09th October 14, DASC-33 (Digital Avionics Systems Conference)

Context

- ARP4754
- ARP4754A
- DO-178A
- DO-178B
- DO-178C
- ..

- What do they require?
- What varies from one version to another?
- What remains unchanged?
- Is it possible to systematize reuse of process-related deliverables?
- Is it possible to automatically generate fragments of process-related deliverables

Motivation

- Problem: absence of a systematic approach allowing for reuse and semi-automatic generation of process-related deliverables

  →Provision of deliverables is inefficient

- How reuse could be enabled and accelerated in the context of safety processes and more specifically avionics-related processes and assurance cases?
- How process-based safety-related arguments could be derived from process models?

Talk outline

- Background
  - DO-178B/C
  - Safety-oriented process lines engineering
  - Safety-oriented process line modeling
  - Process compliance
  - Process compliance documentation
  - Model-driven Engineering/Certification
- THRUST
- Applying THRUST: an intuition
- Related work
- Conclusion and future work

DO-178B/C

- GOAL: guarantee a level of confidence in the correct functioning of the software developed in compliance with airworthiness requirements.
  - series of processes characterized by a set of objectives, activities and expected deliverables
    - Process planning
      - Software Development Plan (SDP)
      - Plan for Software Aspects of Certification (PSAC)

Safety-oriented process lines engineering

- Concurrent engineering of a set o safety-oriented process
  - Why? To reuse systematically!
- Which consists of:
  - Scoping
  - Domain engineering (full and partial commonalities, variabilities)
  - Process engineering

Safety-oriented process lines modeling

- S-TunExSPEM
  - SPEM2.0 extension

Task	Role	Tool	Work product	Guidance	Phase
					

Safety-oriented process lines modeling

- vSPEM
  - SPEM2.0 extension

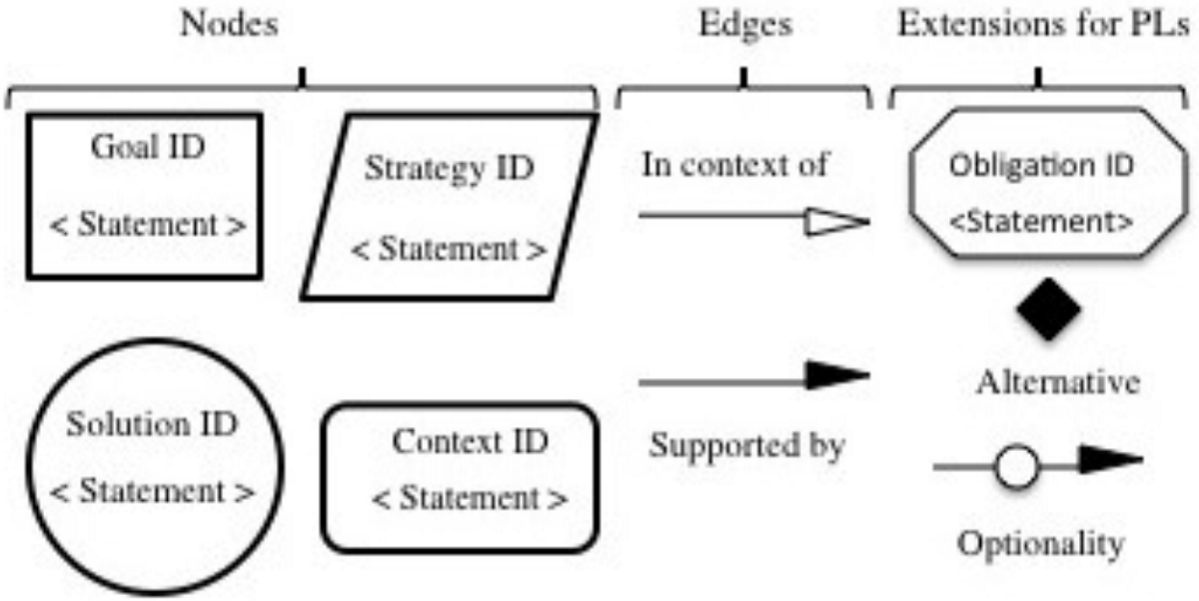
Concept	Variation point	Variant
Task		

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 obtained by applying tailoring rules

Process compliance documentation

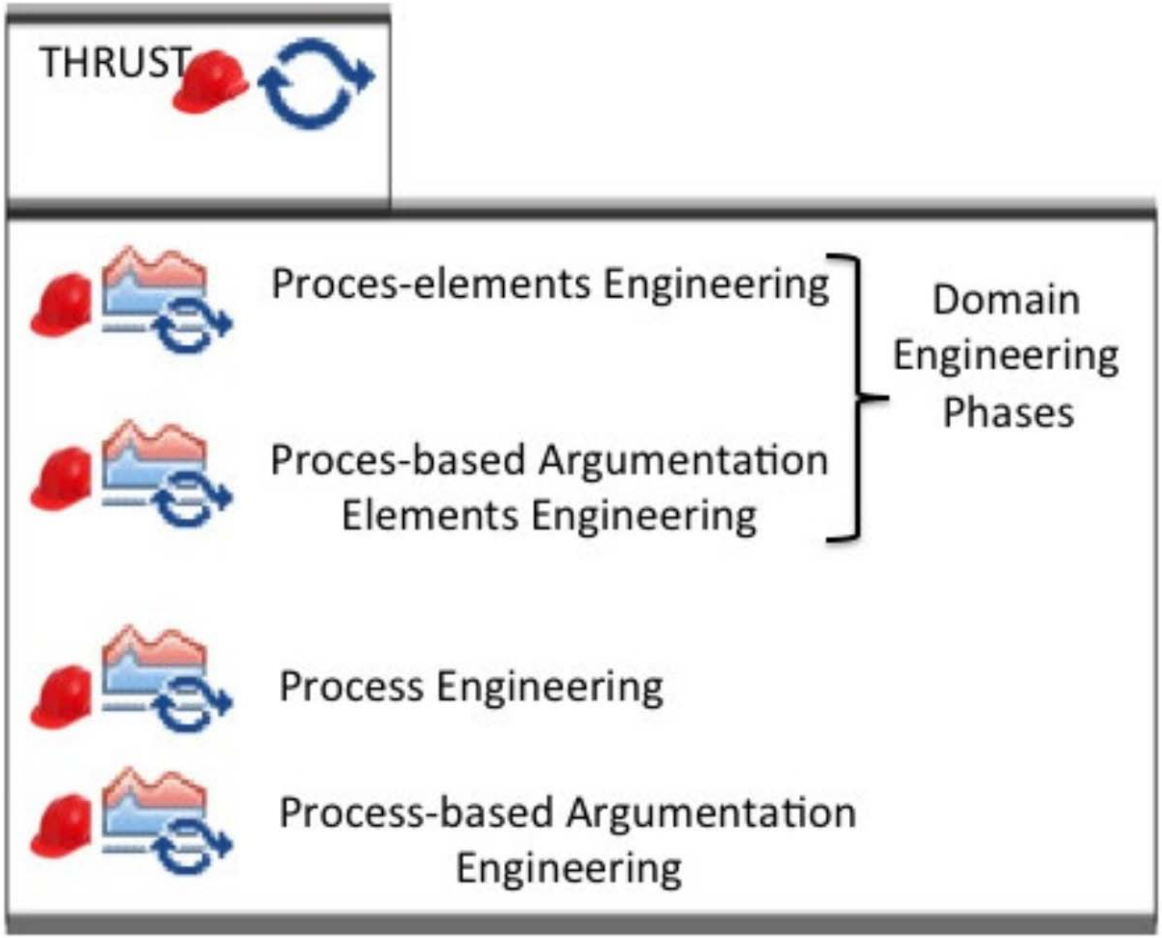
- Textual languages (plain natural language)
- Graphical languages
  - CAE
  - GSN



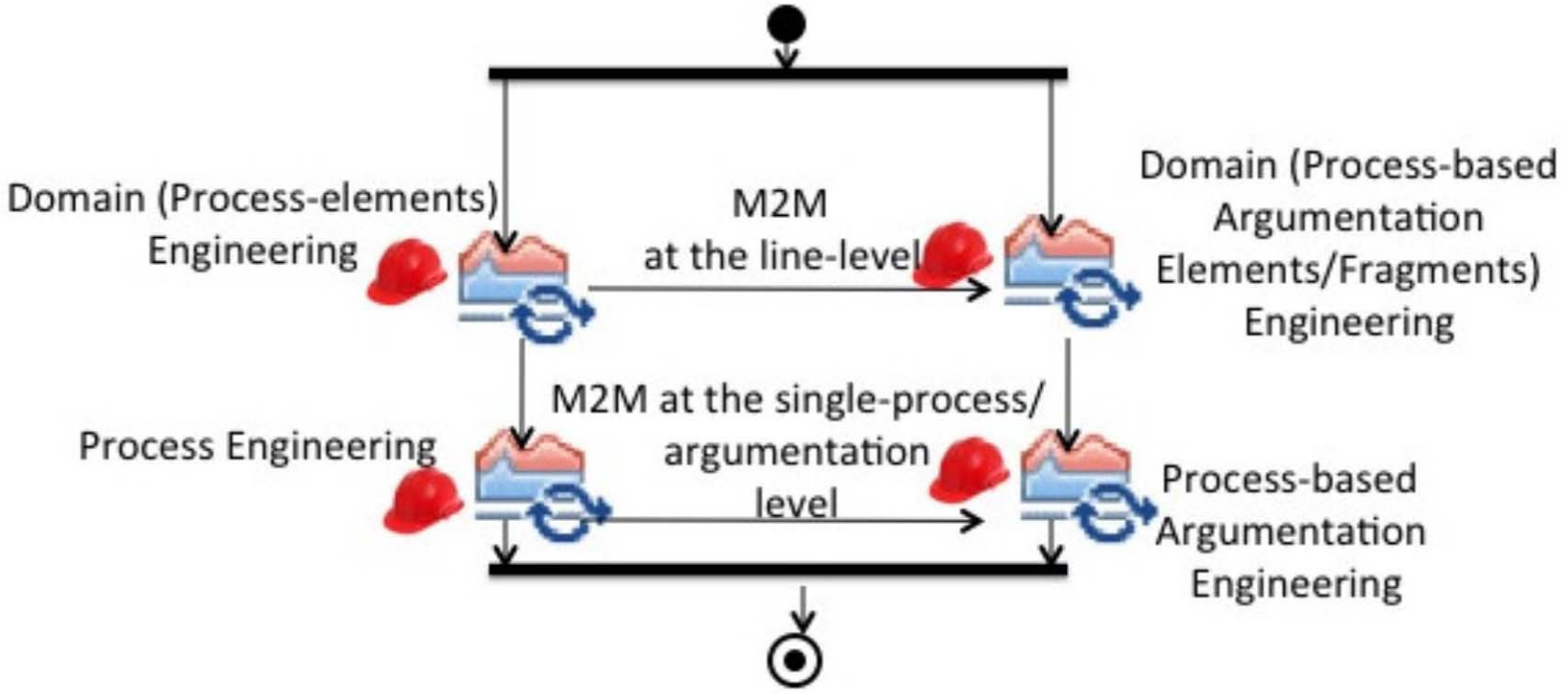
THRUST

- Method for speeding up the creation of process-based artefacts via:
  - Systematic reuse
  - Semi-automatic generation

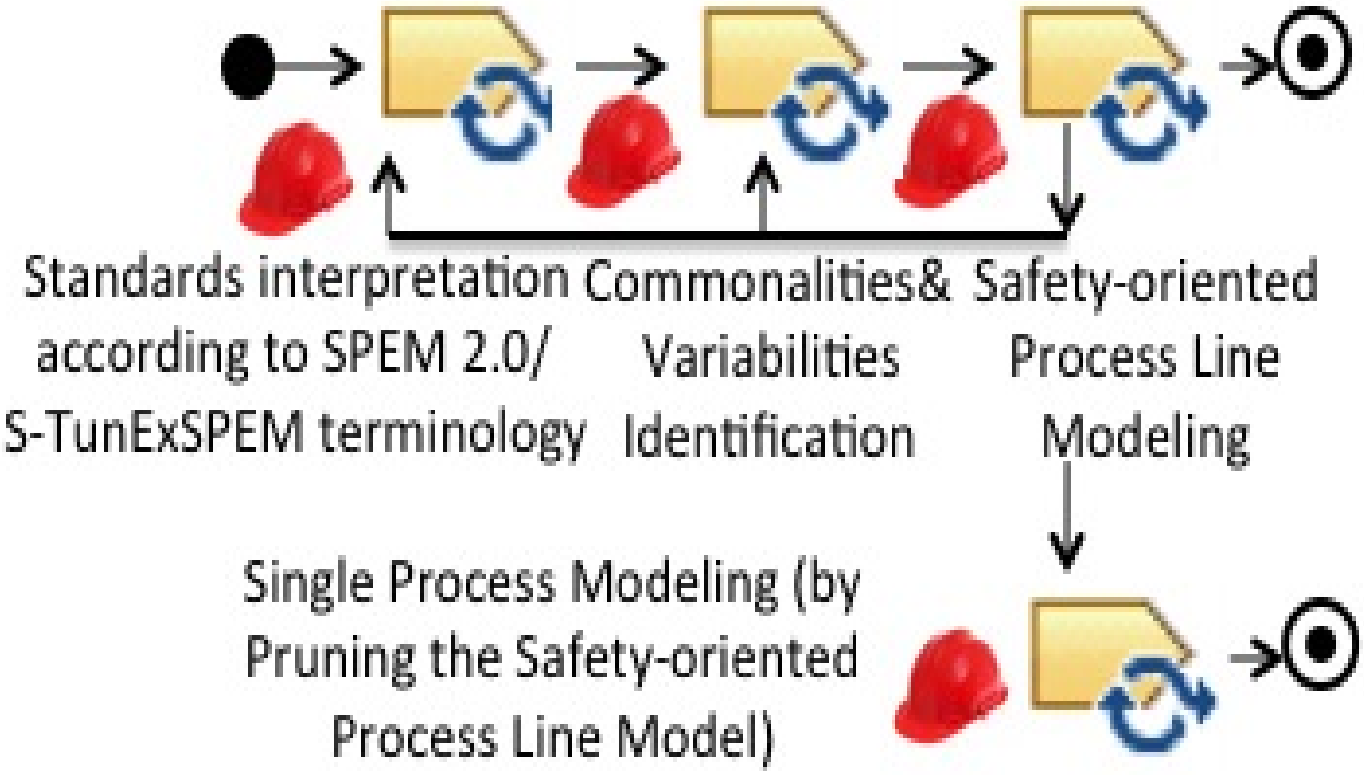
THRUST


THRUST
Proces-elements Engineering
Proces-based Argumentation Elements Engineering
Domain Engineering Phases
Process Engineering
Process-based Argumentation Engineering

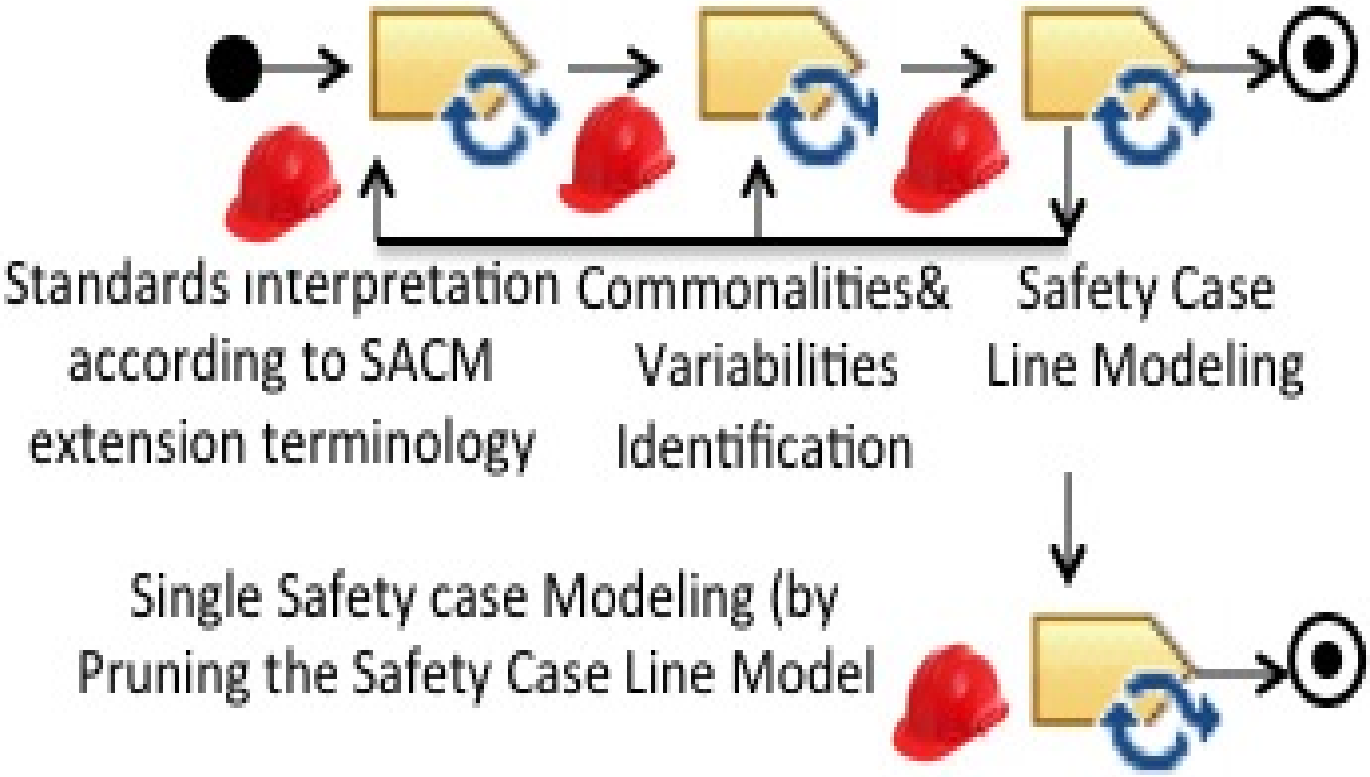
THRUST


Domain (Process-elements) Engineering
M2M at the line-level
Domain (Process-based Argumentation Elements/Fragments) Engineering
M2M at the single-process/ argumentation level
Process Engineering
Process-based Argumentation Engineering

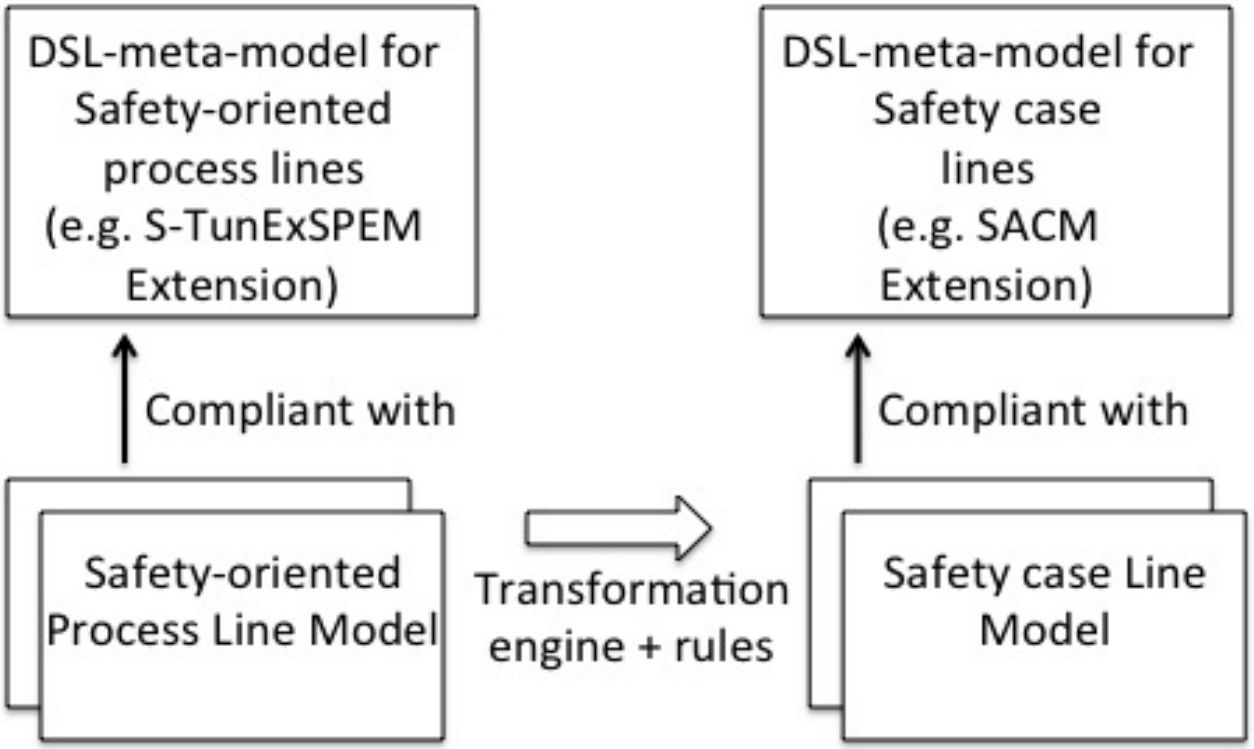
THRUST


Standards interpretation according to SPEM 2.0/ S-TunExSPEM terminology
Commonalities& Variabilities Identification
Safety-oriented Process Line Modeling
Single Process Modeling (by Pruning the Safety-oriented Process Line Model)

THRUST


Standards interpretation according to SACM extension terminology
Commonalities& Variabilities Identification
Safety Case Line Modeling
Single Safety case Modeling (by Pruning the Safety Case Line Model

THRUST

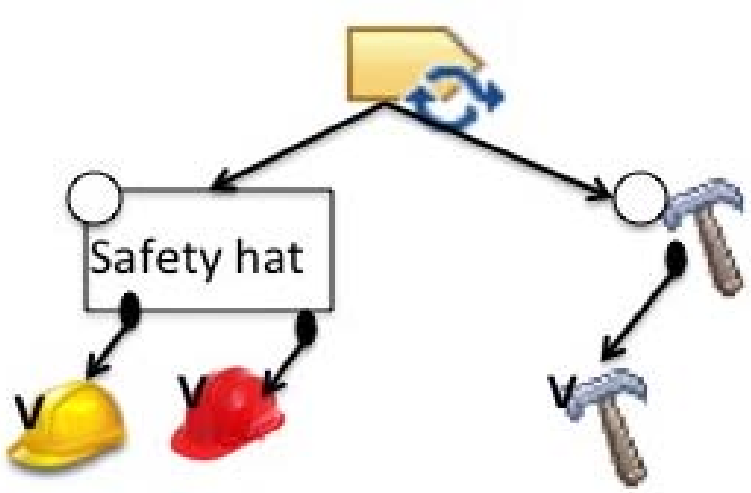

DSL-meta-model for Safety-oriented process lines (e.g. S-TunExSPEM Extension)
DSL-meta-model for Safety case lines (e.g. SACM Extension)
Compliant with
Compliant with
Safety-oriented Process Line Model
Transformation engine + rules
Safety case Line Model

Applying THRUST: an intuition

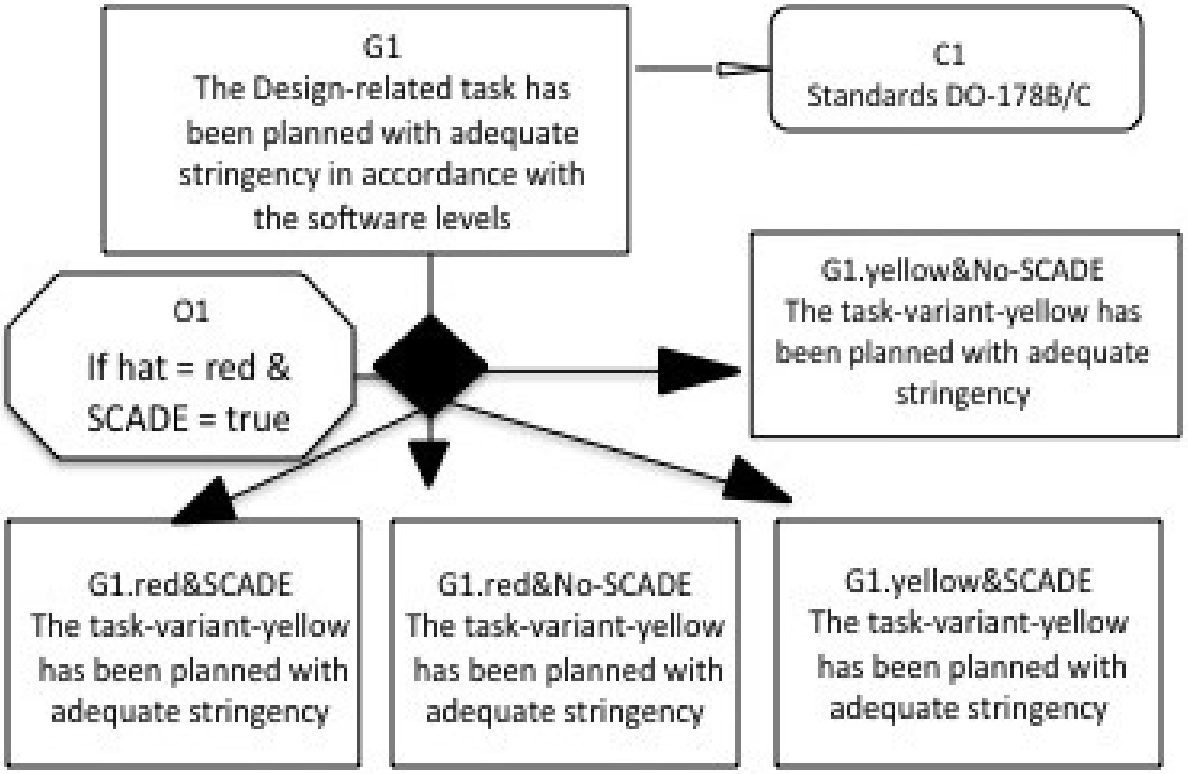
- Within an SDP, a design process could be characterized by:
- *Input:* Software development plan, Software Requirements Data, Software Design Standards.
- *Output:* Design description.
- *Roles:* designers in charge of the design decision related to functional requirements and quality (safety) experts in charge of the design decision related to non- functional requirements.
- *Guidelines:* guidelines, defined in Section 5.2.2 of the standard, contain general as well as safety specific information.
- *Tools* (company-specific decision): Unified Modeling Language (UML) and a model-based development environment (e.g., SCADE Suite).

Remark: This design process may vary due to the software level, whose variation constrains other variabilities, as specified in Annex A

Applying THRUST: an intuition



Applying THRUST: an intuition



Related work

- [Hurtado Alegría et al 2014] authors propose a model-driven-based tailoring method.
- [Rombach et al. 2006] authors propose a research agenda that stresses the relevance of organizing processes for reuse purposes.
- [Marquez 2011] authors perform a comparative study between DO-178A and DO-178B and textually in natural language they describe what varies.

Conclusion and future work

- THRUST: Novel approach for time and cost reduction during the provision of process-related deliverables via reuse and automatic generation
  - Safety-oriented process-line based
  - Safety case line-based (more precisely, process-based argumentation lines)
  - Model-driven-based semi-automatic generation

- Experimental validation on a more complex case-study
- Contribution to provision of adequate meta-models

References

- [Hurtado Alegría et al 2014] Hurtado Alegría, J. A., and M. C. Bastarrica, A. Quispe, S.F. Ochoa, 2014, MDE-based process tailoring strategy. Journal of Software: Evolution and Process, VL-26, IS-4, SN-2047-7481, pp. 386-403.
- [Marquez 2011] Marquez, J. C., 2011, Modification to Legacy Software Developed per DO-178A Level 1 to DO-178B Level A: How to Organize Software Life Cycle Data for Software Approval in Aircraft Certification. In: Latin American Symposium On Dependable Computing (LADC), São José dos Campos.
- [Rombach et al. 2006] Rombach, D., and R. Jeffrey, B. Peterson, M. D'Ambrosa, M. Fusani, H.-W. Jung, S. Ferber, J.Münch, and A. Ocampo, 2006, Process Engineering. In "A Process Research Framework", Eileen Forrester ed., Software Engineering Institute, pp. 20-28.

Thank you for your attention!

Discussion time…