MÄLARDALEN UNIVERSITY
SWEDEN

AMASS

Preventing Omission of Key Evidence Fallacy in Process-based Argumentations

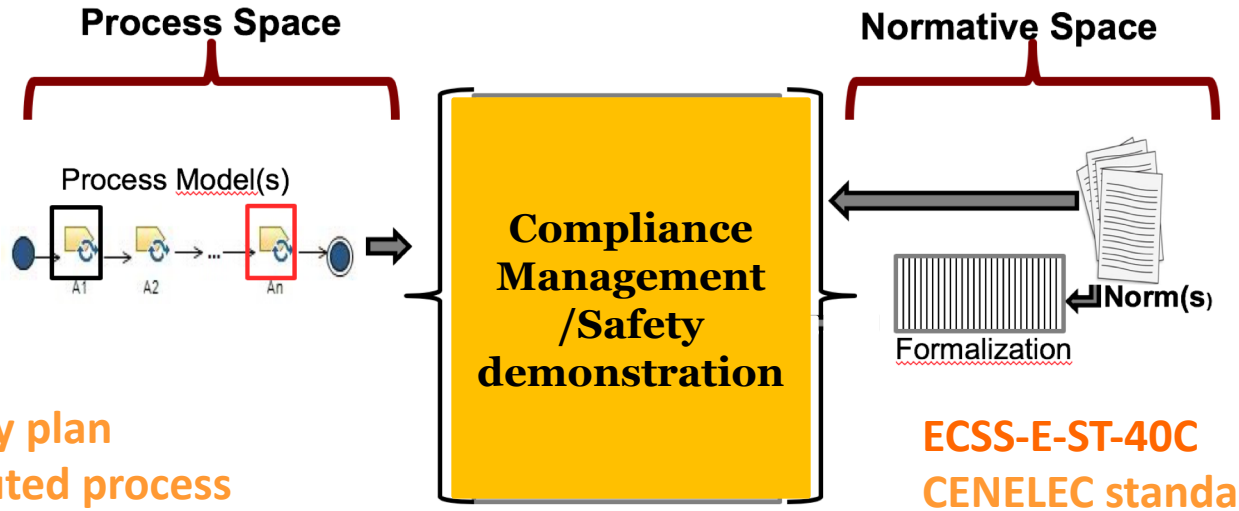
Barbara Gallina
barbara.gallina@mdh.se
Certifiable Evidences & Justification Engineering
Mälardalen University, Västerås, Sweden

F. Ul Muram, **B. Gallina**, Laura Gomez Rodriguez
Preventing Omission of Key Evidence Fallacy in Process-based Argumentations.
11th International Conference on the Quality of Information and Communications Technology (**QUATIC**), IEEE, DOI: 10.1109/QUATIC.2018.00019, Coimbra, Portugal, September, 2018

AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)

7th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY, October 23rd, 2019

Context and Motivation



Safety plan
Executed process

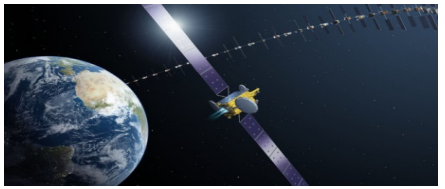
ECSS-E-ST-40C
CENELEC standards EN50128
…

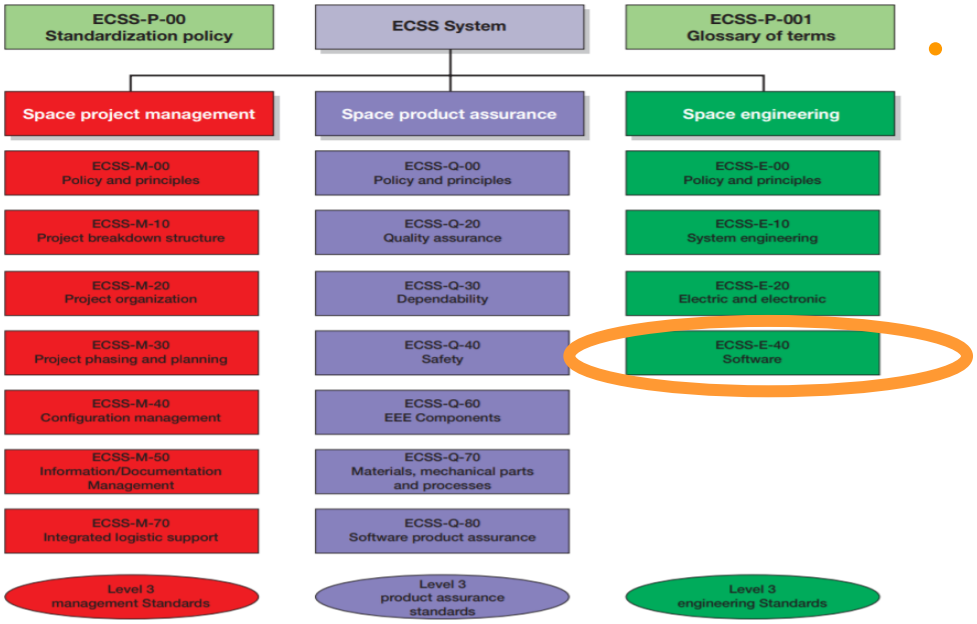
How the management could be facilitated?
How non-fallacious (founded) argumentation can be generated?
How omission of key-evidence could be prevented?

Contents

- Background
  - Standards (ECSS Standards series- ECSS-E-ST-40C; CENELEC series)
  - Process Modelling
  - Argumentation Representation
  - Process-based Argumentation and MDSafeCer
  - Argumentation Fallacies
- A Method for Preventing Fallacies
- Illustrative Example
- Conclusion and Future Work

ECSS-Standards Series





- ECSS-E-ST-40C consists of a set of requirements regarding:
  - activities,
  - guidelines (e.g. coding practices)
  - expected output/work products

Note: Roles are also mentioned but no specific requirement is stated regarding the expected qualifications

M. Jones, E. Gomez, A. Mantineo, and U. Mortensen. Introducing ECSS software-engineering standards within ESA, ESA bulletin, 132 (2002)

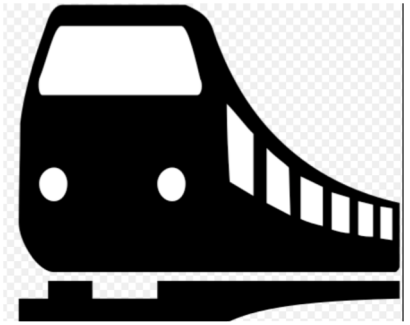
ECSS-Standards Series-ECSS-E-ST-40C

- Section 5.5 (Software Design and Implementation Engineering Process) consists of three phases
  - design of software items,
  - coding and testing,
  - integration

  each of which contains various activities.

  Each activity consists of one or more tasks

CENELEC-Standards Series-EN 50128



- In addition to requirements related to:
  - Reference process models
  - Work breakdown structure
  - Guidelines
  - Workproducts
  - ..

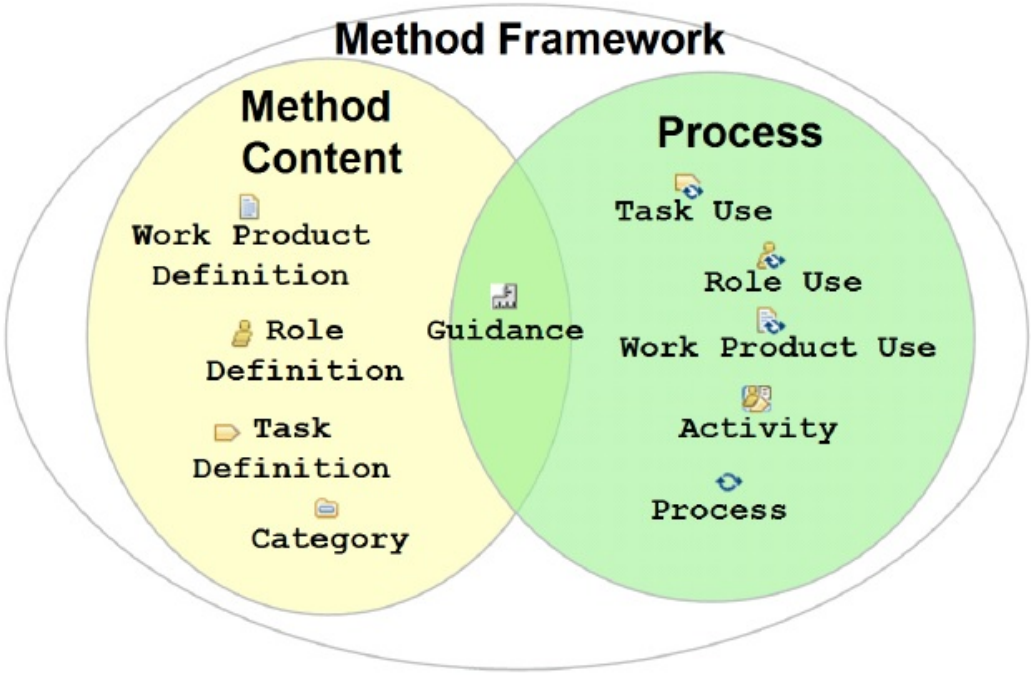
  It also provides requirements regarding roles

  A Designer, for instance, shall be competent in:
  - engineering appropriate to the application area
  - safety design principles
  - design analysis & design test
  - ...

Process Engineering - Metamodel

SPEM (Software & Systems Process Engineering Metamodel)

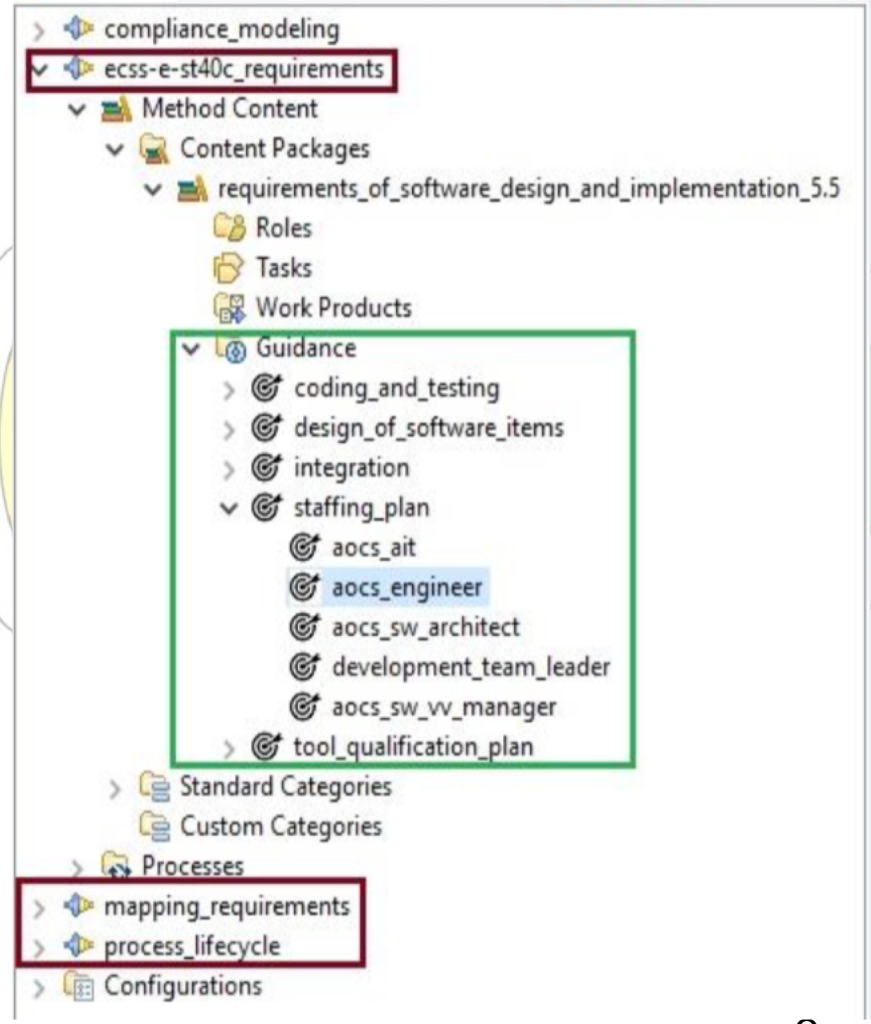
UMA (Unified Method Architecture) Metamodel



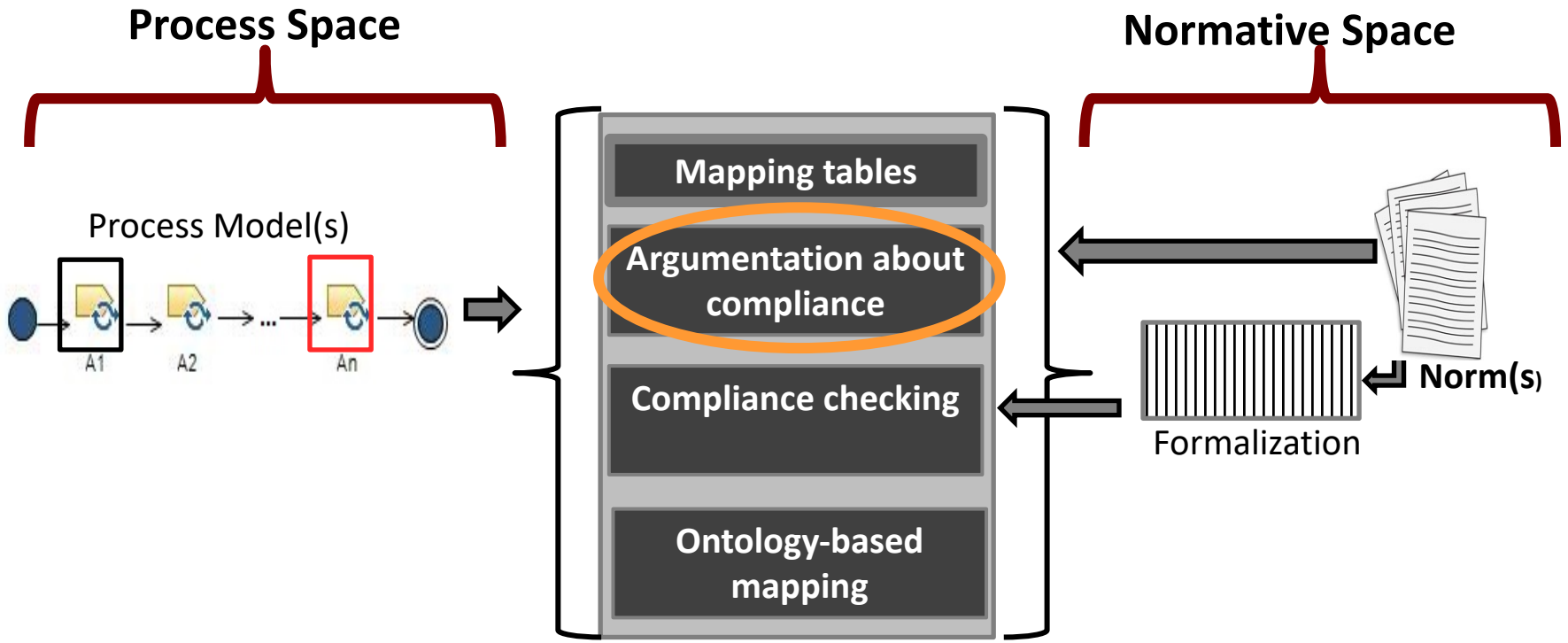
Process Engineering - Metamodel

SPEM (Software & Systems Process Engineering Metamodel)

UMA (Unified Method Architecture) Metamodel



Compliance management



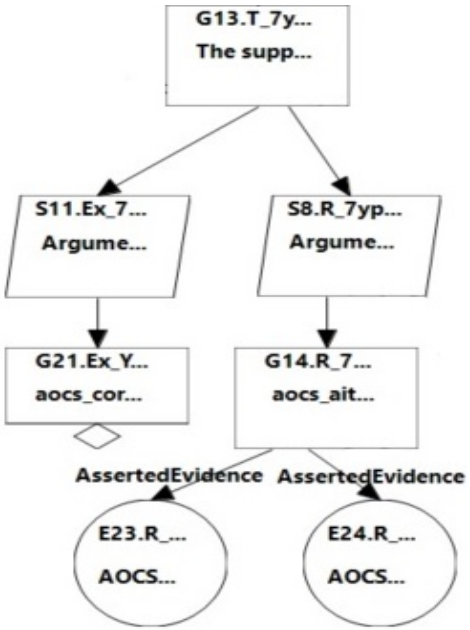
Argumentation Representation

OBJECT MANAGEMENT GROUP®

SACM
(Structured Assurance Case Metamodel)

OpenCert

CACM
(Common Assurance and Certification Metamodel)

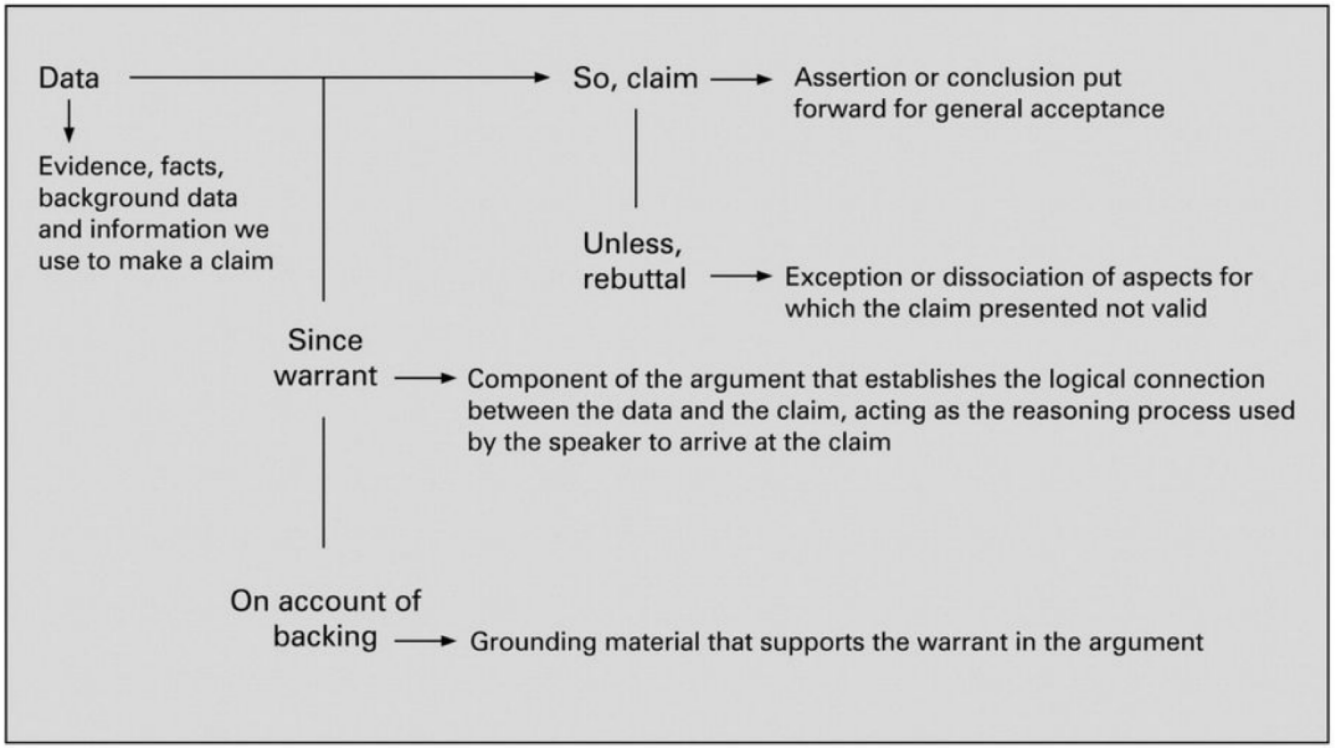


AMASS-partners contributed to the evolution of SACM, specifically version SACM2.1 beta, published March 2019

Argumentation Representation

OBJECT MANAGEMENT GROUP®

SACM
(Structured Assurance Case Metamodel)

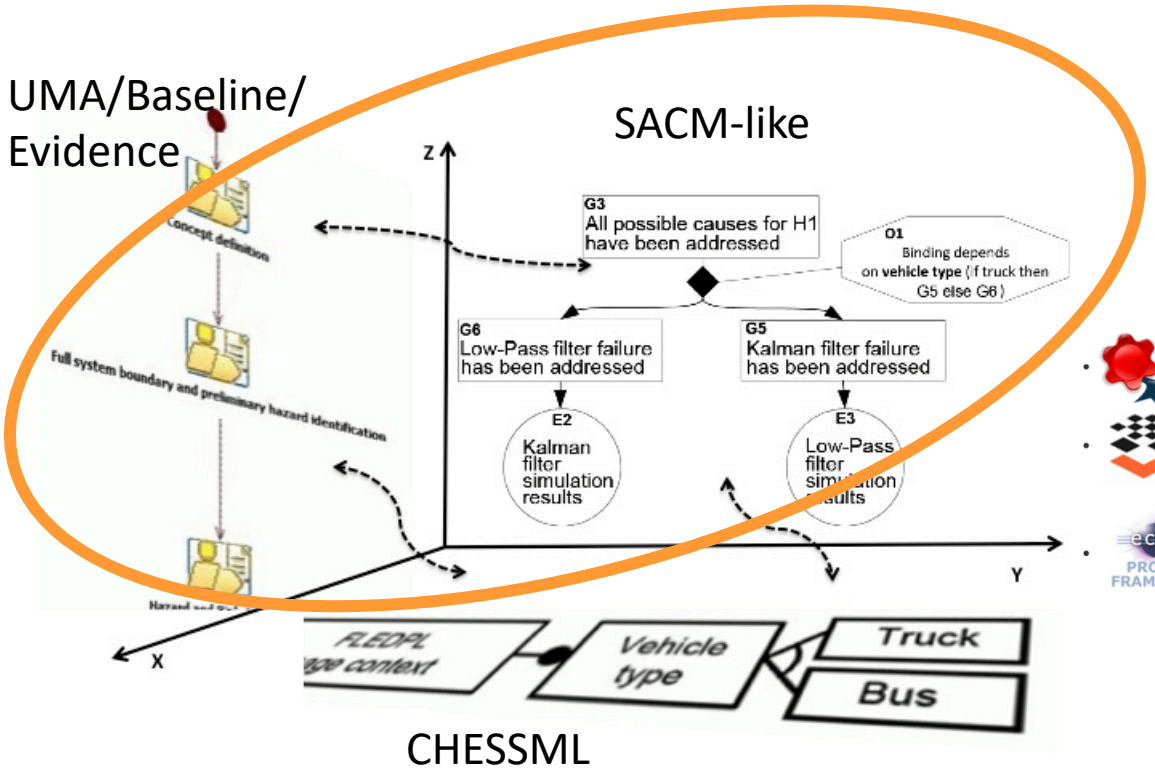


https://slideplayer.com/slide/12972736/

AMASS-partners contributed to the evolution of SACM, specifically version SACM2.1 beta, published March 2019

CACM in context: the AMASS platform

- CACM consists of a combination of metamodels



OpenCert

PolarSys CHESS

eclipse PROCESS FRAMEWORK

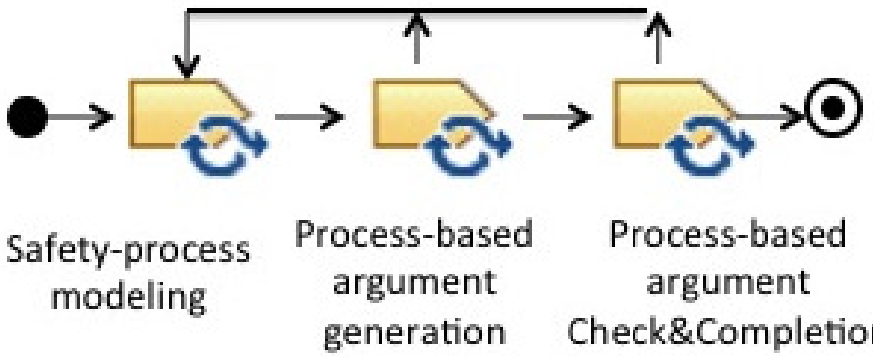
+ BVR Tool

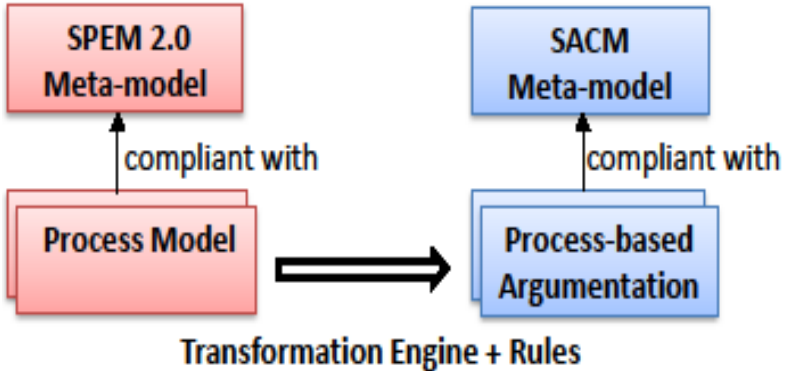
https://www.polarsys.org/**opencert**/

Gallina 2015
(PLEASE Workshop)

Process-based Argumentation and MDSafeCer

- Process-based argumentations (at planning phase) argue about different phases or activities in process planning and provide the convincing evidence that each phase/activity was planned
- MDSafeCer **[Gallina, 2014]** method enables the generation of arguments from process models





B. Gallina. 2014. A Model-driven Safety Certification Method for Process Compliance. In 2nd International Workshop on Assurance Cases for Software-intensive Systems, joint event of ISSRE 2014. IEEE, 204–209.

Argumentation Fallacies

- An **argumentation fallacy** is a mistake or flaw in the reasoning of an argument
- Different types of fallacies have been identified and a taxonomy of common fallacies in safety arguments is available **[Greenwell et al., 2006]**
- **Sufficiency fallacies** are those in which arguments can fail to provide sufficient evidence to support the claims
- **Omission of key evidence** occurs when **no or less** evidence is provided to support the claim and **no valid reasons** are given for its omission

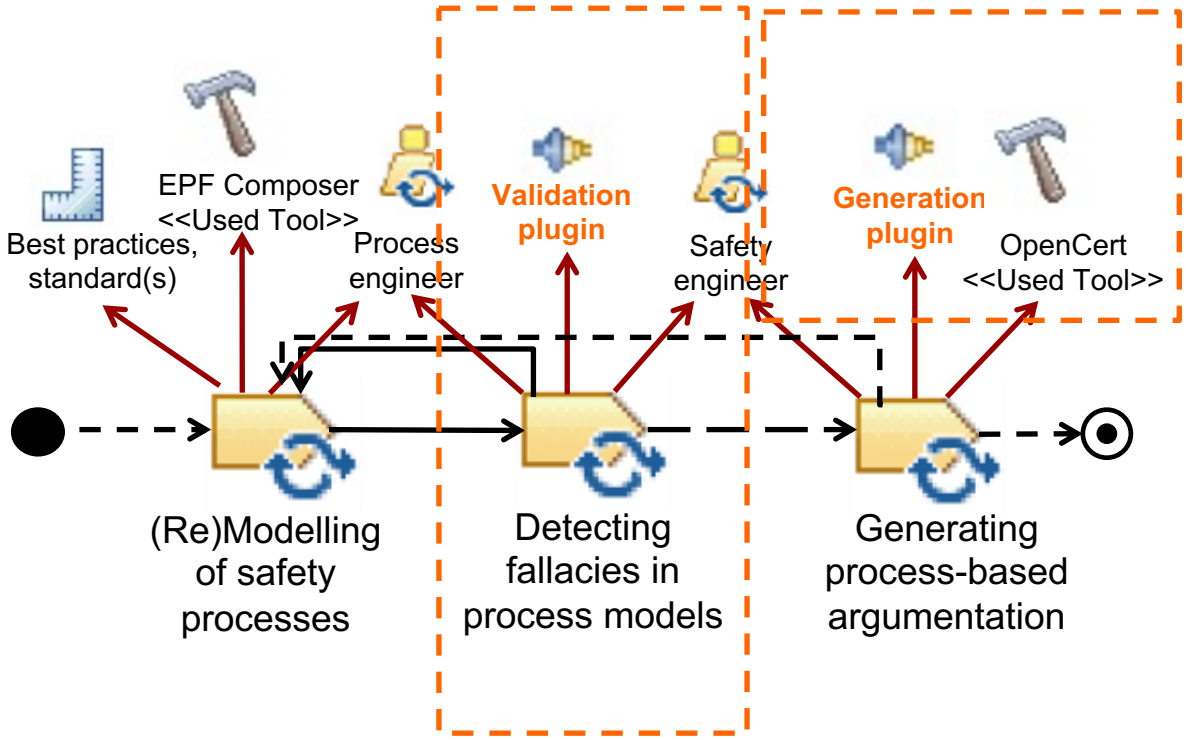
W. S. Greenwell, J. C. Knight, C. M. Holloway, and J. J. Pease, "A Taxonomy of Fallacies in System Safety Arguments," in *24th International System Safety Conference (ISSC), New Mexico, July 31-Aug 4*, 2006.

Contents

- Background
- A Method for Preventing Fallacies
- Illustrative Example
- Conclusion and Future Work

A Method for Preventing Fallacies

- Preventing the omission of key evidence fallacies approach consists of three steps



Generating Process-based Argumentation

Mapping Concepts

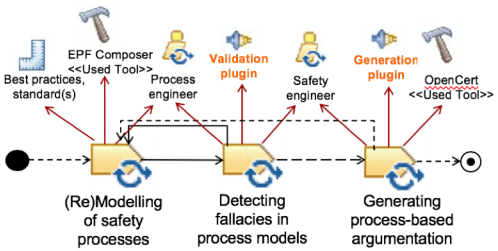
SPEM/UMA	SACM	Diagram
ProcessComponent/DeliveryProcess	Case	
Process purpose (**Standard**)	InformationElementCitation Property type = "**context**"	Context
Capability Pattern, Phase, Activity, TaskUse	Claim	Goal
A set of Phases, Activities, RoleUse, WorkProductUse, Guideline and ToolMentor	ArgumentReasoning	Strategy
Requirements for competency of RoleUse, Tool Qualification	Sub-Claim	Sub-Goal
Evidences associated to WorkProductUse, RoleUse, Guideline and ToolMentor	InformationElementCitation Property type ="**solution**"	Solution
Relationship between Phases, Activities, TaskUses	AssertedInference	SolvedBy
Relationship between competency of RoleUse and certification	AssertedEvidence	SolvedBy
Id, name and description	Id, name and description	Id, name and description

Illustrative Example

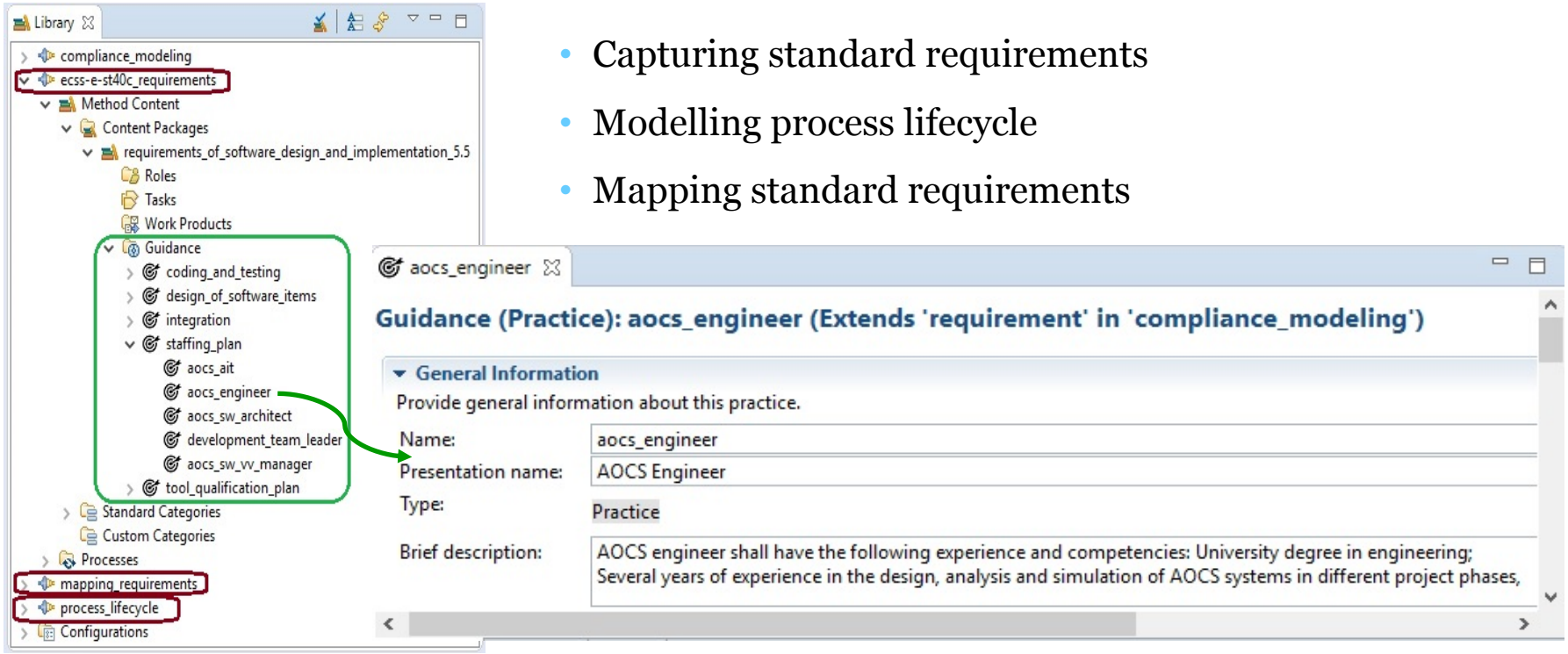
- Software engineering process for AOCS (level B)
  - AOCS- Attitude and Orbit Control Subsystem
    - Attitude control manages the orientation of the satellite
    - Orbit control regulates the positioning of the satellite in orbit
- ECSS-E-ST-40C standard –subset (clause 5.5)

Note: Key competencies required for roles are adapted from EN 50128

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems (AMASS), "Case studies description and business impact D1.1," https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D1.1_Case-studies-description-and-business-impact_AMASS_Final.pdf,

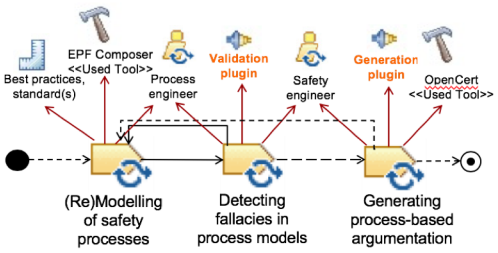


Modelling requirements and processes

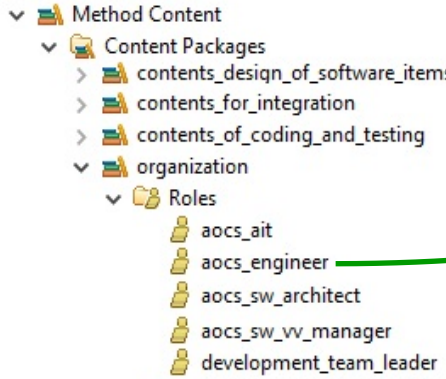


- Capturing standard requirements
- Modelling process lifecycle
- Mapping standard requirements

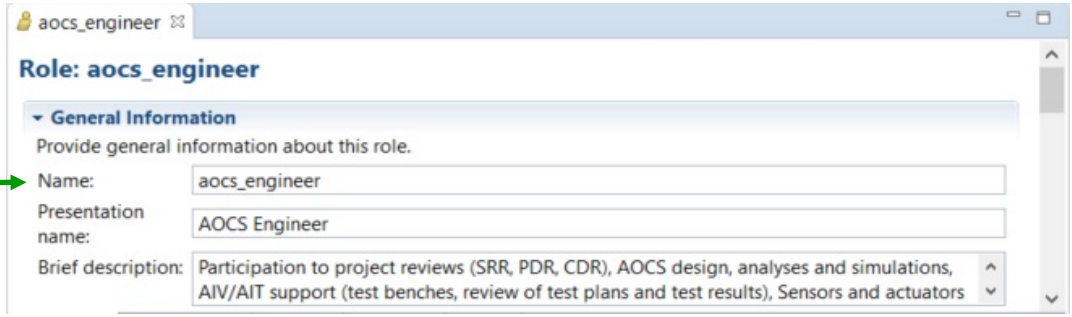
AMASS, Deliverable D6.8, Section 3.4.1. Link: https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D6.8_Methodological-guide-for-cross-intra-domain-reuse-%28b%29_AMASS_Final.pdf

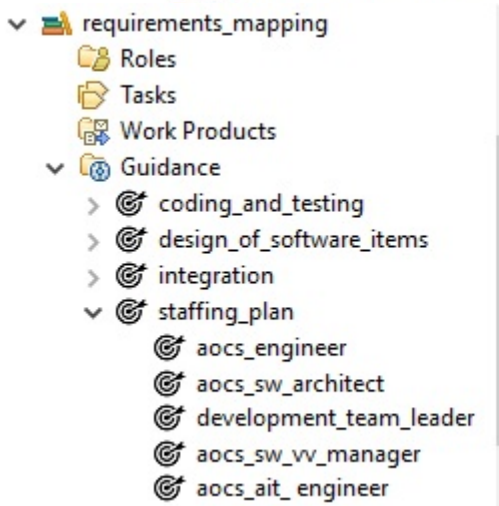


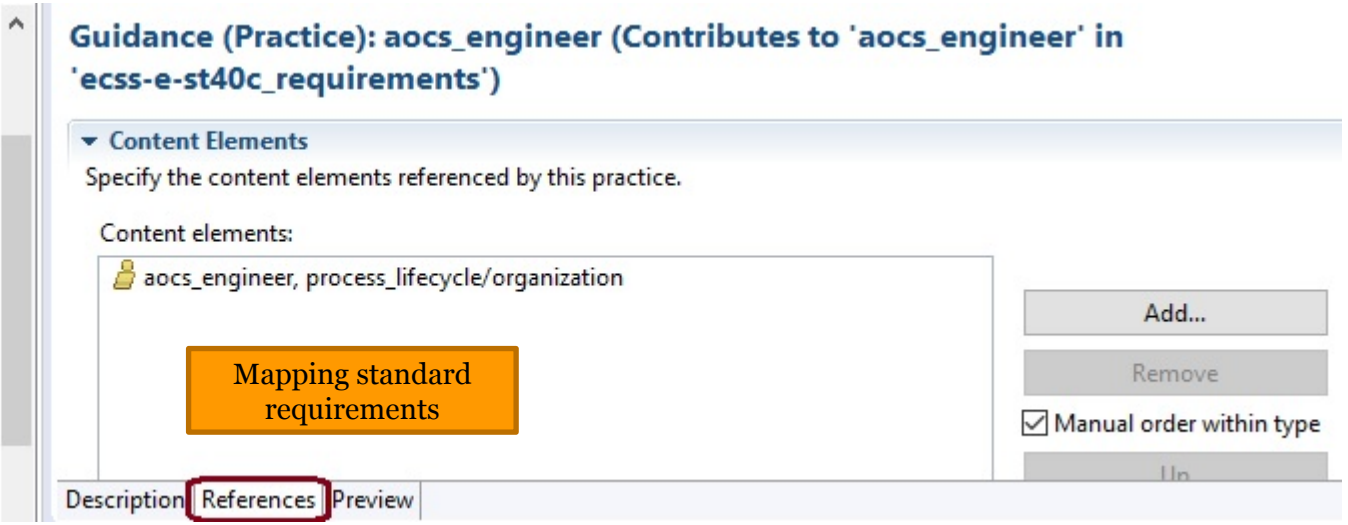
Modelling of Safety Processes



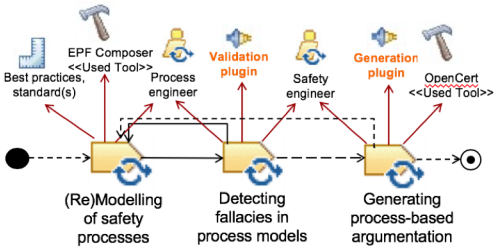
Modelling process lifecycle







Mapping standard requirements



Omission detection

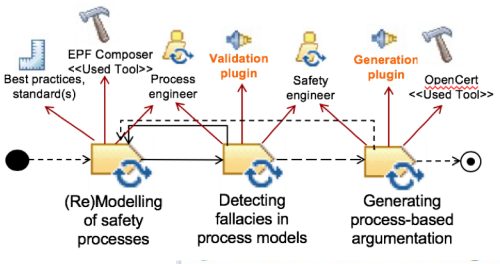
Library

- compliance_modeling
- ecss-e-st40c_requirements
- mapping_requirements
- process_lifecycle
- Method Content
  - Content Packages
  - Standard Categories
  - Custom Categories
- Processes
  - Capability Patterns
  - Delivery Processes
    - ECSS-E-ST-40_Software_D
    - ECSS-E-ST-40_Software_D
- Configurations

Configuration

ECSS-E-ST-40_Software_Design_and_Implementation_Planing

Presentation Name	Index	Predecessors	Model In...	Type	Planned
ECSS-E-ST-40_Planing_Phase_Software_Design_and_Implementation	0			Delivery Process	☑
ECSS-E-40_Planning_Process	1			Capability Pattern	☑
design of software items	2			Phase	☑
coding and testing	29			Phase	☑
Develop and Document Software Units	30			Activity	☑
Development and Documentation of Software Units	31			Task Descriptor	☐
Test Software Units	32			Activity	☑
integration	36			Phase	☑



Result after Detecting Fallacies

and_Implementation_Planing

Presentation Name	Model Info	Team	Type	Planned	Multipl...	Optional
ECSS-E-ST-40_Planing_Phase_Software_Design_and_Implementation			Delivery Process	☑	☐	☐
ECSS-E-40_Planning_Process			Capability Pattern	☑	☐	☐
design of software items			Phase	☑	☐	☐
coding and testing			Phase	☑	☐	☐
Develop and Document Software Units			Activity	☑	☐	☐
AOCS AIT Engineer			Role Descriptor	☑	☐	☐
AOCS Engineer			Role Descriptor	☑	☐	☐
AOCS SW Architect			Role Descriptor	☑	☐	☐
AOCS SW V&V Manager			Role Descriptor	☑	☐	☐
Development Team Leader			Role Descriptor	☑	☐	☐
Test Software Units			Activity	☑	☐	☐
integration			Phase	☑	☐	☐

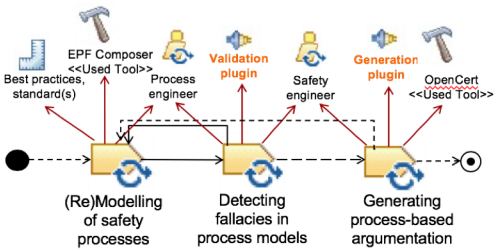
Description | Work Breakdown Structure | Team Allocation | Work Product Usage | Consolidated View

Properties | Problems | Console

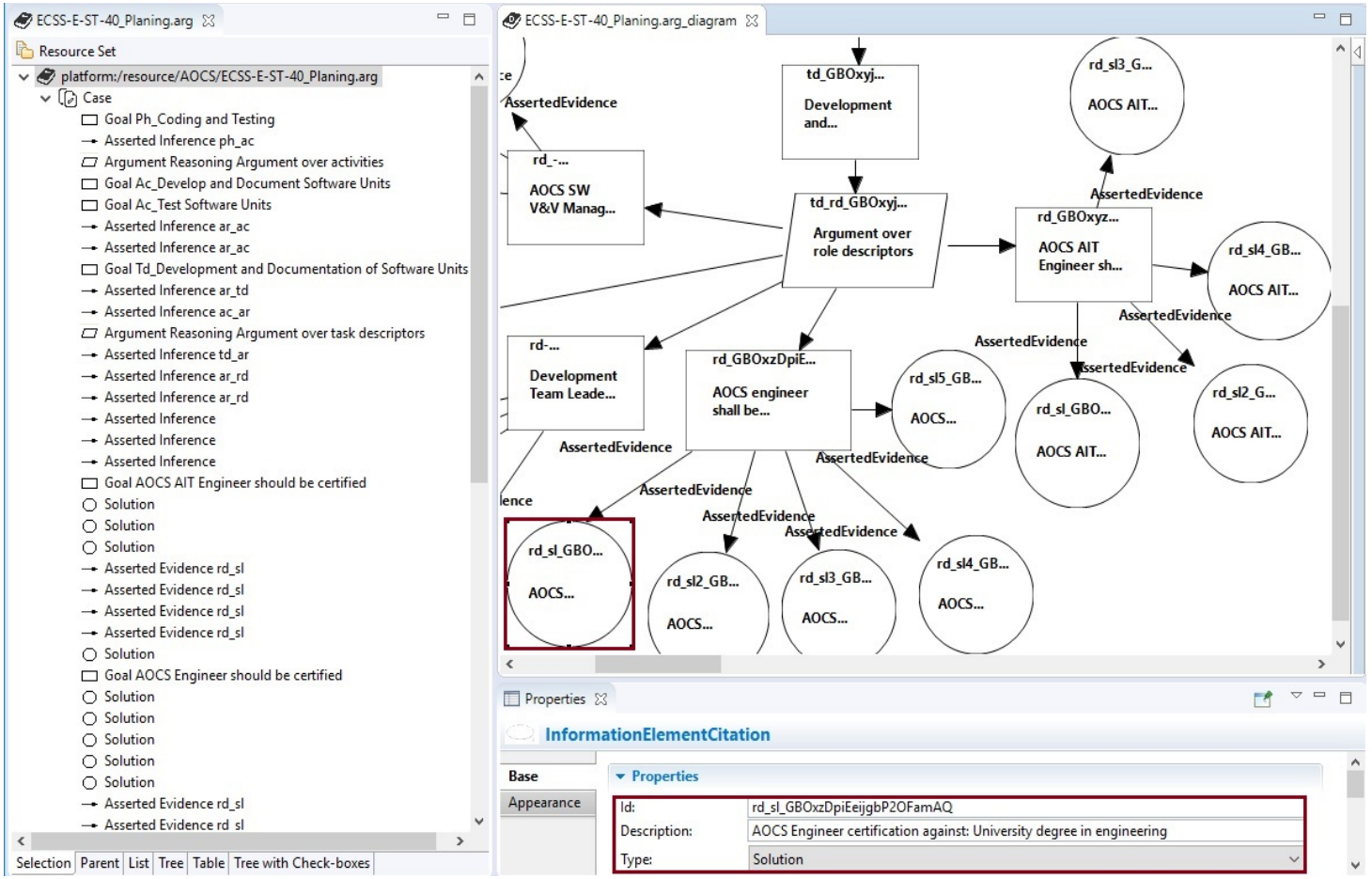
Fallacy Detection Console

```
Certification against following ROLES are INSUFFICIENT:
   1. AOCS ENGINEER
        DETECTED FALLACIES: Certifications against following competencies/requirements are omitted:
        - University degree in engineering
        - Several years of experience in the design, analysis and simulation of AOCS systems in different project phases, Exce
        - Working experience with Linux System, Matlab and Satsim.
        RECOMMENDATION: Add skill certifications against above omitted evidence for the AOCS Engineer role
        to achieve sufficiency or provide rationale for its omission.
   2. DEVELOPMENT TEAM LEADER
        DETECTED FALLACIES: Certifications against following competencies/requirements are omitted:
        - Management of Electra AOCS SW development team
        - Working with Matlab/Simulink
        - Knowledge of design analysis and design test methodologies
        - Good analytical and problem-solving skills.
        RECOMMENDATION: Add skill certifications against above omitted evidence for the Development Team Leader role
        to achieve sufficiency or provide rationale for its omission.

Certification against following ROLES are SUFFICIENT:
   3. AOCS AIT ENGINEER
   4. AOCS SW ARCHITECT
   5. AOCS SW V&V MANAGER
```



Generated Argumentation Model and Diagram



Conclusion and future work

- A tool-supported method to prevent omission of key evidence fallacy in the process-based argumentations
  - Recommendations to solve the fallacious processes are included

- Support for other sufficiency fallacies
- Expand the fallacy detection to other types of fallacies
- Conduct more comprehensive case studies

Thank you for your attention!

Discussion time…

MÄLARDALEN UNIVERSITY
SWEDEN

Publications

-focus on process compliance-

International Peer-reviewed Journals

B. Gallina. Quantitative Evaluation of Tailoring within SPICE-compliant Security-informed Safety-oriented Process Lines. Journal of Software: Evolution and Process, EuroSPI Special Issue, August, 2019, DOI:10.1002/smr.2212.

International Peer-reviewed Conferences

F. Ul Muram, B. Gallina, S. Kanwal. A Tool-supported Model-based Method for Facilitating the EN50129-compliant Safety Approval Process. Third International Conference Reliability, Safety and Security of Railway Systems: Modelling, Analysis, Verification and Certification (RSS-Rail), Lille, France, June 4-6, 2019.

J. P. Castellanos Ardila and B. Gallina and F. Ul Muram. Transforming SPEM 2.0-compatible Process Models into Models Checkable for Compliance. 18th International SPICE Conference (SPICE), Communications in Computer and Information Science book series (CCIS, volume 918), pp. 233-247, DOI: 10.1007/978-3-030-00623-5_16, ISBN: 978-3-030-00622-8, Thessaloniki, Greece, October 9-10, 2018.

M. A. Javed and B. Gallina. Safety-oriented Process Line Engineering via Seamless Integration between EPF Composer and BVR Tool. In 22nd International Systems and Software Product Line Conference (SPLC), Sept 10-14, Gothenburg, Sweden, ACM Digital Library, DOI: 10.1145/3236405.3236406, 2018.

B. Gallina and S. Iyer. Towards Quantitative Evaluation of Reuse within Safety-oriented Process Lines. 25th European & Asian Systems, Software & Service Process Improvement & Innovation (EuroSPI), Communications in Computer and Information Science, Springer, pp. 162-174, DOI: 10.1007/978-3-319-97925-0_40, Bilbao, Spain, 5.-7. Sept. 2018.

MÄLARDALEN UNIVERSITY
SWEDEN

Publications

-focus on process compliance-

International Peer-reviewed Conferences

J. P. Castellanos Ardila and B. Gallina and F. Ul Muram. Enabling Compliance Checking against Safety Standards from SPEM 2.0 Process Models. 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Prague, Czech Republic, 29-31 August, 2018.

T. Varkoi, T. Mäkinen, B. Gallina, F. Cameron and R. Nevalainen. Towards Systematic Compliance Evaluation Using Safety-oriented Process Lines and Evidence Mapping. 24th European & Asian Systems, Software & Service Process Improvement & Innovation, Ostrava, Czech Republic, 5.-8. Sept. 2017.

J. P. Castellanos Ardila and B. Gallina. Towards Increased Efficiency and Confidence in Process Compliance. 24th European & Asian Systems, Software & Service Process Improvement & Innovation, Ostrava, Czech Republic, 5.-8. Sept. 2017.

B. Gallina, A. Andrews. Deriving Verification-related Means of Compliance for a Model-based Testing Process. IEEE 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, US, September 25-29, 2016.

S. Alajarami, A. Romanovsky, and B. Gallina. Software Development in the Post-PC Era: Towards Software Development as a Service. Proceedings of the 17th International Conference on Product-Focused Software Process Improvement (PROFES), Springer, LNCS, Bolzano, Italy, November 24-26, 2016.

S. Alajrami, B. Gallina, I. Sljivo, A. Romanovsky, P. Isberg. Towards Cloud-Based Enactment of Safety-Related Processes. Proceedings of the 35th International Conference on Computer Safety, Reliability and Security (SafeComp), Trondheim, Norway, September 20-23, 2016.

MÄLARDALEN UNIVERSITY
SWEDEN

Publications

-focus on process compliance-

International Peer-reviewed Conferences

B. Gallina, E. Gomez-Martınez, and C. Benac Earle. Deriving Safety Case Fragments for Assessing MBASafe's Compliance with EN 50128. 16th International SPICE Conference on Process Improvement and Capability dEtermination (SPICE), Dublin, Ireland, Vol. 609, Communications in Computer and Information Science series, pp. 3-16, ISBN 978-3-319-38979-0, Springer, 2016.

B. Gallina, Z. Szatmari. Ontology-based Identification of Commonalities and Variabilities among Safety Processes. Proceedings of the 16th International Conference on Product-Focused Software Process Improvement (PROFES), Springer, LNCS 9459, pp. 182-189, ISBN 978-3-319-26843-9, Bolzano, Italy, December 2-4, 2015.

B. Gallina, L. Fabre. Benefits of Security-informed Safety-oriented Process Line Engineering. IEEE 34th Digital Avionics Systems Conference (DASC-34), Prague, Czech Republic, September 13-17, ISBN 978-1-4799-8939-3, 2015.

B. Gallina, L. Provenzano. Deriving Reusable Process-based Arguments from Process Models in the Context of Railway Safety Standards. 20th International Conference on Reliable Software Technologies-Industrial Presentation- (Ada-Europe-2015), Madrid, Spain, June, 2015.

MÄLARDALEN UNIVERSITY
SWEDEN

Publications

-focus on process compliance-

International Peer-reviewed Workshops

J. P. Castellanos Ardila, B. Gallina and G. Governatori. Lessons Learned while Formalizing ISO 26262 for Compliance Checking. 2nd Workshop on TeReCom - Technologies for Regulatory Compliance, CEUR Workshop Proceedings, Vol-2309, pp. 5-16, Gröningen, Netherlands, December 12, 2018.

B. Gallina, F. Ul Muram, and J. P. Castellanos Ardila. Compliance of Agilized (Software) Development Processes with Safety. 4th international workshop on agile development of safety-critical software (ASCS), May 21st, Porto, Portugal, 2018, in Proceedings of the 19th International Conference on Agile Software Development: Companion (XP '18). ACM, New York, NY, USA, Article 14, 6 pages. DOI: https://doi.org/10.1145/3234152.3234175.

J. P. Castellanos Ardila and B. Gallina. Formal Contract Logic Based Patterns for Facilitating Compliance Checking against ISO 26262. Proceedings of the 1st Workshop on Technologies for Regulatory Compliance co-located with the 30th International Conference on Legal Knowledge and Information Systems (JURIX 2017), CEUR Workshop Proceedings, Vol-2049, pp. 65-72, Luxembourg, Luxembourg, 13 of December, 2017.

J. P. Castellanos Ardila and B. Gallina. Towards Efficiently Checking Compliance Against Automotive Security and Safety Standards. Proceedings of the 7nd IEEE Workshop on SOftware CERtification (WoSoCER), IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), IEEE Computer Society, pp. 317-324, DOI: 10.1109/ISSREW.2017.33, Toulouse, France, 23 of October, 2017.

B. Gallina. Towards Enabling Reuse in the Context of Safety-critical Product Lines. 5th International Workshop on Product LinE Approaches in Software Engineering (PLEASE), joint event of ICSE, Florence, Italy, May 19th, 2015.

MÄLARDALEN UNIVERSITY
SWEDEN

Publications

-focus on process compliance-

International Peer-reviewed Workshops

I. Ayala, B. Gallina. Towards Tool-based Security-informed Safety Oriented Process Line Engineering. 1st ACM International workshop on Interplay of Security, Safety and System/Software Architecture (ISSA), Copenhagen, Denmark, November 28th, ISBN: 978-1-4503-4781-5, DOI: 10.1145/2993412.3007554, 2016.

B. Gallina. A Model-driven Safety Certification Method for Process Compliance. 2nd IEEE International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), joint event of ISSRE, Naples, Italy, doi: 10.1109/ISSREW.2014.30, pp. 204-209, November 3-6, 2014.

B. Gallina, S. Kashiyarandi, K. Zugsbrati and A. Geven. Enabling Cross-domain Reuse of Tool Qualification Certification Artefacts. Proceedings of the 1st International Workshop on DEvelopment, Verification and VAlidation of cRiTical Systems (DEVVARTS), joint workshop at SafeComp conference, Springer, LNCS 8696, ISBN: 978-3-319-10556-7, pp. 255-266, Florence (Italy), 8 September, 2014.

B. Gallina, S. Kashiyarandi, H. Martin and R. Bramberger. Modeling a Safety- and Automotive-oriented Process Line to Enable Reuse and Flexible Process Derivation. Proceedings of the 8th IEEE International Workshop on Quality-Oriented Reuse of Software (QUORS), joint workshop at COMPSAC conference, IEEE Computer Society, doi: 10.1109/COMPSACW.2014.84, pp. 504-509,Västerås (Sweden), 2014.

B. Gallina, I. Sljivo, and O. Jaradat. Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. Post-proceedings of the 35th IEEE Software Engineering Workshop (SEW-35), IEEE Computer Society, ISBN 978-1-4673-5574-2, Heraclion, Crete (Greece), 2012.