MÄLARDALEN UNIVERSITY
SWEDEN

AMASS

Assurance and Certification of Cyber-Physical Systems within the AMASS platform

Barbara Gallina

Certifiable Evidences & Justification Engineering

School of Innovation, Design and Engineering,

Mälardalen University, Västerås, Sweden

barbara.gallina@mdh.se

Work supported by the **EU and VINNOVA** via the **ECSEL JU project AMASS**

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

77th Meeting IFIP-WG 10.4, Reggio Calabria, Italy, 29th January 2020

Workshop on Security-Oriented Situational Awareness for Safety-Critical Infrastructures

Talk outline

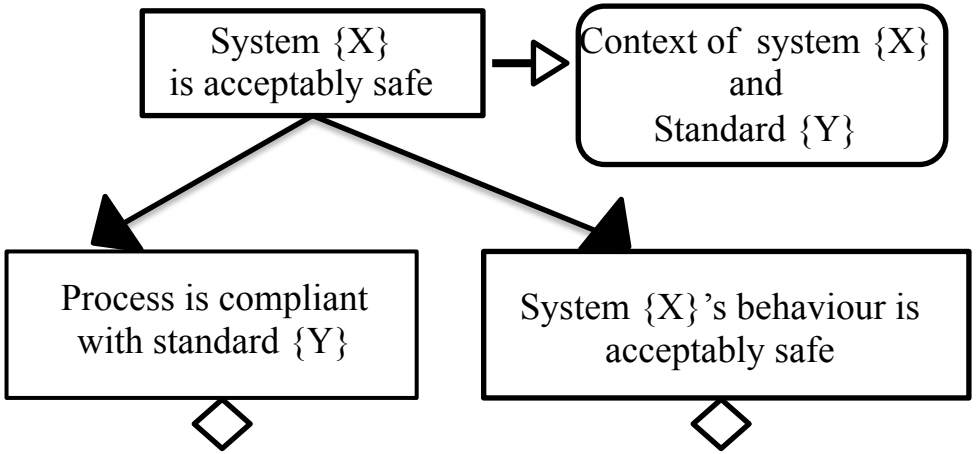
- My research/education focus
- Assurance & Certification
- AMASS project overview
- AMASS platform core
- AMASS platform and ecosystem
- AMASS platform in action
- AMASS platform future development

Research/education focus

- Research
  - Systematic reuse of (Relaxed) ACID-based transactional artifacts
  - Dependability modelling and analysis of high integrity (socio-technical) systems
  - ISO 26262-compliant safety case building
  - Systematic reuse of product-related certification artifacts
  - Systematic reuse of process-related certification artifacts
  - Compliance management
- Education
  - DVA437-Safety-critical systems engineering
  - DVA433-Functional safety, PROMPT initiative
  - DVA467- Quality assurance - Certification of safety-critical (software) systems, PROMPT initiative
  - Contribution to the discussion related to the Manifesto on Software Process Education, Training and Professionalism
    - Constructive Alignment extension for safety critical systems

Assurance and 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.



AMASS project overview -Goals

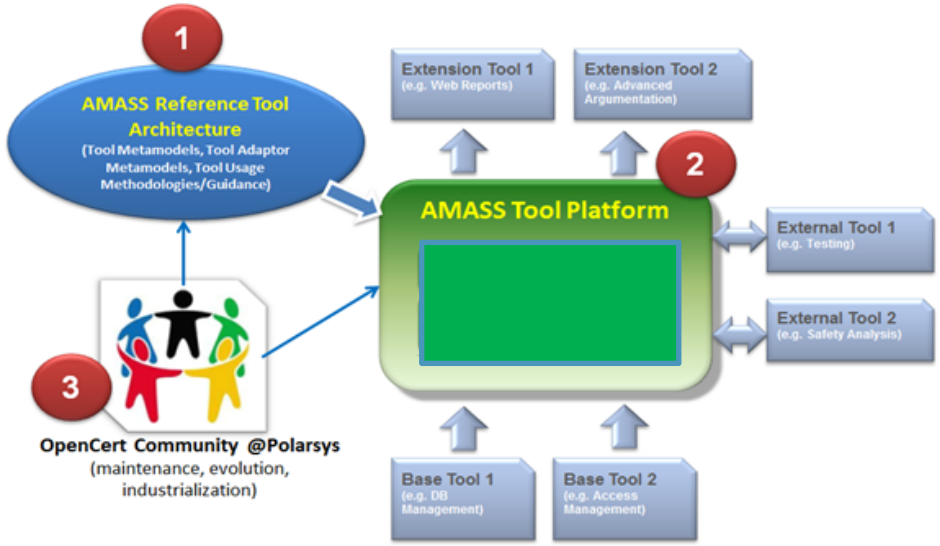
Project Goals

Develop an holistic approach and tool support for

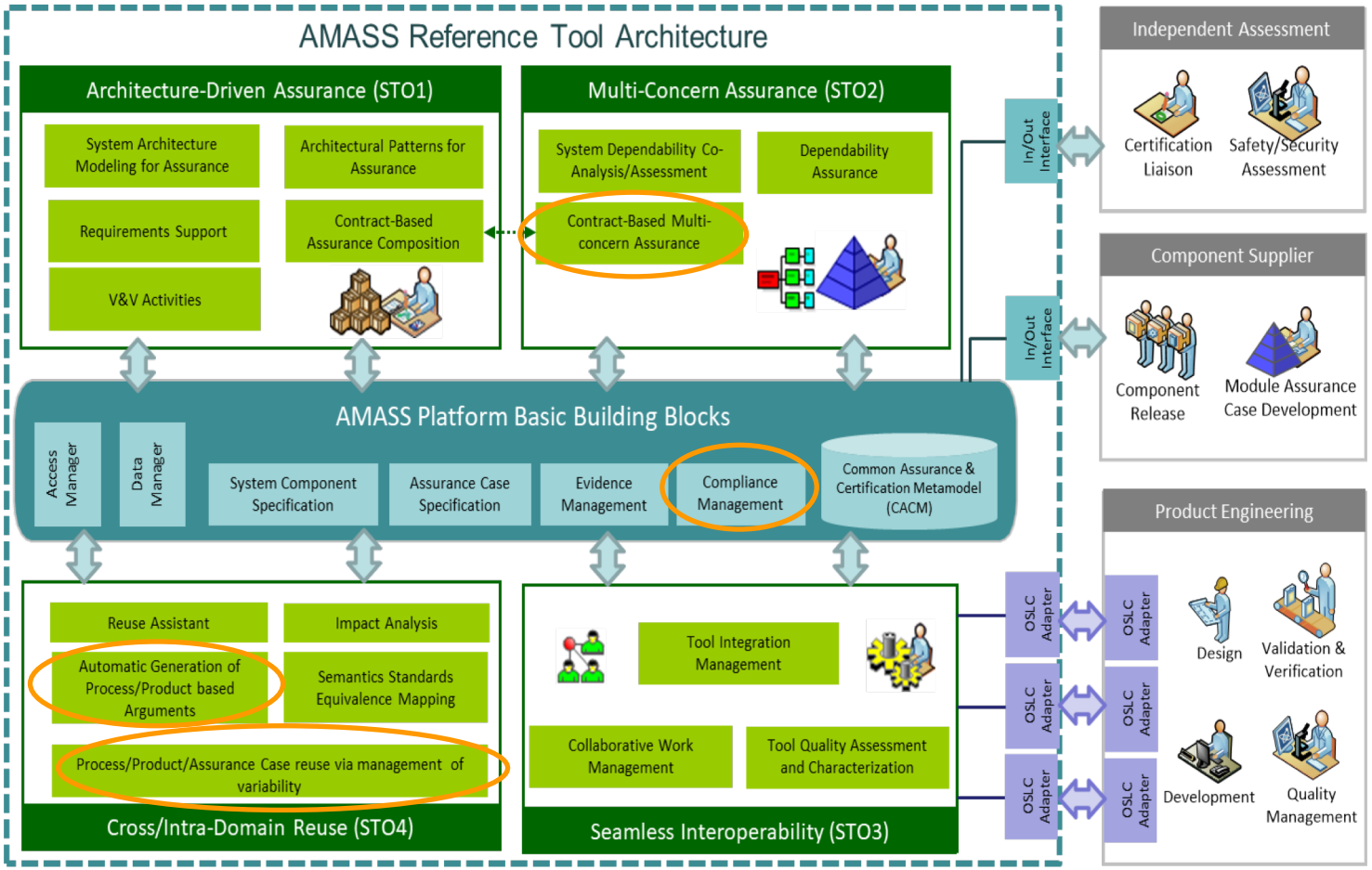
Architecture-driven, Multi-concern, Seamless, Reuse-Oriented Assurance & Certification

G1: Gain for Design Efficiency
G2: Reuse of assurance artefacts
G3: Raise of technology innovation
G4: Increase harmonisation and interoperability

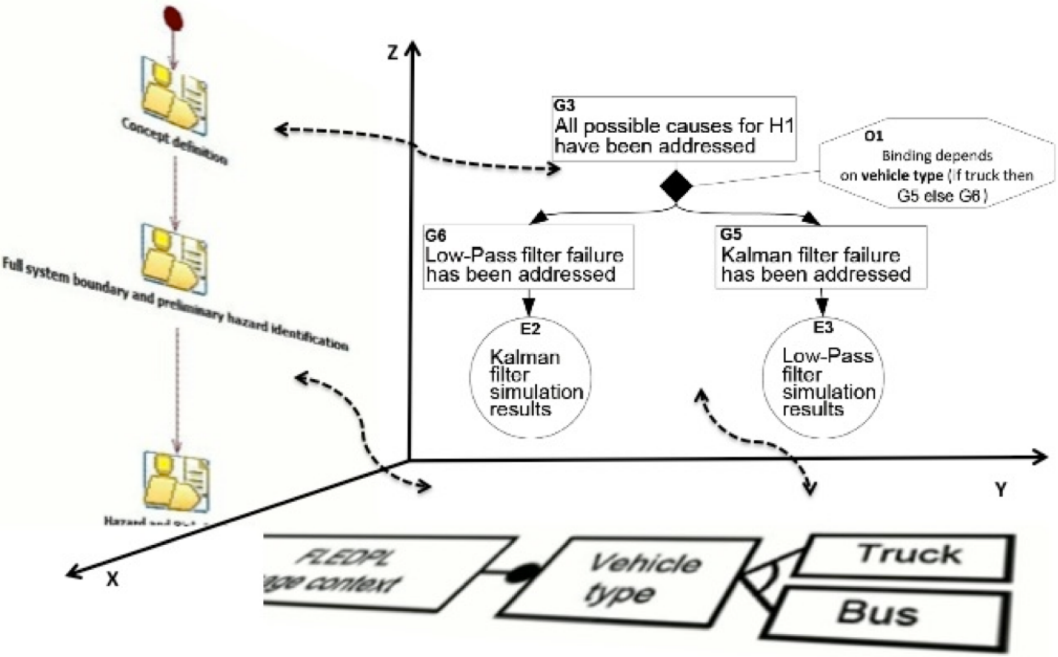
Tangible Results



AMASS project overview
-Scientific Objectives-

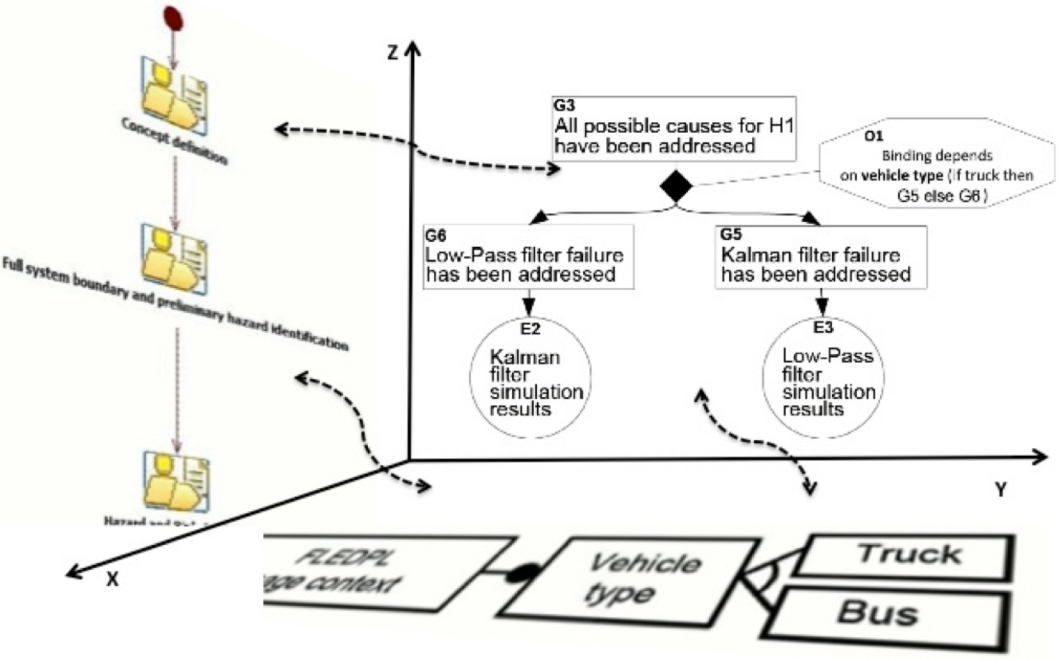


AMASS platform core



[Gallina, 2015]

AMASS platform core



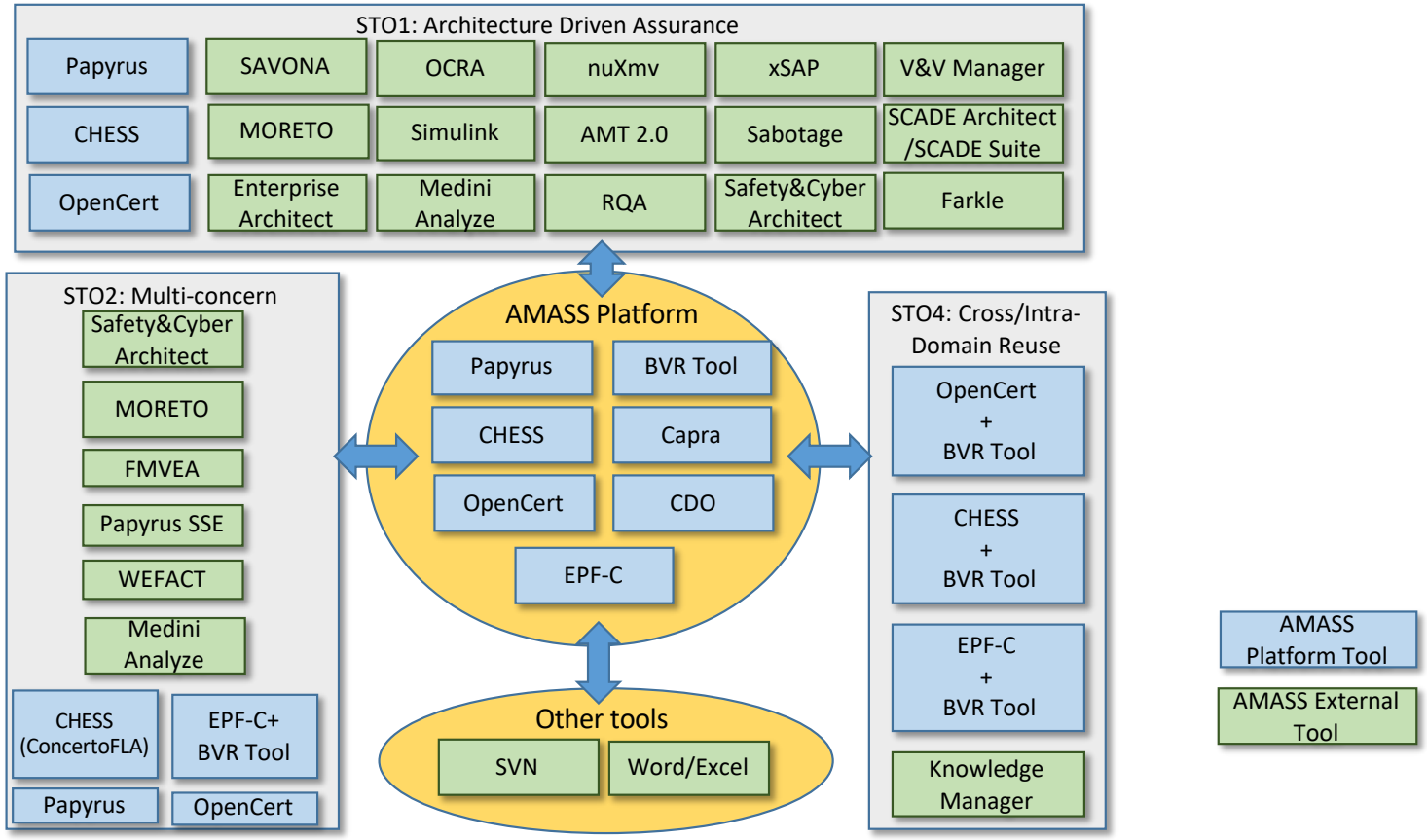
- OpenCert
- PolarSys CHESS
- eclipse PROCESS FRAMEWORK

+ BVR Tool

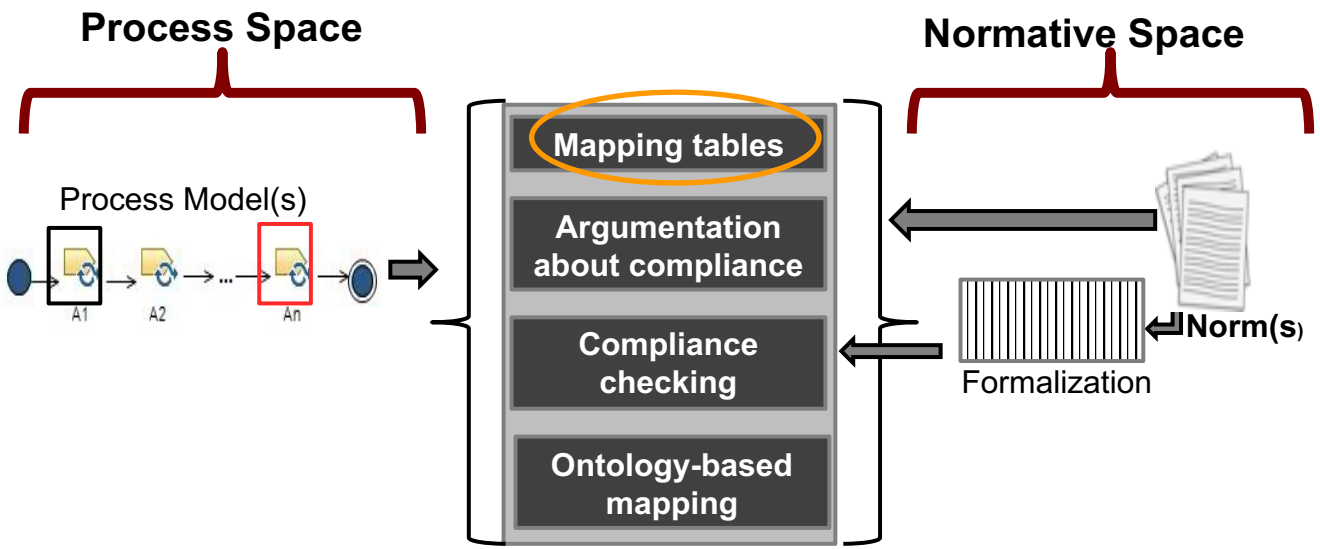
[Gallina, 2015]

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

AMASS platform and ecosystem

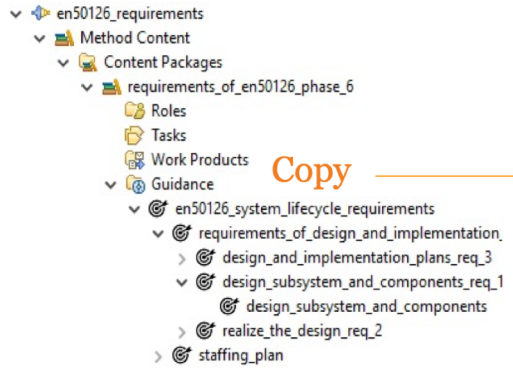


AMASS platform in action



AMASS platform in action

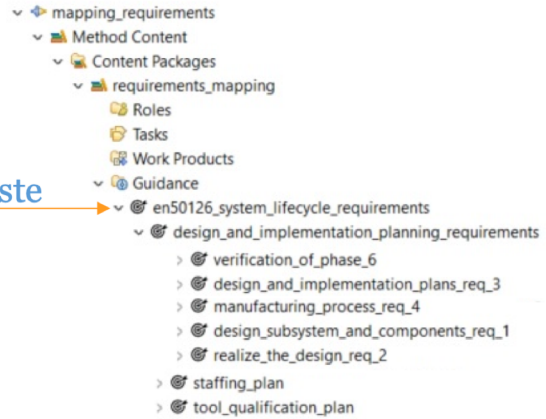
Standard Requirements plugin



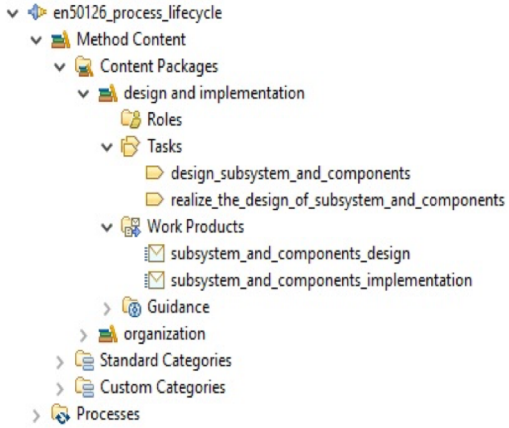
Copy

Paste

Mapping Requirements plugin

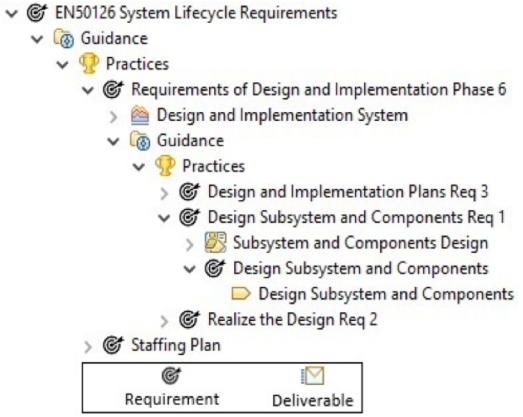


Process Lifecycle plugin

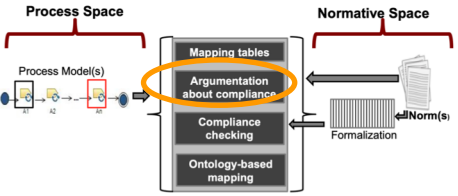


The links between process elements to each "standard requirement" have been established through "references" tab

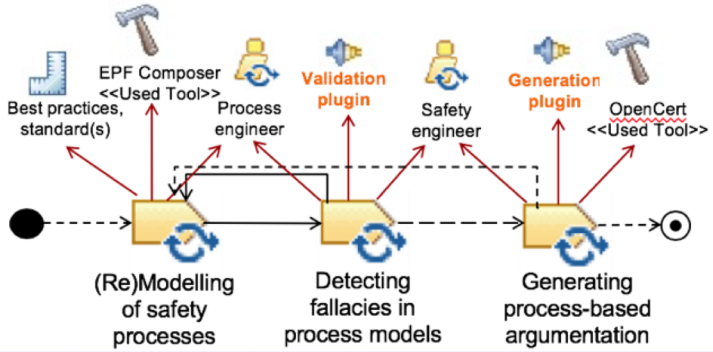
Mapped requirements in Browsing perspective

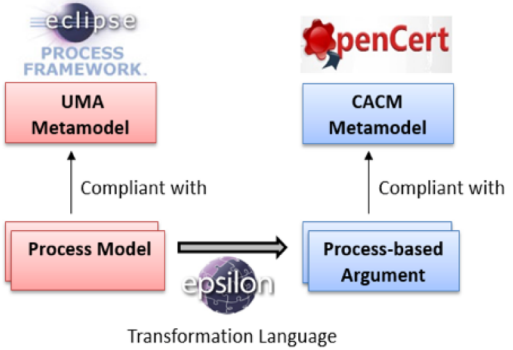


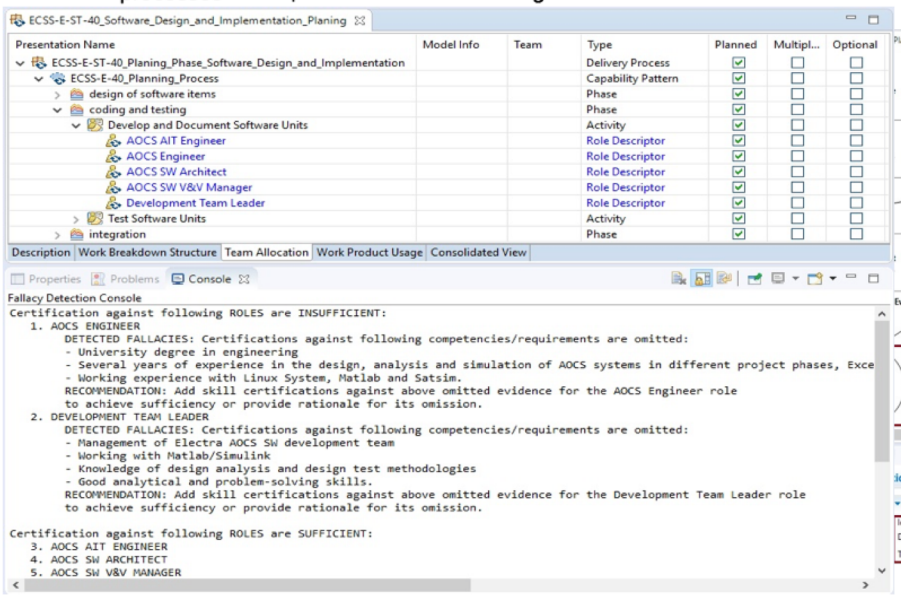
[Ul Muram et al. 2019]

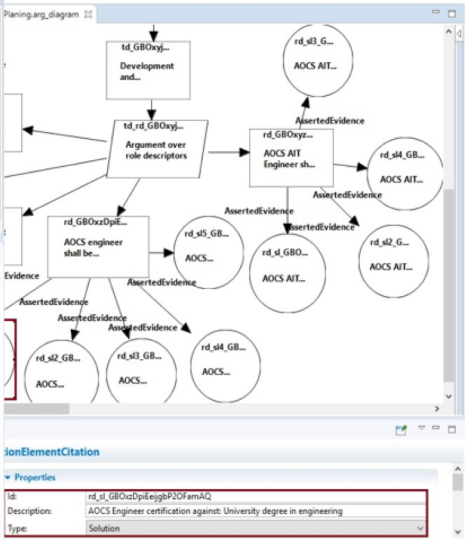


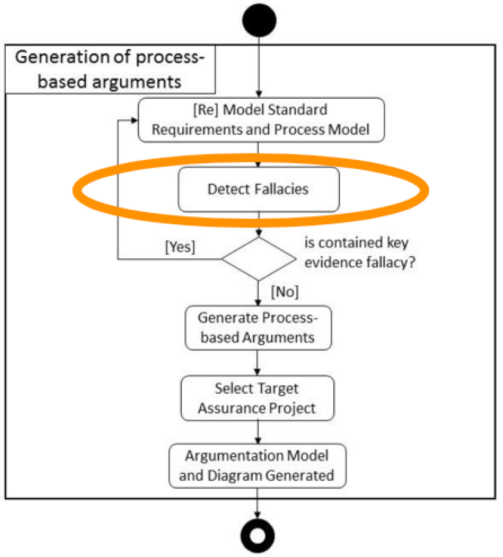
AMASS platform in action





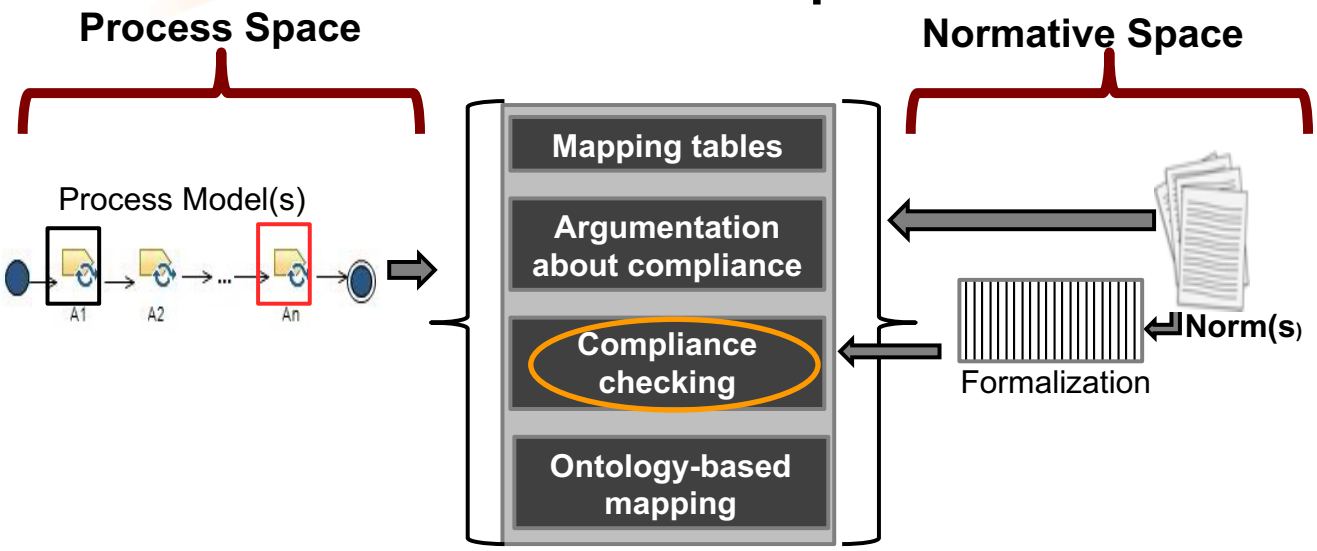




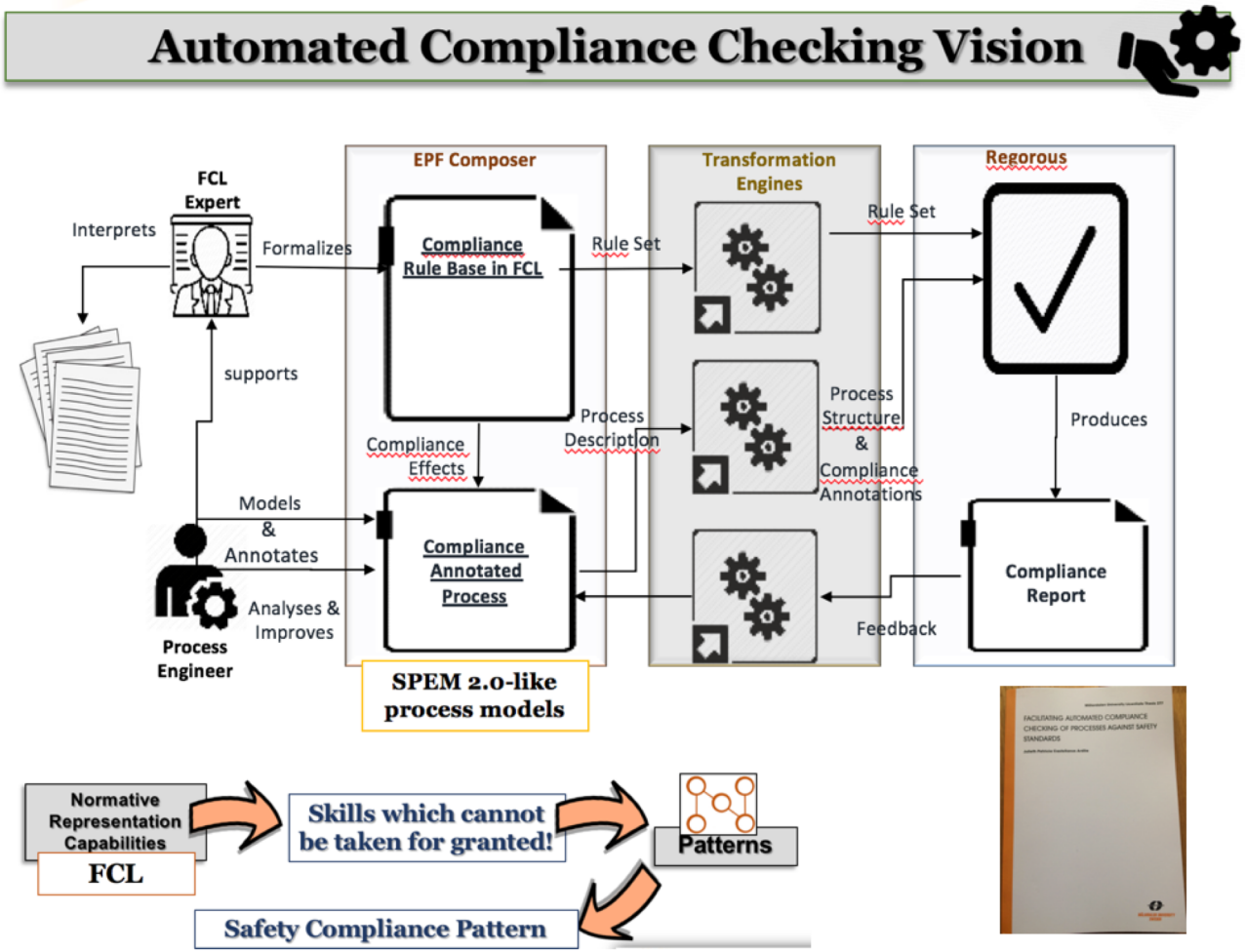


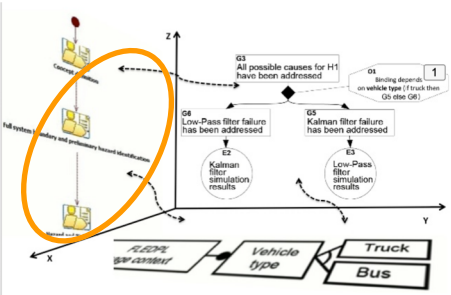
[Ul Muram, 2018]

AMASS platform in action



AMASS platform in action





AMASS platform in action

A software process modelled in EPF Composer

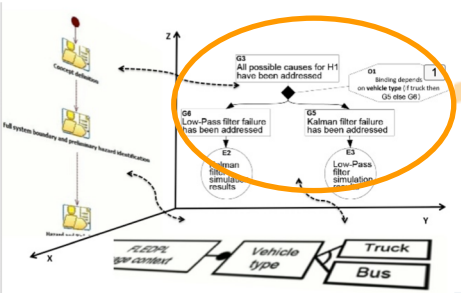
The achievement of error free models

Backward propagation of configured models

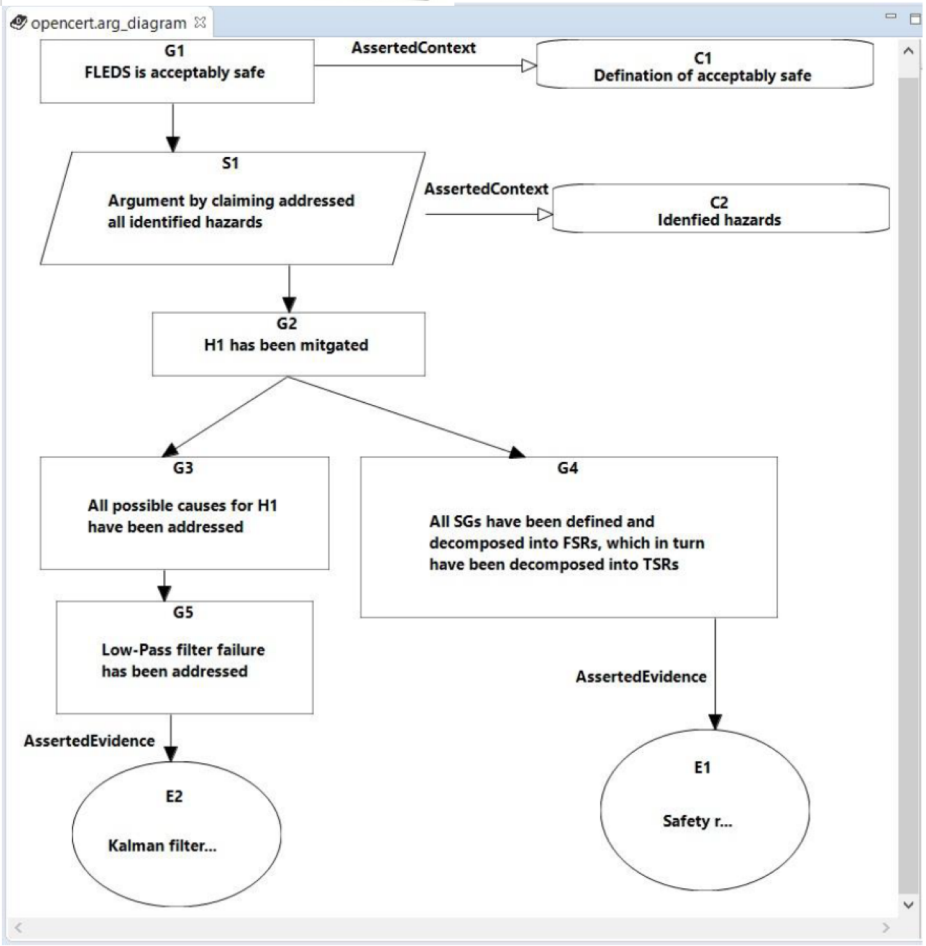
BVR Resolution editor

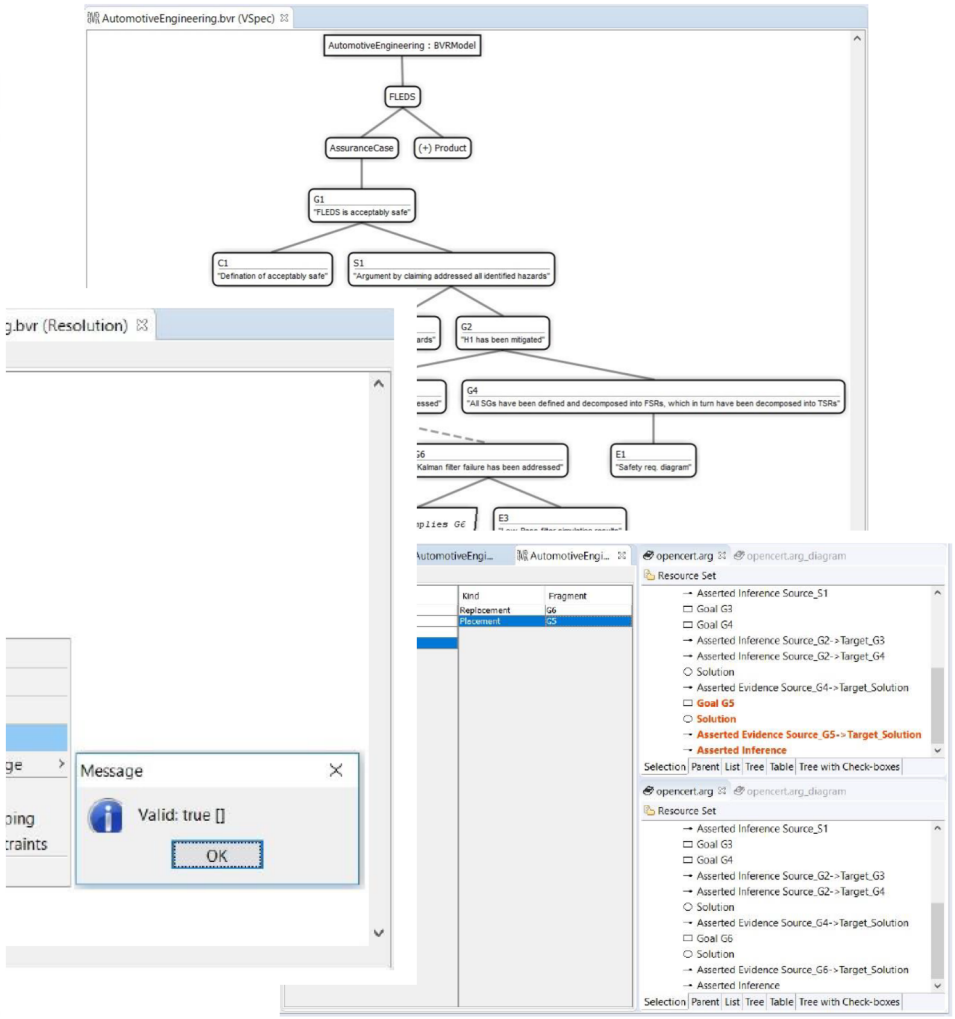
BVR VSpec editor

BVR Realization editor

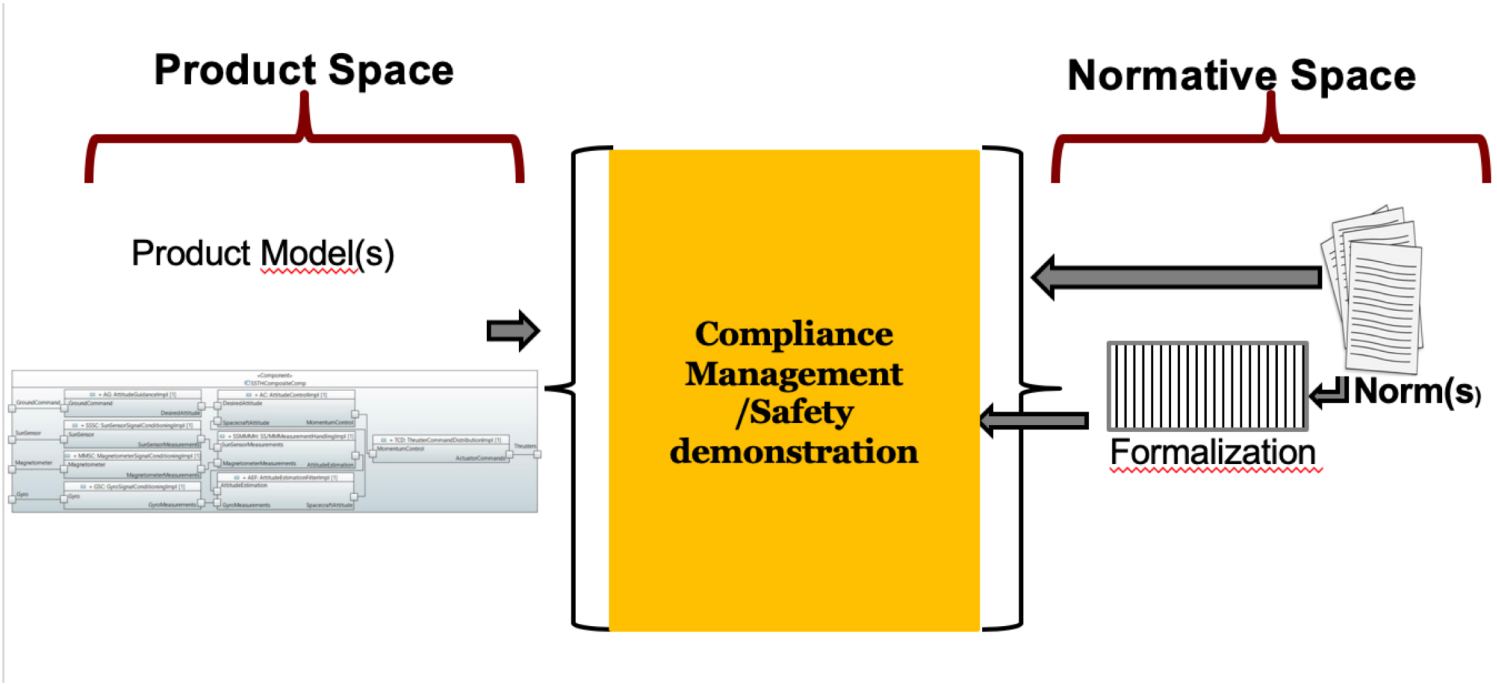


AMASS platform in action

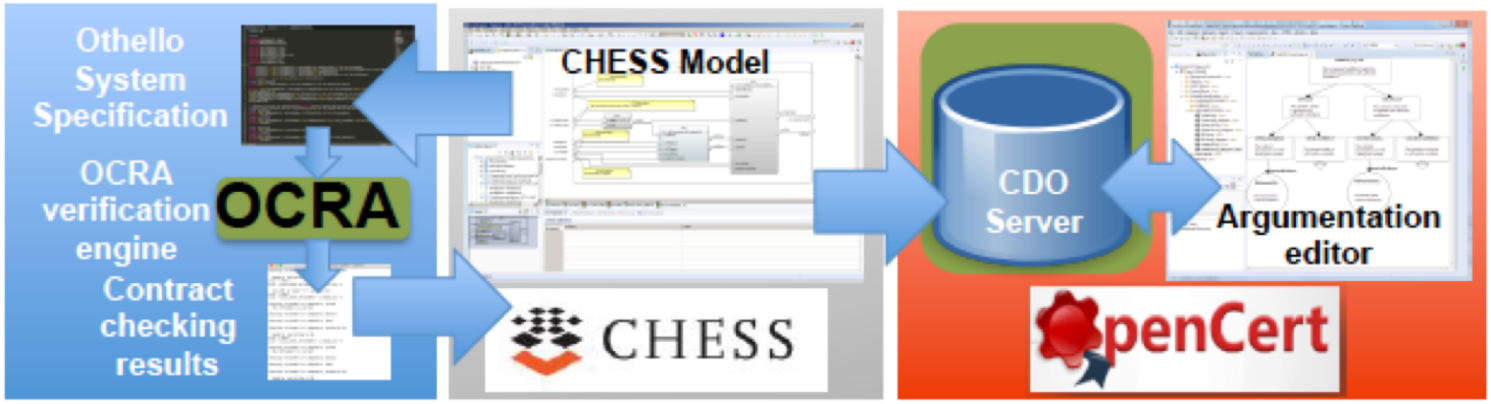




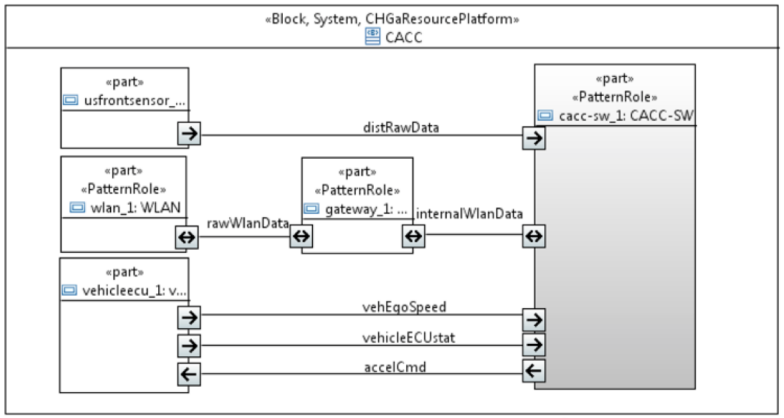
AMASS platform in action



AMASS platform in action



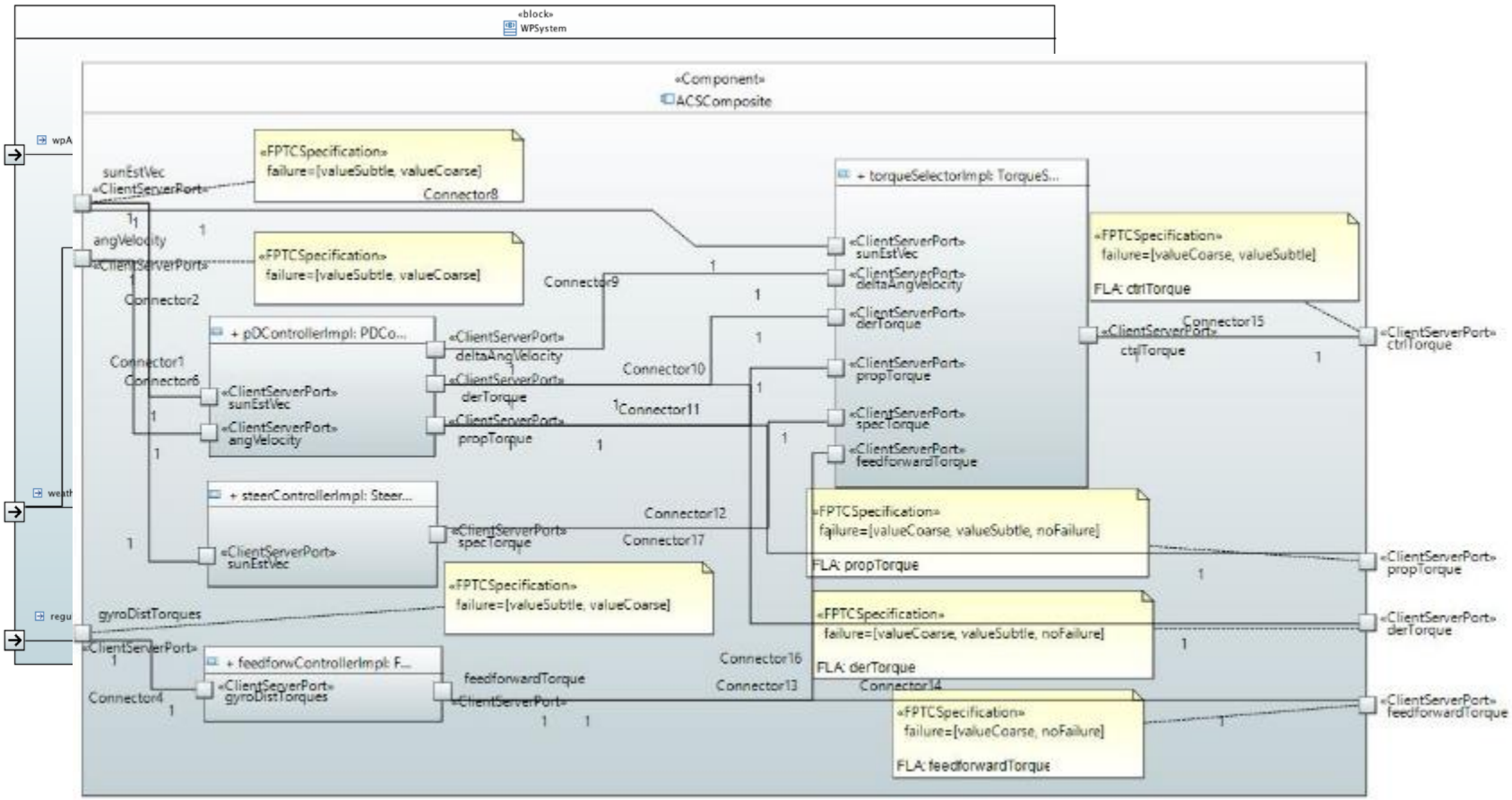
[Sljivo, 2018]



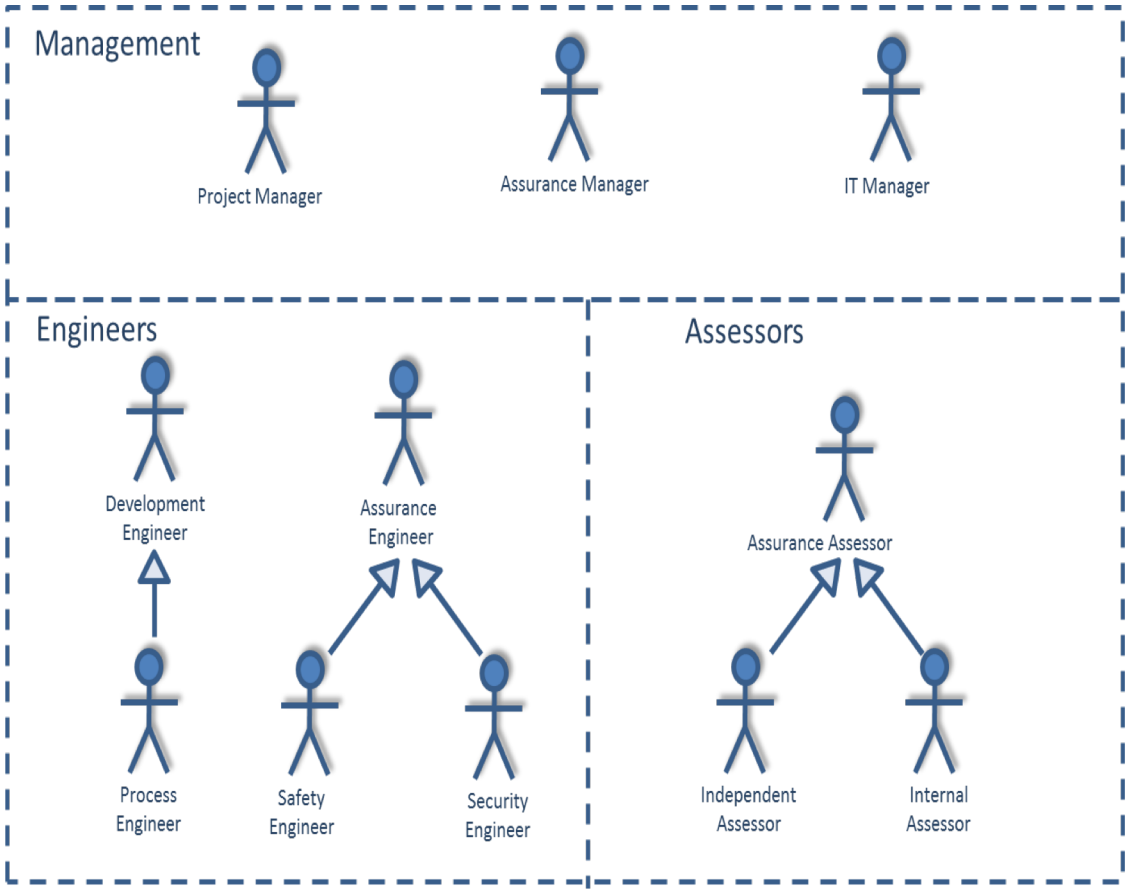
[Pattern-based architectural specification: CS3, Security Gateway Pattern]

[Pattern-based argumentation generation]

AMASS platform in action

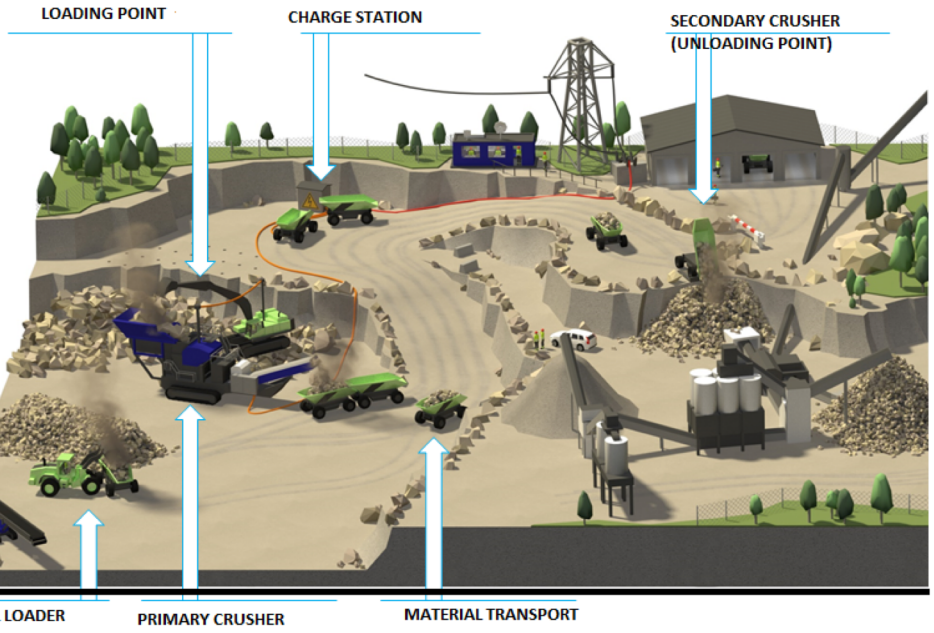


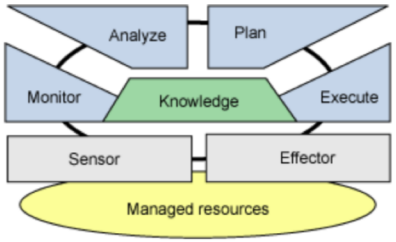
AMASS platform future development
Call for Users and Contributors



AMASS platform future development

in the context of SACSys- Safe and Secure Adaptive Collaborative Systems





Perception
Comprehension
Projection

Situation awareness
Decision making
Action

Source: https://www.volvoce.com/global/en/news-and-events/press-releases/2018/testing-begins-at-worlds-first-emission-free-quarry/

References

- AMASS Project (online) https://www.amass-ecsel.eu/
- AMASS Project: Deliverables (online) https://www.amass-ecsel.eu/content/deliverables
- AMASS Project: Deliverable 1.6 - AMASS demonstrators (c) (2019)
- AMASS Project: Deliverable 1.7 - AMASS solution benchmarking (2019)
- AMASS Project: Deliverable 2.4 - AMASS reference architecture (c) (2018)
- AMASS Project: Deliverable 2.5 - AMASS user guidance and methodological fwk. (2018)
- AMASS Project: Deliverable D7.7 - AMASS open source platform (c) (2018)
- AMASS Project: Publications (online) https://www.amass-ecsel.eu/content/publications
- The AMASS Platform: https://www.polarsys.org/opencert/
- YouTube: Opencert (online) https://youtube.com/channel/UCw_D0l5sDgysEphi6tzzDyw
- Gallina, B., et al.: AMASS: Call for Users and Contributors. Eclipse Newsletter (2019)
- Espinoza, H., et al.: Meet the new Eclipse-based tools for Assurance and Certification of Cyber-Physical Systems. Eclipse Newsletter (2018)
- [Variability Management at Assurance Case Level (MDH)] https://www.youtube.com/watch?v=m0vci8lZQxk
- [Automate Compliance Checking (MDH)] https://www.youtube.com/watch?v=DY8kuyigv_4&feature=youtu.be
- [Basic Compliance in EPF (MDH)] https://www.youtube.com/watch?v=stmoYPOK7iw&feature=youtu.be
- [Product-based Multi-Concern Argument Fragment Generation (MDH)] https://www.youtube.com/watch?v=NUS2GouUNvM
- [System Dependability Functionality via concerto FLA (MDH)] https://www.youtube.com/watch?v=3XWn1VrL2_8

References

- 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.
- 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.
- 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.
- 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), Thessaloniki, Greece, October 9-10, 2018.
- 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.
- I. Sljivo, B. Gallina, J. Carlson, H. Hansson, S. Puri. Tool-Supported Safety-Relevant Component Reuse: From Specification to Argumentation. 23rd International Conference on Reliable Software Technologies (Ada-Europe), Lisbon, Portugal, June 18-22, 2018.
- I. Sljivo, Garazi Juez Uriagereka, Stefano Puri, and B. Gallina. Guiding Assurance of Architectural Design Patterns for Critical Applications. Ada Europe SI, accepted paper, 2019.
- 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.
- 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.

Thank you for your attention!

Discussion time…