The AMASS Tool Platform: An Innovative Solution for Assurance and Certification of Cyber-Physical Systems

Jose Luis de la Vara
University of Castilla-La Mancha
Albacete, Spain
joseluis.delavara@uclm.es

Eugenio Parra
Carlos III University of Madrid
Leganes, Spain
eparra@inf.uc3m.es

Alejandra Ruiz
Tecnalia Research and Innovation
Derio, Spain
alejandra.ruiz@tecnalia.com

Barbara Gallina
Mälardalen University
Västerås, Sweden
barbara.gallina@mdh.se

Abstract

Cyber-physical systems are usually subject to assurance and certification processes, including thorough requirements engineering tasks, to ensure that they are acceptably dependable. The underlying activities can be complex and labour-intensive, thus practitioners need tools that facilitate them. We present the AMASS Tool Platform as an example of these tools. This Platform is an open source solution that supports the main activities for assurance and certification. It also provides advanced features such as argument fragment composition and automated assurance evidence generation and collection. In addition, we present the main insights gained from tool usage. Among them, practitioners expect improvement in relation to usability, performance, and ease of configuration. Videos showing tool usage are available online, including general usage scenarios[1].

Keywords: cyber-physical systems, assurance, certification, AMASS.

1 Introduction

Cyber-physical systems (CPS), e.g. aircrafts, cars, and trains, are usually subject to rigorous assurance and certification processes to provide adequate confidence and evidence that the systems satisfy given requirements and thus are dependable [Nai14], i.e. acceptably safe, secure, reliable, etc. This is typically performed in compliance with standards. For complex systems, the activities are challenging and labour-intensive because

In: M. Sabetzadeh, A. Vogelsang, S. Abualhaija, M. Borg, F. Dalpiaz, M. Daneva, N. Fernández, X. Franch, D. Fucci, V. Gervasi, E. Groen, R. Guizzardi, A. Herrmann, J. Horkoff, L. Mich, A. Perini, A. Susi (eds.): Joint Proceedings of REFSQ-2020 Workshops, Doctoral Symposium, Live Studies Track, and Poster Track, Pisa, Italy, 24-03-2020, published at http://ceur-ws.org

[1] https://youtu.be/9cEhDcai_9g

of the large set of compliance criteria to fulfil, the amount of evidence to manage, and the need for providing valid dependability justifications, among other issues [dlV16][Nai15]. Therefore, practitioners need adequate tool support for assurance and certification. The activities are however usually executed with different tools that are not integrated, and most often with basic tools such as Excel that provide very limited specific support.

The AMASS project (Architecture-driven, Multi-concern and Seamless Assurance and Certification of CPS; [Ama20]) provided innovative tool support for assurance and certification. AMASS was an industry-academia research project in which 29 partners from eight countries worked on the creation and consolidation of the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification.

The ultimate goal of AMASS was to lower certification costs for CPS. To this end, a novel holistic approach was defined for architecture-driven assurance (compatible with standards such as SysML), multi-concern assurance (for co-analysis and co-assurance of e.g. security and safety aspects), seamless interoperability between assurance and engineering activities (including their tool support), and cross- and intra-domain reuse of assurance assets (e.g. of assurance evidence between projects).

The tool that supports the approach is referred to as AMASS Tool Platform. It is an open source solution that has integrated and further developed several existing technologies and toolsets for compliance management, system modelling, process engineering, traceability, variability management, and tool interoperability. The Platform includes support for requirements engineering (RE) tasks such as elicitation, specification, and analysis of dependability requirements. It is managed as an Eclipse project [OpC20].

The following sections introduce the requirements, architecture, and implementation of the AMASS Tool Platform and the experience in using it. These aspects have not been introduced in conjunction in any prior publication. Nonetheless, AMASS deliverables [Ama20] include details about them separately. Prior publications also provide more information about the motivation [Rui16] and objectives [dlV19a] of the AMASS project, the process that underlies Platform usage [dlV19b], and the Eclipse open source project [Esp18][Gal19]. Publications on specific research topics are available, e.g. on artefact quality analysis [Par19].

2 Workflow and Requirements

The AMASS Tool Platform provides a collaborative tool environment that supports the main activities for CPS assurance and certification, including activities dealing with product requirements and with process requirements. The general assurance project stages supported, as high-level features, are *Standards Compliance Definition*, *Process Reusability Definition*, *Assurance Project Definition*, *System Design Analysis and V&V*, *Assurance Case Management*, and *Evidence Management* [Ama18b]. Not all stages need to be performed for each project; e.g. the first two stages are project independent and the outcome could be re-used for multiple projects.

Three categories of user roles exist [Ama18a]: Manager, such as Project, Assurance, and IT Managers; Engineer, such as Development Engineer (including Process Engineer) and Assurance Engineer (including Safety and Security Engineers), and; Assessor, such as Assurance Assessor (including Independent and Internal Assessors).

For *Standards Compliance Definition*, the Assurance Manager and the Process Engineer capture and retrieve compliance knowledge from standards about requirements and other compliance criteria. The Assurance Manager and the Process and Assurance Engineers participate in *Process Reusability Definition* to manage reusable compliant process elements. During *Assurance Project Definition*, the Assurance Manager and the Process Engineer define the compliance needs, reuse possibilities, and compliance means for a project. For *System Design Analysis and V&V*, the Development and the Assurance Engineers elicit and specify system requirements, define the system architecture, define and validate component contracts, and execute dependability analyses. *Assurance Case Management* addresses argumentation using compliance and product arguments, resolution of safety-security trade-offs, and the link to system architecture, involving the Assurance Manager and the Process, Assurance, and Development Engineers. The Assurance Manager and the Assurance and Process Engineers perform *Evidence Management* by collecting and specifying data about project artefacts, traceability, process execution, and compliance.

The analysis and specification of these high-level features, users, and workflow was conducted in parallel to the elicitation and documentation of 151 high-level requirements [Ama17] (e.g. "The AMASS Tool Platform shall be able to validate formal requirements" and "The AMASS Tool Platform shall allow an assurance engineer to specify the characteristics of assurance evidence") and 73 use cases [Ama18a] (e.g. "Analyse requirements" and "Characterise evidence artefact") for the main overall functional areas of the Platform: platform infrastructure, architecture-driven assurance, multi-concern assurance, seamless interoperability, and cross- and intra-domain reuse. The requirements and use cases were also grouped by finer-grain architectural building blocks (Section 3).

3 Architecture and Implementation

The logical architecture of the AMASS Tool Platform is referred to as AMASS Reference Tool Architecture (Figure 1; [Ama18a]). The Architecture provides a conceptual framework for architecture-driven assurance, multi-concern assurance, seamless interoperability, and cross- and intra-domain reuse of assurance assets. It contains both technological building blocks, e.g. System architecture modelling for assurance, and the Common Assurance & Certification Metamodel. The metamodel provides an information model for CPS assurance and certification, e.g. for Compliance management and for Assurance case specification. Basic application services such as Access and Data management are also considered. The main stakeholder groups of the architecture are Manufacturer, Supplier, Assessor & Authorities, and Tool Vendors.

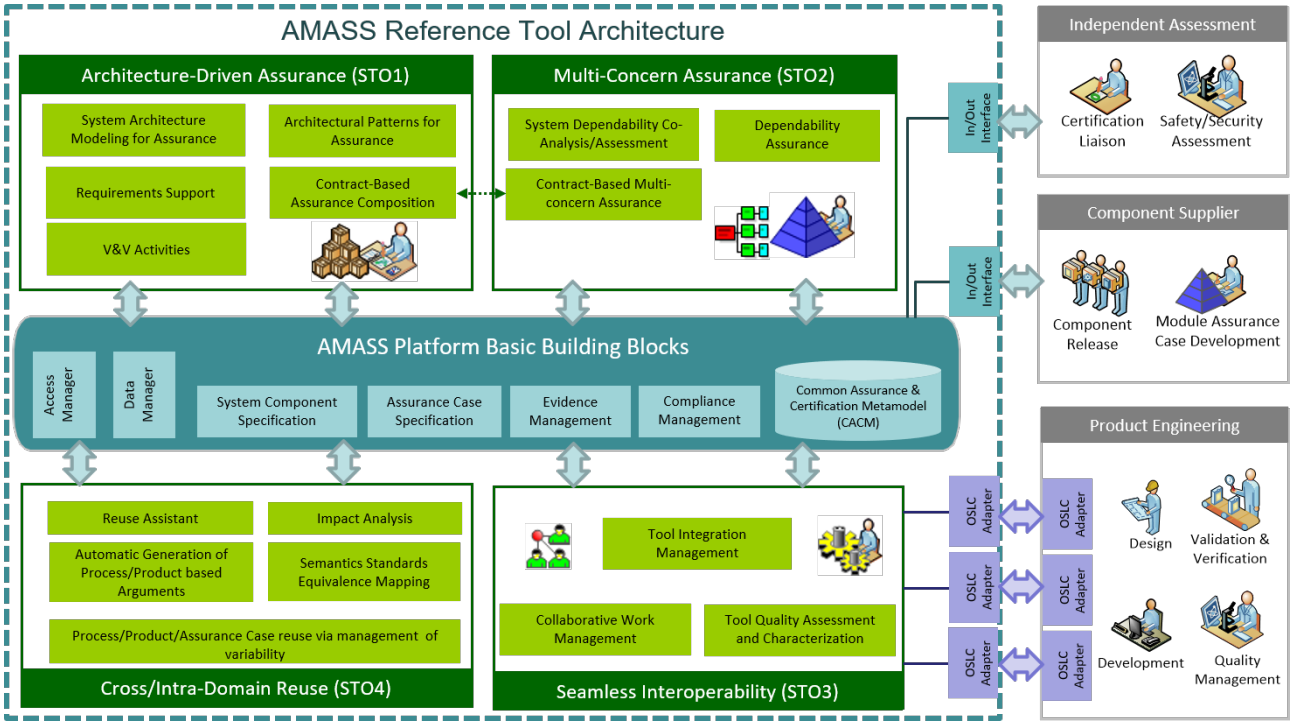

Figure 1: AMASS Reference Tool Architecture

All the building blocks relate to RE, as CPS assurance and certification deals with the determination of dependability requirements for the systems, both for products and for processes and both from standards and from system analyses, as well as with the justification of requirement satisfaction. The most RE-focused building block is arguably Requirements support, which addresses requirements derivation from dependability analyses, formalisation, quality analysis, and verification.

The AMASS Tool Platform is a concrete implementation of the AMASS Reference Tool Architecture with capability for evolution and adaptation (Figure 2). Eclipse is the main environment for Platform usage, but web-based support also exists for some functionality. The Platform has integrated and further developed:

- OpenCert for compliance management, evidence management, assurance case specification, and dependability assurance modelling.
- Papyrus and CHESS for system modelling, system analysis, contract modelling, contract-based multi-concern assurance, contract-based trade-off analysis, and design verification.
- EPF-Composer for assurance process modelling, compliance, and tailoring.
- Capra for traceability management for requirements and other system artefacts.
- BVR for orthogonal variability management, also in relation to assets created with EPF-Composer, CHESS, and OpenCert.

- OSLC for tool interoperability features.
- CDO for data storage management.

An integrated usage workflow could be as follows. OpenCert would be used to specify and analyse the compliance criteria for a project such as the requirements to satisfy from applicable standards, and EPF-Composer to define a project-specific assurance process according to process requirements. BVR would help a user study their variants, e.g. for compliance. Papyrus and CHESS would then support system modelling and automated analysis, including requirements needs. The results could be traced with Capra and used in evidence management. If data had to be imported from or exported to an external tool, OSLC would enable it. Finally, assurance cases could be managed throughout the workflow to justify requirement satisfaction, updating them according to design decisions and the available evidence, and generating fragments.

In addition, the AMASS Tool Platform interacts with over a dozen tools that provide additional features, typically commercial ones, e.g.:

- MORETO [Ama18d] for security analysis and generation of security requirements.
- Medini Analyze [ANS20] for workflow support and for safety and security analyses.
- SAVONA [Exp20] for contract modelling.
- SafetyArchitect and CyberArchitect [RiO20] for dependability co-analysis.
- OCRA [OCR20] for system V&V.
- RQA - Quality Studio [TRC20] for requirements quality analysis.

The resulting open source ecosystem and community are managed as an Eclipse project [OpC20]. The community deals with the maintenance, evolution, and industrialization of the AMASS Tool Platform and is supported by a governance board and by rules, policies, and quality models. Last but not least, the documentation of the AMASS Tool Platform includes a detailed developers' guide [Ama18b] for those interested in implementing new functionality for or on top of the Platform.

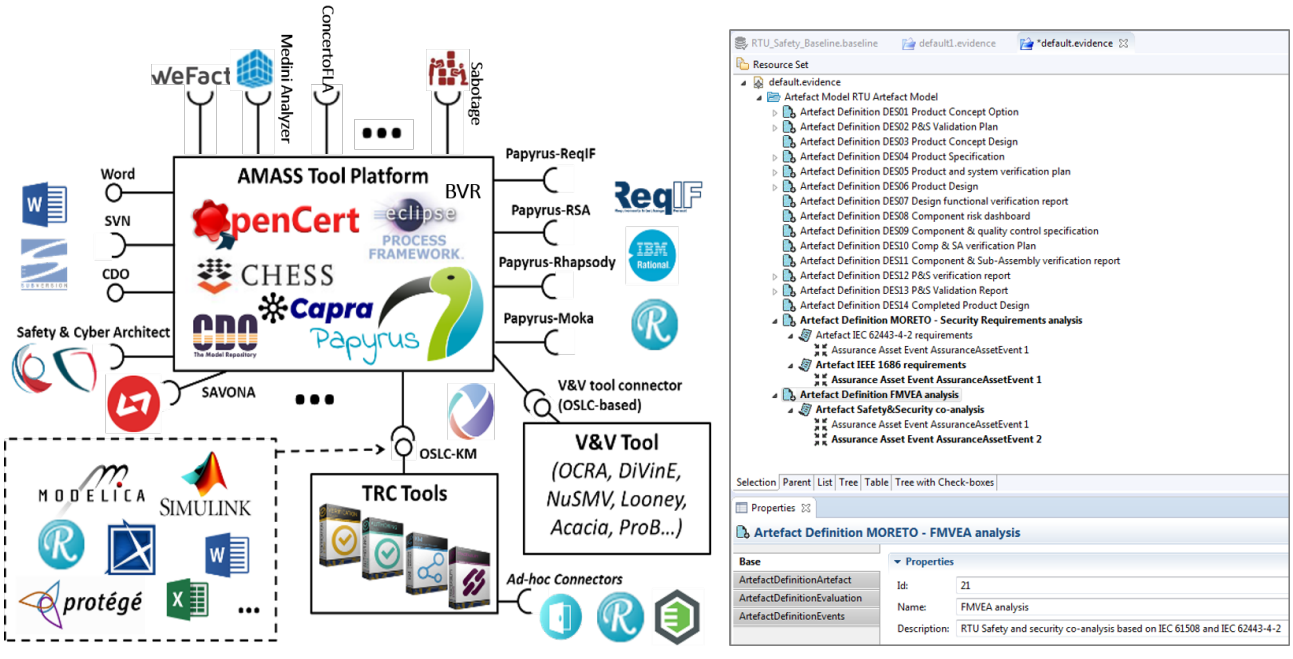

Figure 2: General view of the AMASS Tool Platform and its ecosystem

4 Experience and Lessons Learned

The main experience and lessons learned from using the AMASS Tool Platform are a result of three different activities during the AMASS project.

Validation [Ama18c][Ama19c]. Three versions of the Platform were released during the AMASS project. Each version underwent validation tasks. The execution of 141 test cases confirmed the implementation of 93% of the high-level requirements specified for the Platform. The usability analysis results suggest that EPF-Composer and Papyrus provide a good user experience and that the rest of tools have larger potential for improvement. The documentation of the Platform could also be enhanced, as inconsistency was found because of insufficient homogeneity in the documentation style by all the contributors and for all the features. Finally, it appeared that the main data storage technology could impact performance under certain configurations.

Application [Ama19a]. The AMASS Tool Platform was used in 11 industrial case studies from air traffic management, automotive, avionics, industrial automation, railway, and space. Each case study selected a subset of the functionality of the AMASS Tool Platform for its application, and each piece of functionality was applied in at least one case study. For example, requirements were modelled, analysed, and verified and their satisfaction was justified, among other activities, in the scope of safety assessment of multi-modal interactions in cockpits for the avionics domain. Practitioners in the AMASS consortium reported achievements, benefits, improvement opportunities, and recommendations from the application of the Platform. Suggestions were made on user interaction (e.g. to further guide the users), the value of the new features was stated (e.g. modelling of standards), and easier configuration was expected for the Platform. It is a large tool with many sub-tools, but an organisation would typically be interested only in a subset of the functionality. The selection, configuration, and tailoring of the subset could be better supported, e.g. with a dashboard for feature selection.

Benchmarking [Ama19b]. The industrial case studies were used to compare how assurance and certification could be executed with the Platform and how they were executed before. Quantitative evaluations were performed to study the reduction of effort in assurance and certification (initial target: 50%), reduction of risks (35%), reduction of costs in (re)certification (40%), and increase in technology harmonisation and interoperability (60%). These goals were achieved in general, but to a varying extent among the case studies. The use of different features is one of the reasons.

The above-mentioned activities also allowed the AMASS consortium to estimate the Technology Readiness Level of its components [Ama19c]. Such a level differs among them. EPF-Composer and Papyrus can be regarded as the most mature technologies. Tool qualification considerations of the AMASS Tool Platform have also been analysed [Ama19c]. Although the Platform itself cannot directly introduce errors in a system, the specific aspects to consider will depend on how the Platform is used, e.g. regarding the verification of its automatic actions and the toolchain deployed.

5 Conclusion

The AMASS project developed innovative tool support for CPS assurance and certification, and thus for certain RE needs of CPS, focusing on architecture-driven assurance, multi-concern assurance, seamless interoperability, and cross- and intra-domain reuse of assurance assets. The resulting AMASS Tool Platform is an open source solution that facilitates system modelling and analysis, compliance management, argumentation, process engineering, variability management, and traceability. The Platform is also integrated with external tools for additional features, e.g. for requirements quality analysis. Although the Platform needs to further mature, we argue that its finalisation and its public release are initial, major milestones. It is the first integrated environment for assurance and certification and benefits from its use have been demonstrated.

The development of the AMASS Tool Platform focused on supporting assurance and certification for CPS, but the Platform can be used for any system or project having to deal with e.g. system modelling or compliance. Nonetheless, Platform usage would in principle have to be tailored.

We plan to continue working on the development of tool support that improves assurance and certification. This includes the development of novel solutions for traceability, assurance case management, and privacy assurance.

Acknowledgements

The research leading to this paper has received funding from the AMASS (H2020-ECSEL grant agreement no 692474), iRel4.0 (H2020-ECSEL grant agreement no 876659), VALU3S (H2020-ECSEL grant agreement no

876852), and Treasure (JCCM ref. SBPLY/19/180501/000270) projects, and from the Ramon y Cajal Program (MICINN ref. RYC-2017-22836; European Social Fund). We are also grateful to all the people that have contributed to the development of the AMASS Tool Platform.

References

[Ama17] AMASS Project: Deliverable 2.1 - Business cases and high-level requirements. 2017.

[Ama18a] AMASS Project: Deliverable 2.4 - AMASS reference architecture (c). 2018.

[Ama18b] AMASS Project: Deliverable 2.5 - AMASS user guidance and methodological framework. 2018.

[Ama18c] AMASS Project: Deliverable 2.8 - Integrated AMASS platform (c). 2018.

[Ama18d] AMASS Project: Deliverable 4.6 - Prototype for multi-concern assurance (c). 2018.

[Ama19a] AMASS Project. Deliverable 1.6 - AMASS demonstrators (c). 2019.

[Ama19b] AMASS Project: Deliverable 1.7 - AMASS solution benchmarking. 2019.

[Ama19c] AMASS Project: Deliverable 2.9 - AMASS platform validation. 2019.

[Ama20] AMASS Project (online) https://www.amass-ecsel.eu/ (Accessed Feb 17, 2020)

[ANS20] ANSYS. Ansys medini analyze (online) https://www.ansys.com/products/systems/ansys-medini-analyze (Accessed Feb 17, 2020)

[dlV16] J.L. de la Vara, et al. An Industrial Survey on Safety Evidence Change Impact Analysis Practice. *IEEE Transactions on Software Engineering*, 42(12): 1095-1117, 2016.

[dlV19a] J.L. de la Vara, et al. AMASS: A Large-Scale European Project to Improve the Assurance and Certification of Cyber-Physical Systems. PROFES 2019.

[dlV19b] J.L. de la Vara, et al. The AMASS Approach for Assurance and Certification of Critical Systems. embedded world Conference 2019.

[Esp18] H. Espinoza, et al. Meet the new Eclipse-based tools for Assurance and Certification of Cyber-Physical Systems. Eclipse Newsletter, July 2018.

[Exp20] Expleo. SAVONA: Design, Specification & Verification of Embedded Systems (online) https://www.expleo-germany.com/en/products/savona/ (Accessed Feb 17, 2020)

[Gal19] G. Gallina, et al. AMASS: Call for Users and Contributors. Eclipse Newsletter, July 2019.

[Nai14] S. Nair, et al. An extended systematic literature review on provision of evidence for safety certification. *Information and Software Technology*, 56(7): 689-717, 2014.

[Nai15] S. Nair, et al. Evidence management for compliance of critical systems with safety standards: A survey on the state of practice. *Information and Software Technology* 60: 1-15, 2015.

[OCR20] OCRA (online) https://ocra.fbk.eu/ (Accessed Feb 17, 2020)

[OpC20] OpenCert (online) https://www.polarsys.org/opencert/ (Accessed Feb 17, 2020)

[Par19] E. Parra, et al. Advances in Artefact Quality Analysis for Critical Systems. ISSRE 2019.

[RiO20] RiskOversee (online) https://www.riskoversee.com/en/home/ (Accessed Feb 17, 2020)

[Rui16] A. Ruiz, et al. Architecture-driven, Multi-concern, Seamless, Reuse-Oriented Assurance and Certification of Cyber-Physical Systems. SAFECOMP Workshops 2016.

[TRC20] The REUSE Company. RQA - Quality Studio (online) https://www.reusecompany.com/rqa-quality-studio (Accessed Feb 17, 2020)

[You20] Youtube. AMASS Prototype P1 Architecture-driven (online) https://youtu.be/9cEhDcai_9g (Accessed Feb 17, 2020)