AMASS: A Large-Scale European Project to Improve the Assurance and Certification of Cyber-Physical Systems

Jose Luis de la Vara[1(✉)], Eugenio Parra[2], Alejandra Ruiz[3], and Barbara Gallina[4]

[1] University of Castilla-La Mancha, Albacete, Spain
joseluis.delavara@uclm.es
[2] Carlos III University of Madrid, Leganes, Spain
eparra@inf.uc3m.es
[3] Tecnalia Research and Innovation, Derio, Spain
alejandra.ruiz@tecnalia.com
[4] Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se

Abstract. Most safety-critical systems must undergo assurance and certification processes. The associated activities can be complex and labour-intensive, thus practitioners need suitable means to execute them. The activities are further becoming more challenging as a result of the evolution of the systems towards cyber-physical ones, as these systems have new assurance and certification needs. The AMASS project (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) tackled these issues by creating and consolidating the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of cyber-physical systems. The project defined a novel holistic approach for architecture-driven assurance, multi-concern assurance, seamless interoperability, and cross- and intra-domain reuse of assurance assets. AMASS results were applied in 11 industrial case studies to demonstrate the reduction of effort in assurance and certification, the reduction of (re)certification cost, the reduction of assurance and certification risks, and the increase in technology harmonisation and interoperability.

Keywords: AMASS · Cyber-physical system · CPS · Assurance · Certification

1 Introduction

Safety-critical systems are usually subject to rigorous assurance and certification processes to provide confidence that the systems are dependable [18], i.e. acceptably safe, reliable, etc. This is typically performed in compliance with standards, e.g. ISO 26262 in automotive and DO-178C in avionics, and is a requirement so that the systems are allowed to operate. The associated activities are usually complex and labour-intensive because of the large set of compliance criteria to fulfil, the amount of assurance

X. Franch et al. (Eds.): PROFES 2019, LNCS 11915, pp. 626–632, 2019.
https://doi.org/10.1007/978-3-030-35333-9_49

evidence to manage, and the need for providing valid justifications of system dependability, among other issues [18]. Therefore, practitioners need support.

Safety-critical systems have also significantly increased in technical complexity and sophistication toward open, interconnected, networked systems such as "the connected car". This has brought a "cyber-physical" dimension with it, exacerbating the problem of ensuring dependability in the presence of human, environmental, and technological risks. New approaches for assurance and certification are needed so that these activities are cost-effective. The approaches must consider the new system characteristics, e.g. new architectures and the need for guaranteeing several dependability concerns, and provide means that facilitate the collection, management, and reuse of assurance assets.

The AMASS project (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems; [1]) created and consolidated the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets including automotive, railway, aerospace, space, and energy.

The ultimate goal of AMASS was to lower certification costs for CPS in face of rapidly changing features and market needs. This was achieved by establishing a novel holistic approach for architecture-driven assurance (fully 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 along with third-parties (e.g. supplier assurance), and cross- and intra-domain reuse of assurance assets (e.g. of assurance evidence between projects).

The AMASS project started in April 2016 and finished in March 2019. AMASS work built on the results from previous successful EU projects such as OPENCOSS [21], SafeCer [26], CRYSTAL [14], and CHESS [12]. Results from these projects were integrated and further developed in AMASS.

The next sections summarise the AMASS project by presenting its objectives, its organisation, and its main outcomes. Our purpose is to raise the awareness about the project and its results, including its open source community, so that further people and other projects continue researching on and developing solutions for assurance and certification from AMASS outcomes. Prior publications [10] provide further details about the motivation for the project [25], the process for approach application [15], and the Eclipse open source project [16, 17]. Publications on specific research topics are also available, e.g. on quality analysis of system artefacts for assurance [22]. More information about the project and its results are available in AMASS deliverables [2].

2 Project Objectives

The high-level **goals** of AMASS were the demonstration of:

1. G1: A potential gain for design efficiency of complex CPS by reducing their assurance and certification effort by 50%;
2. G2: A potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for product (re)certification activities;

3. G3: A potential raise of technology innovation led by 35% reduction of assurance and certification risks of new CPS products, and;
4. G4: A potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification tool technologies by 60%.

To achieve the goals, these project **objectives** were specified:

- O1: Define a holistic approach for architecture-driven assurance to leverage the reuse opportunities in assurance and certification by directly and explicitly addressing current technologies and hardware and software architectures needs.
- O2: Define a multi-concern assurance approach to ensure not only safety and security, but also other dependability aspects such as availability and reliability.
- O3: Consolidate a cross-domain and intra-domain assurance reuse approach to improve mutual recognition agreement of compliance approvals and to help assess the return of investment of reuse decisions.
- O4: Develop a fully-fledged open tool platform that allows developers and other assurance stakeholders to guarantee seamless interoperability of the platform with other tools used in the development of CPSs.
- O5: Benchmark the tool infrastructure against real industrial cases in relevant environments.
- O6: Consolidate the AMASS ecosystem and community for:
  - O6.a: Adoption of the AMASS conceptual and methodological approach as a reference tool architecture for CPS assurance and certification.
  - O6.b: Maintenance and further development of the open tool platform as a long-term, API-standardized, and industry-driven assurance and certification environment.

The main envisioned **impact** on the different stakeholders is as follows:

- OEMs (including system integrators) and Component suppliers can use AMASS results to increase CPS design cost-effectiveness, ease innovation, and reduce the costs and risks of CPS assurance and certification.
- Assessors and Certification authorities can provide services that better fit CPS-specific needs.
- Tool vendors can extend their products with new features and integrate them with AMASS tools.
- European society will benefit from the use of CPS with a higher confidence in their dependability.

3 Organisation

The **AMASS consortium** (Table 1) consisted of **29 partners from eight countries** and covered the whole value chain for CPS assurance and certification. The project manager was Alejandra Ruiz (Tecnalia R&I), the technical manager was Barbara

Gallina (Mälardalen University), and the quality manager was Cristina Martínez (Tecnalia R&I). Information about other roles and the implementation plan structure is available online [9]. AMASS also had an **External Advisory Board** [8] that included 14 relevant and influential experts on the topics of the project, including assessors, assurance and certification managers, consultants, engineers, and researchers. This board advised on technical decisions, standardization, and community building.

The industrial application of AMASS was analysed in **11 case studies** [3] from air traffic management, automotive, avionics, industrial automation, railway, and space, e.g. on autonomous driving features and satellite software design. The AMASS partners established **links with related ongoing EU projects** for networking, discussion, and collaboration, such as AQUAS [11], CP-SETIS [13], PDP4E [23], RobMosys [24], and SafeCOP [27]. AMASS also established **links with national projects**. Result **standardisation** was addressed, e.g. through system assurance work at OMG [19].

Table 1. AMASS partners per country and their main role in the value chain: ASR – Assessor, CER – Certification Authority, COS – Component Supplier, OEM – Original Equipment Manufacturer, RES – research, TOV – Tool Vendor

Country	Partner	Role
AT	AIT	RES
	Virtual Vehicle	RES
CZ	Honeywell	COS
	Masaryk Uni.	RES
DE	Ansys medini	TOV
	Assystem	TOV
	Eclipse Found.	TOV
	Infineon	COS
	Lange Aviation	OEM
ES	Carlos III Uni.	RES
	GMV	COS
	Schneider Electric	OEM
	Tecnalia R & I	RES
	Thales Alenia	COS
	The REUSE Co.	TOV
FR	ALL4TEC	TOV
	Alstom Transport	OEM
	CEA List	RES
	ClearSy	COS
IT	FBK	RES
	Intecs	ASR
	Rina	CER
	Thales	OEM
SE	Alten	ASR
	Comentor	ASR
	Mälardalen Uni.	RES
	OHB	COS
	RISE	RES
UK	Rapita Systems	TOV

4 Main Outcomes

AMASS resulted in three main tangible outcomes.

The **AMASS Reference Tool Architecture** (Fig. 1; [5]) 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 such as System architecture modelling for assurance and Tool integration management, and the Common Assurance & Certification Metamodel,

which provides an information model for CPS assurance and certification, e.g. for Compliance management and for Assurance case specification.

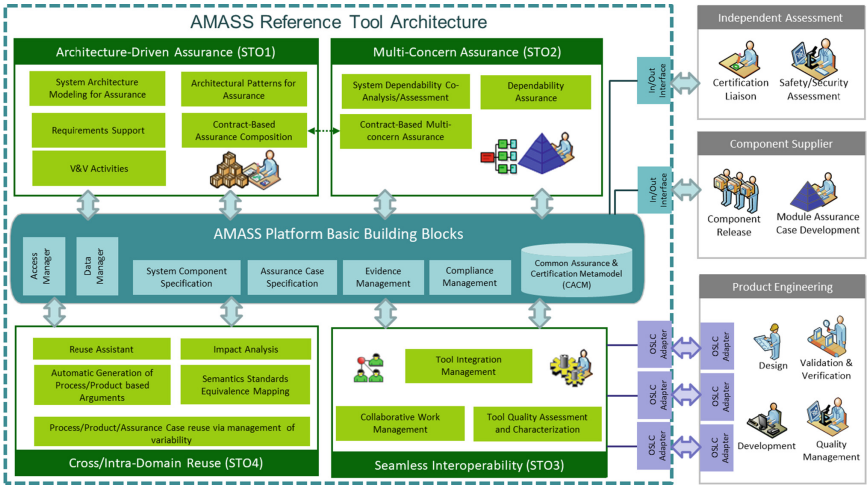

Fig. 1. AMASS Reference Tool Architecture

The **AMASS Tool Platform** (Fig. 2; [6]) is a collaborative tool environment that represents a concrete implementation of the AMASS Reference Tool Architecture with capability for evolution and adaptation. It is released as an open technological solution that integrates and extends different existing open source tools for system modelling and analysis (Papyrus, CHESS, Concerto-FLA), compliance management and argumentation (OpenCert), process engineering (EPF-Composer), variability management (BVR), and traceability (Capra). It is further integrated with over a dozen external tools that provide additional features; usually commercial ones.

The **Open AMASS Community** [7] manages the main project results for maintenance, evolution and industrialization. The Open Community is supported by a governance board and by rules, policies, and quality models. This includes support for AMASS base tools and for extension tools. The OpenCert project of PolarSys/Eclipse [20] hosts the Community.

The achievement of the AMASS goals thanks to these outcomes was demonstrated in the industrial case studies [4]. The achievement varied among the case studies because of their different characteristics (e.g. different base situation) and the different features applied. Videos demonstrating AMASS outcomes are available online [28].

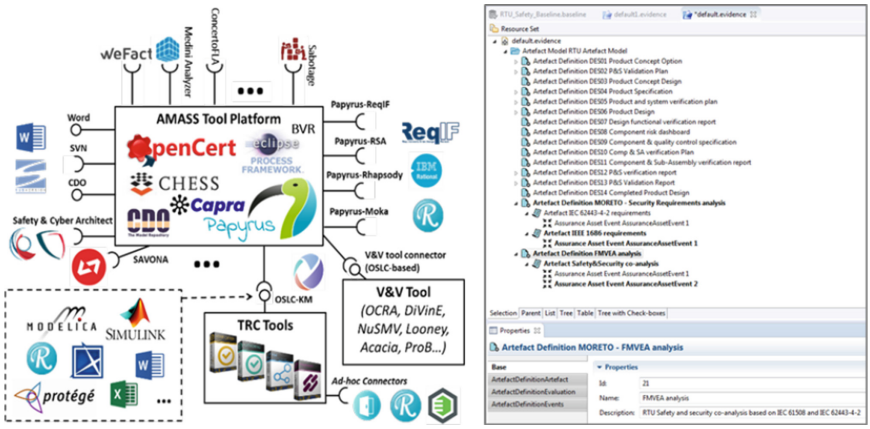

Fig. 2. General view of the AMASS Tool Platform and its ecosystem

5 Conclusion

The AMASS project developed a novel approach for CPS assurance and certification by addressing architecture-driven assurance, multi-concern assurance, seamless interoperability, and cross- and intra-domain reuse of assurance assets. The approach integrated and further developed results from other projects and resulted in three main tangible outcomes: the AMASS Reference Tool Architecture, the AMASS Tool Platform, and the Open AMASS Community. The benefits from using the outcomes were demonstrated in 11 industrial case studies.

We expect that further researchers and practitioners gain interest in AMASS results thanks to the summary presented. They could exploit the results in activities dealing with process or product improvement, mainly for critical systems. New collaborations on assurance and certification could also be created, e.g. around the open community.

We plan to continue working on CPS assurance and certification in the future from the results developed in AMASS. This includes the development of novel solutions for advanced assurance case management and for privacy assurance.

Acknowledgments. The research leading to this paper has received funding from the AMASS project (H2020-ECSEL grant agreement no 692474; Spain's MINECO ref. PCIN-2015-262; Sweden's Vinnova) and the Ramon y Cajal Program (Spain's MICINN ref. RYC-2017-22836; EC's European Social Fund). We are also grateful to all the AMASS partners. Their work and results are summarised in this paper.

References

1. AMASS Project. https://www.amass-ecsel.eu/
2. AMASS Project: Deliverables. https://www.amass-ecsel.eu/content/deliverables
3. AMASS Project: Deliverable 1.6 - AMASS demonstrators (c) (2019)
4. AMASS Project: Deliverable 1.7 - AMASS solution benchmarking (2019)

5. AMASS Project: Deliverable 2.4 - AMASS reference architecture (c) (2018)
6. AMASS Project: Deliverable 2.5 - AMASS user guidance and methodological fwk. (2018)
7. AMASS Project: Deliverable D7.7 - AMASS open source platform (c) (2018)
8. AMASS Project: External Advisory Board. https://www.amass-ecsel.eu/content/external-advisory-board
9. AMASS Project: Organization. https://www.amass-ecsel.eu/content/organization
10. AMASS Project: Publications. https://www.amass-ecsel.eu/content/publications
11. AQUAS Project. https://aquas-project.eu/
12. CHESS Project. http://www.chess-project.org/
13. CP-SETIS Project. https://cp-setis.eu/
14. CRYSTAL Project. http://www.crystal-artemis.eu/
15. de la Vara, J.L., et al.: The AMASS approach for assurance and certification of critical systems. In: Embedded World Conference (2019)
16. Espinoza, H., et al.: Meet the new eclipse-based tools for assurance and certification of cyber-physical systems. Eclipse Newsletter, July 2018. https://www.eclipse.org/community/eclipse_newsletter/2018/july/amass.php
17. Gallina, B., et al.: AMASS: call for users and contributors. Eclipse Newsletter, July 2019. https://www.eclipse.org/community/eclipse_newsletter/2019/july/amass.php
18. Nair, S., et al.: An extended systematic literature review on provision of evidence for safety certification. Inform. Softw. Technol. **56**(7), 689–717 (2014)
19. OMG: System Assurance Task Force. https://www.omg.org/sysa/
20. OpenCert. https://www.polarsys.org/opencert/
21. OPENCOSS Project. http://www.opencoss-project.eu/
22. Parra, E., et al.: Analysis of requirements quality evolution. In: ICSE (2018)
23. PDP4E Project. https://www.pdp4e-project.eu/
24. RobMosys Project. https://robmosys.eu/
25. Ruiz, A., et al.: Architecture-driven, multi-concern, seamless, reuse-oriented assurance and certification of cyber-physical systems. In: SAFECOMP Workshops (2016)
26. SafeCer Project. https://artemis-ia.eu/project/40-nsafecer.html
27. SafeCOP Project. http://www.safecop.eu/
28. YouTube: Opencert. https://youtube.com/channel/UCw_D0l5sDgysEphi6tzzDyw