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

Newsletter #3 - October 2017 https://amass-ecsel.eu/

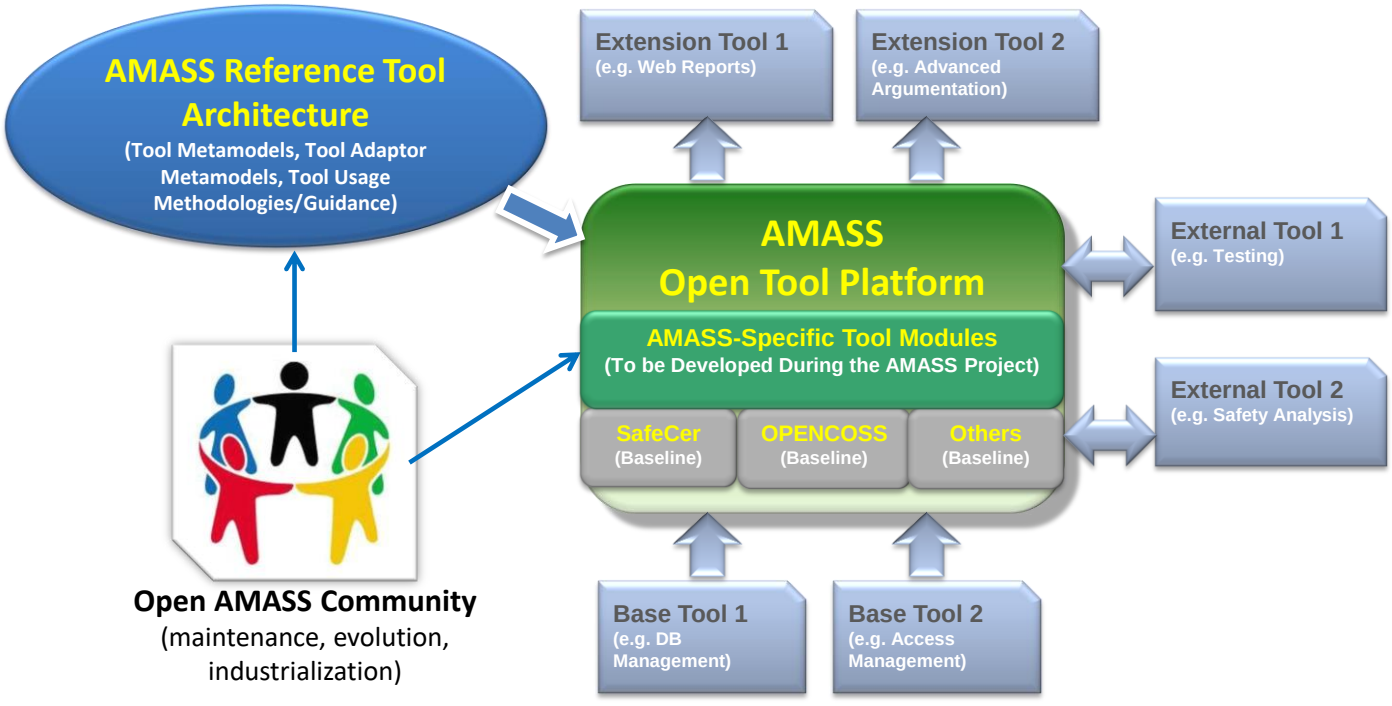
The work on the European-wide open platform and community for assurance and certification of cyber-physical systems is progressing!

AMASS is a H2020-ECSEL project that is creating and consolidating 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.

The AMASS consortium includes the **main stakeholders for CPS assurance and certification**: OEMs, system integrators, component suppliers, system assessors, certification authorities, tool vendors, research institutes, and universities. The main application domains on which AMASS is working are aerospace, automotive, industrial automation, space, and railway. The AMASS project coordinator is TECNALIA Research & Innovation and the named Project Manager is Dr. Huascar Espinoza from the ICT Division.

The ultimate goal of AMASS is to **lower certification costs for CPS** in face of rapidly changing features and market needs. This will be achieved by establishing a novel holistic and reuse-oriented approach for architecture-driven assurance (fully compatible with standards such as AUTOSAR and IMA), multi-concern assurance (for co-analysis and co-assurance of e.g. security and safety aspects), and for seamless interoperability between assurance and engineering activities along with third-party activities (e.g. external assessments and supplier assurance). Society will benefit from the use of **CPS with a higher confidence in their dependability**, for a wide range of applications in transport, manufacturing, healthcare, energy, defence, and communications.

AMASS work is building on the **results from previous** successful EU **projects** such as OPENCOSS, SafeCer, CRYSTAL, and CHESS. The Eclipse Foundation, via the PolarSys initiative, will play a major role towards the creation of the AMASS community.



AMASS Progress during its Third Semester

During the third semester of the project, the AMASS consortium has worked in the following technical activities**: (1) completion of the conceptual approach and design of the second prototyping iteration of the AMASS platform (Prototype P1), (2) definition of the benchmarking and metrics framework to be used by Case Study realizations, and (3) partial implementation of the main functionalities for the second tool platform prototype**.

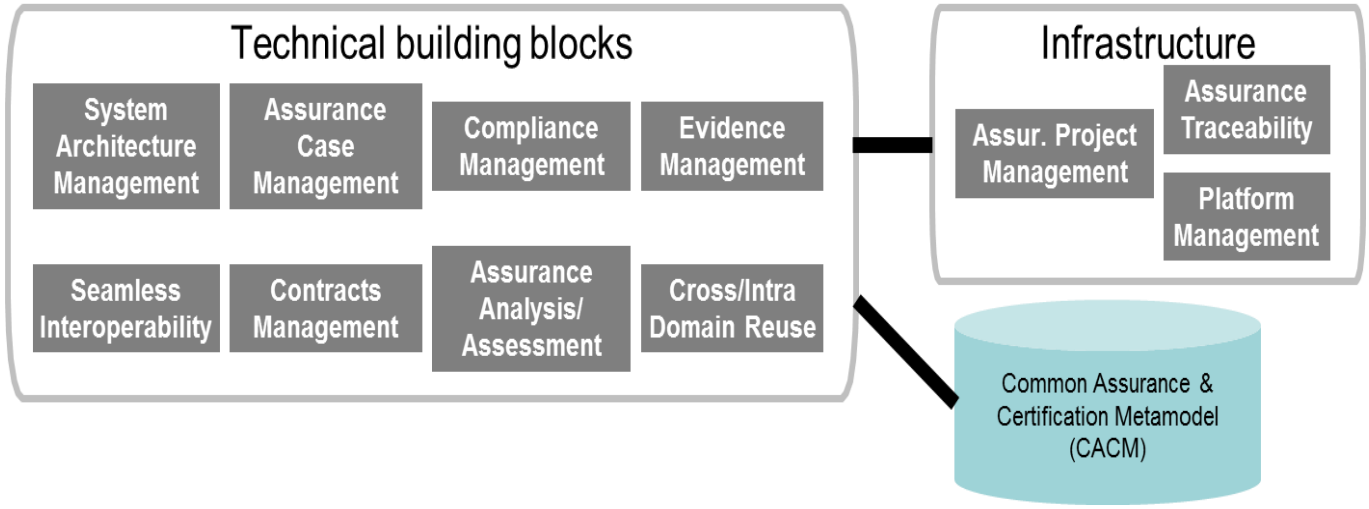
The first aspect was addressed by work packages WP3, WP4, WP5 and WP6. WP3 was focused on **the contract-based design and assurance approach and its integration with functionalities for contract verification and refinement** (supported by the OCRA tool). The functions for V&V-driven assurance were also designed by integrating the system design tool (Papyrus/CHESS) with V&V tools. WP4 designed solutions **for dependability assurance modelling, contract-based multi-concern assurance and system dependability co-analysis and assessment**. The conceptual extensions to the integrated tools OpenCert Assurance Case Editor, CHESS and EPF Composer, and to the external tool WEFACT, were defined. WP5 worked on the update and extension of the functions for seamless interoperability, and on the **design of generic tool integration approaches based on the OSLC technology**. This includes the traceability functionalities by extending the CAPRA tool and connectors with some external tools for analysis. WP6 designed the AMASS approaches and features for cross and intra-domain reuse. Different functionalities have been identified for **semantic standards equivalence mapping, reuse assistant, and product/process/assurance-case line specification**. Within WP6, the global AMASS vision for compliance management was also designed, including new features (such as automatic compliance checking as well as generation of arguments), which have the potential to contribute to increased efficiency.

Regarding the second aspect, **the benchmarking framework of the AMASS approach has been defined** in work package WP1. Partners have focused on creating common metrics that have been derived from the AMASS goals. Case Studies have also specified their specific metrics to be used in the benchmarking phase. Case studies have also been further developed after releasing the first demonstrators in the previous period.

Regarding the third aspect, **the second AMASS Prototype (P1) has been implemented for the main functionalities**. On top of the baseline tools (OpenCert, Papyrus/CHESS and EPF Composer), new functionalities have been added to cover the conceptual designs realised as part of the first aspect mentioned above. These also include functionalities for enhanced process definition, connection with the BVR tool for variability management, improvements on compliance management to filter by criticality levels, and enhanced assurance case patterns specification.

Regarding non-technical activities, dissemination has been again an active area during the third semester of the project. **AMASS has organized several workshops and conferences** (e.g. SASSUR 2017, Euromicro 2017, DECSoS 2017, and SafeComp 2017).

We also organised **the first EAB (External Advisory Board) workshop** and got very useful feedback that is being considered throughout all the AMASS work packages. We collected revised individual exploitation plans, and made progress on standardisation activities.



Second Version of the AMASS Reference Tool Architecture

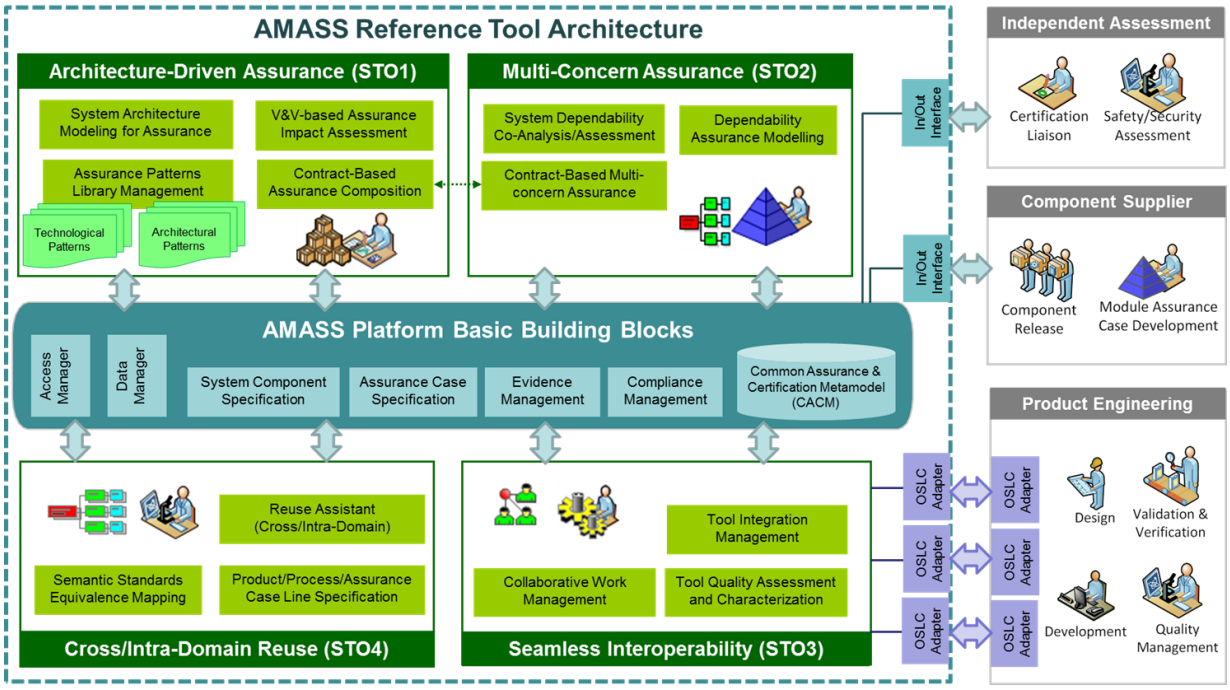
The AMASS Reference Tool Architecture (**ARTA**) is a conceptual entity that embodies a **common set of tool interfaces/adaptors, working methods, tool usage methodologies, and protocols** that will allow any stakeholder of the assurance and certification process to seamlessly integrate their activities (e.g., product engineering, external/independent assessment, component/parts supply) into tool chains adapted to the specific needs of the targeted CPS markets. The second ARTA version has been finished in September 2017. It has been based on the first version prepared by November 2016 and will evolve into a final version by May 2018.

ARTA proposes a specification for a collaborative tool environment, which aims to support CPS assurance and certification activities. **ARTA builds upon OPENCOSS, SafeCer, and CHESS conceptual, modelling and methodological frameworks**. ARTA not only connects project achievements but also extends them for architecture-driven and multi-concern assurance, as well as for further cross-domain and intra-domain reuse capabilities and seamless interoperability mechanisms. In the second iteration, **the main evolutions have been to (1) improve the functionalities of the basic building blocks** solving some problems provided as feedback during the validation of the first prototype, **and (2) provide more information about the interactions between these basic building blocks**. We have also started providing some of the functionalities envisioned in the "advanced building blocks".

The stakeholders of the ARTA can be divided into **Managers** (Project Manager, Assurance Manager, and IT Manager), **Engineers** (Development Engineer, Process Engineer, Assurance Engineer, Safety Engineer, and Security Engineer), **and Assessors** (Assurance Assessor, Independent Assessor, and Internal Assessor). The ARTA functional blocks correspond to **overall infrastructure support** (Assurance Project Management, Platform Management, and Assurance Traceability) **and specific technical support** (System Architecture Management, Assurance Case Management, Compliance Management, Evidence Management, Seamless Interoperability, Contract Management, Assurance Analysis/Assessment, and Cross/Intra-Domain Reuse).

Use cases have been specified for each functional block to represent the **logical view** of the ARTA. For example, for Assurance Case Management, seven use cases have been specified for Assurance Case Edition: Define and navigate an assurance case structure, Develop claims and links to evidence, Apply argument patterns, Reuse an argument module, Semi-automatic generation of product arguments, Automatic generation of process arguments, and Monitor status of argumentation. The functional blocks have also been decomposed into finer-grained components to define the **structural view** of the ARTA. For example, the components for Contract Management are Contract editor and Contract-based multi-concern assurance. Finally, the **interactional view** has also been created. An example of interaction corresponds to those necessary for Multi-concern co-analysis/assessment. The involved components are Assurance case editor, Co-analysis/assessment, and Evidence editor, as an assurance analysis could be defined while creating an assurance and the analysis results could be stored as evidence information in the AMASS Tool Platform.

Tool vendors or other stakeholders could either implement the AMASS platform following the information provided in the architectural views or use the functionalities and connect with their own external tools.



AMASS Meetings

There have been several meetings during the last six months in AMASS. Among them, the main meetings have been the First EC Project Review, the First EAB workshop, and the Fourth General Meeting.

The **Project Review** was held on June 9th, 2017, at ECSEL premises in Brussels. The expert external reviewers were Philippe Baufreton, from SAFRAN Electronics & Defense, and Christopher Johnson, from the University of Glasgow. The Project Officer is Berta Ferrer. The review team considered that the project is progressing very well and appreciated the clear baseline established, based on results from previous projects. As main suggestions, future deliverables could further explain the differences of interpretation of standards among member states and pay greater attention to the difficulty in defining CPS boundaries.

The **EAB workshop** was held in Trento, Italy, on September 11th, at FBK premises. This board consists of international experts in critical-system assurance and certification, from different domains and with different roles. The members suggested that AMASS needs to pay special attention to: (1) the use of contracts for architecture-driven assurance and argumentation; (2) how to unify processes for safety & security co-assurance; (3) the provision of clear information about the objectives and limitations of the tool integration solutions, and; (4) the extent to which certain domains pose additional constraints for reuse (e.g. through product lines). A report is available online.

Regarding the **General Meeting**, the AMASS consortium gathered together in Brno on September 27th- 29th at Honeywell premises. The discussions on technical aspects included the areas that will be covered in the case studies for the second prototype of the AMASS Tool Platform (prototype P1), how to integrate the different metamodels and tools of the Platform, what type of information should be provided as methodological guidance for AMASS results, and the overall plan for implementation finalisation, validation, and evaluation of the prototype P1.

SASSUR & SAFECOMP 2017

SASSUR 2017, the **6th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems**, was held on September 12, 2017, in Trento, Italy, as a SAFECOMP 2017 workshop. SASSUR is one of the key events for scientific dissemination in AMASS, and the project supported the organisation of the workshop.

Over 25 people attended the workshop, including people from academia and from industry. Among the AMASS partners, Alejandra Ruiz (TEC) and Jose Luis de la Vara (UC3) participated in the workshop as co-organisers, and Helmut Martin (VIF) and Irfan Sljivo (MDH) presented a paper each. The keynote speaker was Johnny Marques, Principal Product Development Engineer and responsible for Software Quality Assurance at Embraer. Embraer produces commercial, military, executive and agricultural aircrafts and provides aeronautical services. Johnny presented a set of metrics to assess and monitor compliance with RTCA DO-178C, explaining how they have been developed and how they are used at Embraer.

In addition, AMASS partners participated in other SAFECOMP 2017 (**36th International Conference on Computer Safety, Reliability and Security**) events.

SAFECOMP 2017 was organized by the AMASS partners Erwin Schoitsch (AIT) and Stefano Tonetta (FBK). Many other AMASS partners participated in the conference, including B&M, CEA, MDH, ViF, and TEC. The conference was co-located with four workshops, including SASSUR and DecSOS (organized by AIT; co-chair Erwin Schoitsch), and with the 5th International Symposium on Model Based Safety Assessment (IMBSA 2017) organized by FBK (co-chair Marco Bozzano). Barbara Gallina (MDH) was the chair of the "Safety and Security" session at the main conference, which hosted interesting discussions on co-engineering of safety and security. She also presented the EWICS-SEC sub-group and its current agenda during the session dedicated to EWICS.

AMASS participation in European events

The AMASS consortium has continued its extensive dissemination activity during the last months, such as the preparation of publications at different conferences and workshops. The partners have also participated in several European events.

The **Digital Innovation Forum** (DIF) is an international industry-driven event that focuses on Digital Innovation in Europe and beyond. DIF 2017 took place on 10 & 11 May 2017 in Amsterdam, and the global software innovation community participated in the event: large industry, SMEs, academics, start-ups, investors, representatives from funding agencies, and public authorities. The first edition of DIF was dedicated to the 'Digital Transformation. ARTEMIS and ITEA organised the event.

The **ECSEL Symposium** too place in Malta on 13 & 14 June 2017. A wide range of European and global stakeholders in the Electronics Components and Systems field, including Industry, Research and Financial Communities, European, National and Regional decision-makers, and international partners, attended the event. The Symposium provided opportunity and space for the ECSEL funded projects to present their progress and results to date, to disseminate the scientific and technological achievements, and to cast light on their contributions to the programme.

EclipseCon France is the Eclipse Foundation's event for the French and entire European Eclipse community. It gives opportunities to learn, explore, share, and collaborate on the latest ideas and information about Eclipse technologies, the Eclipse Working Groups, and Eclipse member companies. In 2017, the conference was held in Toulouse on 21 & 22 June 2017. AMASS participated in the Research Corner, where H2020 and ITEA projects were presented.

Participation in such a kind of events, especially at industry-targeted events, is expected in the future to continue making relevant stakeholders aware of AMASS objectives and results.

Recent AMASS Presence at Events (selection)

DIF 2017: Digital Innovation Forum. May 10th-11th, 2017, Amsterdam (Netherlands).

ICSE 2017: 39th International Conference on Software Engineering. May 20th-28th, 2017, Buenos Aires (Argentina).

5th Scandinavian Conference on System & Software Safety. May 22nd-23rd, 2017, Stockholm (Sweden).

ECSEL Symposium 2017. June 13th-14th, 2017, Malta.

EclipseCon France 2017. June 21st-22nd, 2017, Toulouse (France).

INCOSE Symposium 2017: 27th Annual INCOSE International Symposium. July 15th-20th, 2017, Adelaida (Australia).

RE 2017: 25th International Requirements Engineering Conference. September 4th-8th, 2017, Lisbon (Portugal).

EuroAsiaSPI 2017: European Conference on Systems and Software Process and Product Improvement and Innovation. September 6th-8th, 2017, Ostrava (Czech Republic).

IWES 2017: 2nd Italian Workshop on Embedded Systems. September 7th-8th, 2017, Rome (Italy).

IMBSA 2017: 5th International Symposium on Model Based Safety Assessment. September 11th-13th, 2017, Trento (Italy).

SAFECOMP 2017: 6th International Conference on Computer Safety, Reliability and Security. September 12th-15th, 2017, Trento (Italy).

DECSoS 2017: 12th International Workshop on "Dependable Smart Embedded and Cyber-physical Systems and Systems-of-Systems". September 12th, 2017, Trento (Italy).

Safe Comp 2017

Recent AMASS Publications (selection)

Carlan, C., Gallina, B., Kacianka, S., Breu, R.: *Arguing on Software-level Verification Techniques Appropriateness*. 36th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2017)

de la Vara, J.L., Marín, B., Ayora, C., Giachetti, G.: *An Experimental Evaluation of the Understanding of Safety Compliance Needs with Models*. 36th International Conference on Conceptual Modeling (ER 2017)

Juez, G., Amparan, E., Lattarulo, R., Ruiz, A., Perez, J., Espinoza, H.: *Early Safety Assessment of Automotive Systems Using Sabotage Simulation-Based Fault Injection Framework*. 36th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2017)

Martin, H., Bramberger, R., Schmittner, C., Ma, Z., Gruber, T., Ruiz, A., Macher, G.: *Safety and Security Co-engineering and Argumentation Framework*. 6th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR-2017)

Montecchi, L., Gallina, B.: *SafeConcert: a Metamodel for a Concerted Safety Modeling of Socio-Technical Systems*. 5th International Symposium on Model-Based Safety and Assessment (IMBSA 2017).

A complete publication list is available on the AMASS website: https://amass-ecsel.eu/content/publications

Public AMASS Deliverables (until September 2017; selection)

D1.1 - Case studies description and business impact

D1.3 - Evaluation framework and quality metrics

D1.4 - AMASS demonstrators (a)

D2.1 - Business cases and high-level requirements

D2.6 - Integrated AMASS platform (a)

D3.5 - Prototype for architecture-driven assurance (b)

D4.1 - Baseline and requirements for multiconcern assurance

D4.4 - Prototype for multiconcern assurance (a)

D5.4 - Prototype for seamless interoperability (a)

D6.4 - Prototype for cross/intra-domain reuse (a)

D7.1 - External advisory board and industrial adoption program roadmap

D7.4 - AMASS open source platform marketing and outreach plan

D7.5 - AMASS open source platform provisioning and website (a)

D7.3 - AMASS open source platform project proposal

D8.2 - Exploitation Plans and Initial Market Megatrends Analysis (a)

D8.6 - Dissemination and Training Progress (a)

D8.9 - Standardization Survey

A complete deliverable list is available on the AMASS website: https://amass-ecsel.eu/content/deliverables

ECSEL Joint Undertaking

European Commission

H2020-ECSEL-2015
Research and Innovation Action
Grant agreement no. 692474