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

Newsletter #5 - October 2018 https://amass-ecsel.eu/ @AMASSproject

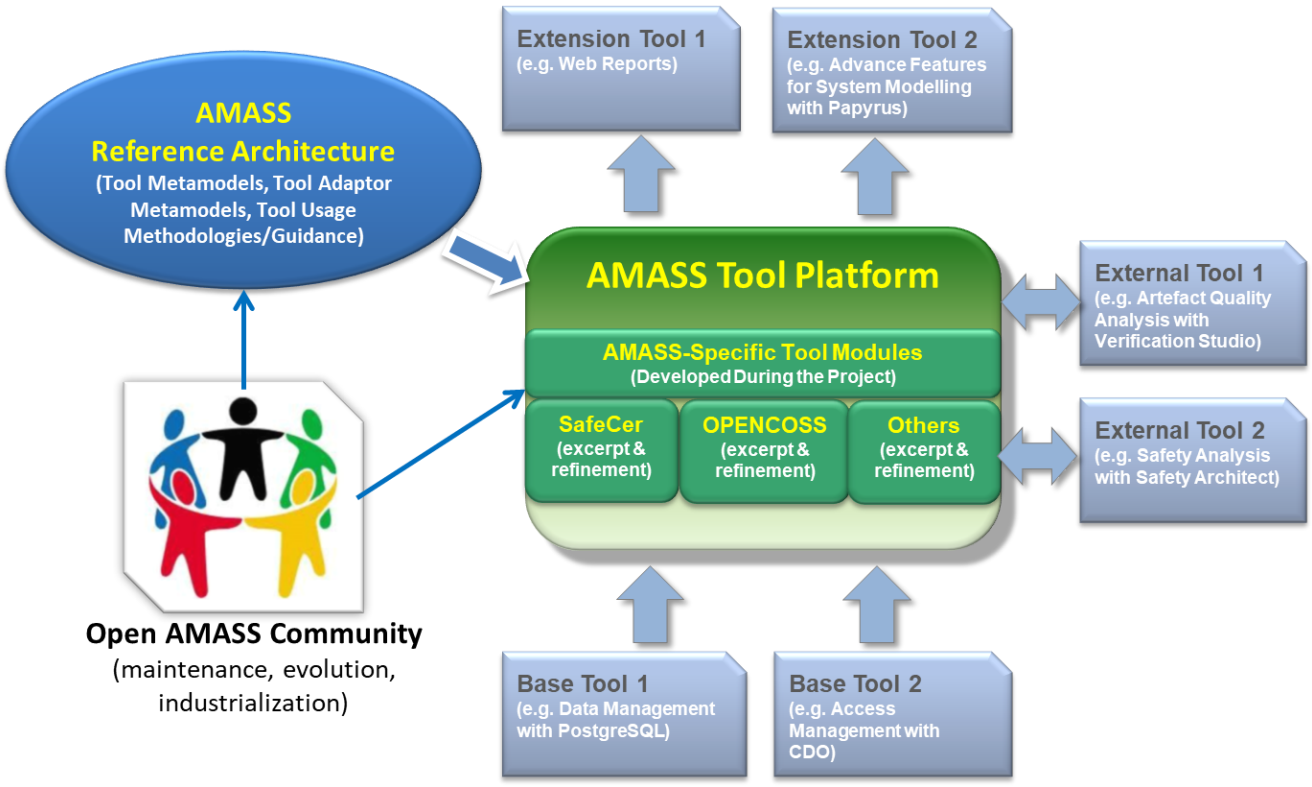
The work on the European-wide open platform and community for assurance and certification of cyber-physical systems is close to its finalization!

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. Alejandra Ruiz from the ICT Division.

The ultimate goal of AMASS is to **lower the certification costs for CPS** in face of rapidly changing features and market needs. This has been achieved by establishing a novel holistic and reuse-oriented 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), 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, is playing a major role towards the creation of the AMASS community.



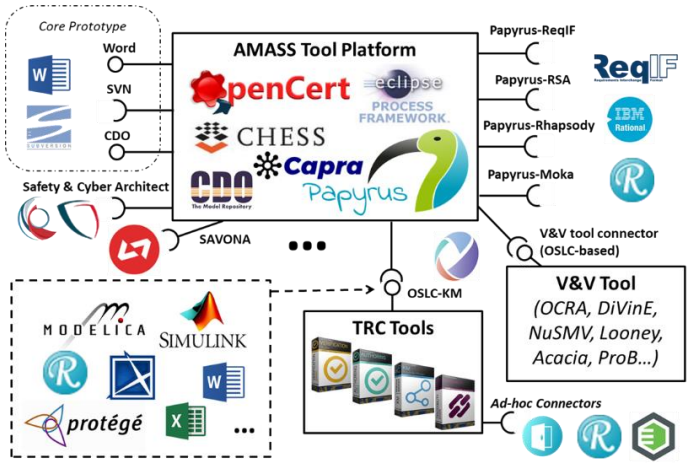
AMASS Progress between March 2018 and September 2018

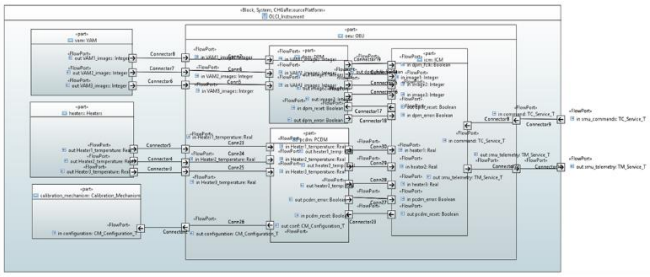
During the fifth semester of the project, the technical work by the AMASS consortium has strongly focused on the design and implementation of the third version of the AMASS Tool Platform (Prototype P2).

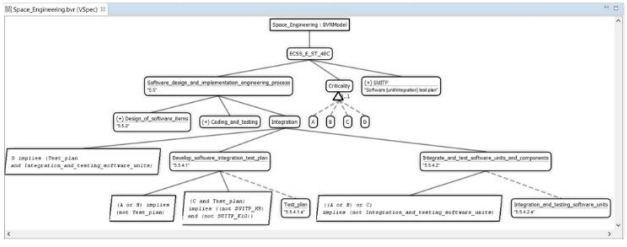
For Architecture-Driven Assurance, the new features of the **AMASS Prototype P2** have aimed to ensure that the provided functionalities include support for both (1) the left-hand side of the V-model at high- and low-level design and (2) the corresponding V&V activities on the right-hand side. For example, extended support has been provided for nominal and fault behavioural components specification, and to trace the elements of the architecture to assurance cases and to evidence and process data. The new results for Multi-Concern Assurance include extensions concerning the automatic generation of argument fragments for dependability assurance, the integration of safety and security analysis tools for system dependability co-analysis and co-assessment, and the management of multi-concern argument fragments for contract-based multi-concern assurance. Seamless Interoperability has been improved by largely extending the set of tools with which the AMASS Tool Platform can exchange data with, including commercial tools commonly used in CPS engineering and covering tools from practically all CPS lifecycle phases, and by providing new means for access management and data management towards enhanced collaborative work. Regarding cross- and intra-domain reuse, reuse assistance now exploits data mining and semantic technologies to identify reusable assets, new features have extended the available support for automatic argument generation and for product-, process-, and argument-related reuse via management of variability, and compliance checking uses formal approaches for compliance analysis of processes against standards.

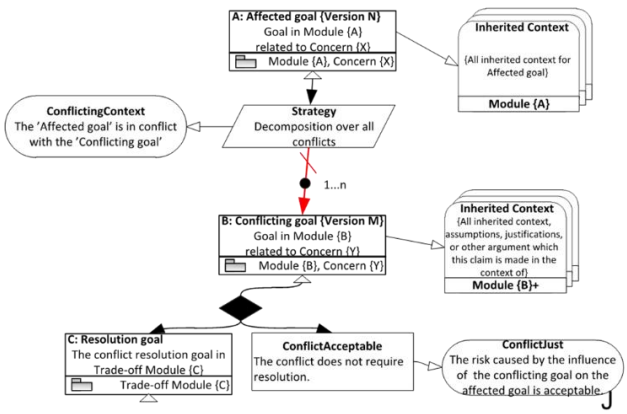
Deliverables **D3.3, D4.3, D5.3 and D6.3** describe the conceptual design for Prototype P2, **D3.6, D4.6, D5.6 and D6.6** document the implementation results, and deliverables **D3.8, D4.8, D5.8 and D6.8** present the methodological guidance to use the results. In relation to use by practitioners, **D1.6** will present the application of the results on the industrial case studies and **D1.7** the benchmarking of the results. The analysis of the features that will be deployed in each case study is currently under finalisation.

Regarding **non-technical aspects**, the AMASS Open Platform (https://www.polarsys.org/opencert/), composed of OpenCert, CHESS and EPF Composer and hosted by Polarsys/Eclipse, has continued its development and has been published. The Platform website has been updated, including getting started material to help the adoption of these open source tools, and an article about the AMASS Open Platform has been published in the Eclipse Foundation newsletter, which counts 250,000+ subscribers. Feedback has been collected from the EAB members at a workshop in September 2018 in Västerås, September. This workshop was held just before the SAFECOMP 2018 conference, which has been one of the main events at which AMASS partners have conducted dissemination activities, including the DECSoS, SASSUR, and WAISE workshops. Finally, the analysis of the trends and market needs that the project intends to address has been updated for exploitation-targeted purposes, and contributions to several functional safety standards and their related complementary cybersecurity standards have been made for standardisation.









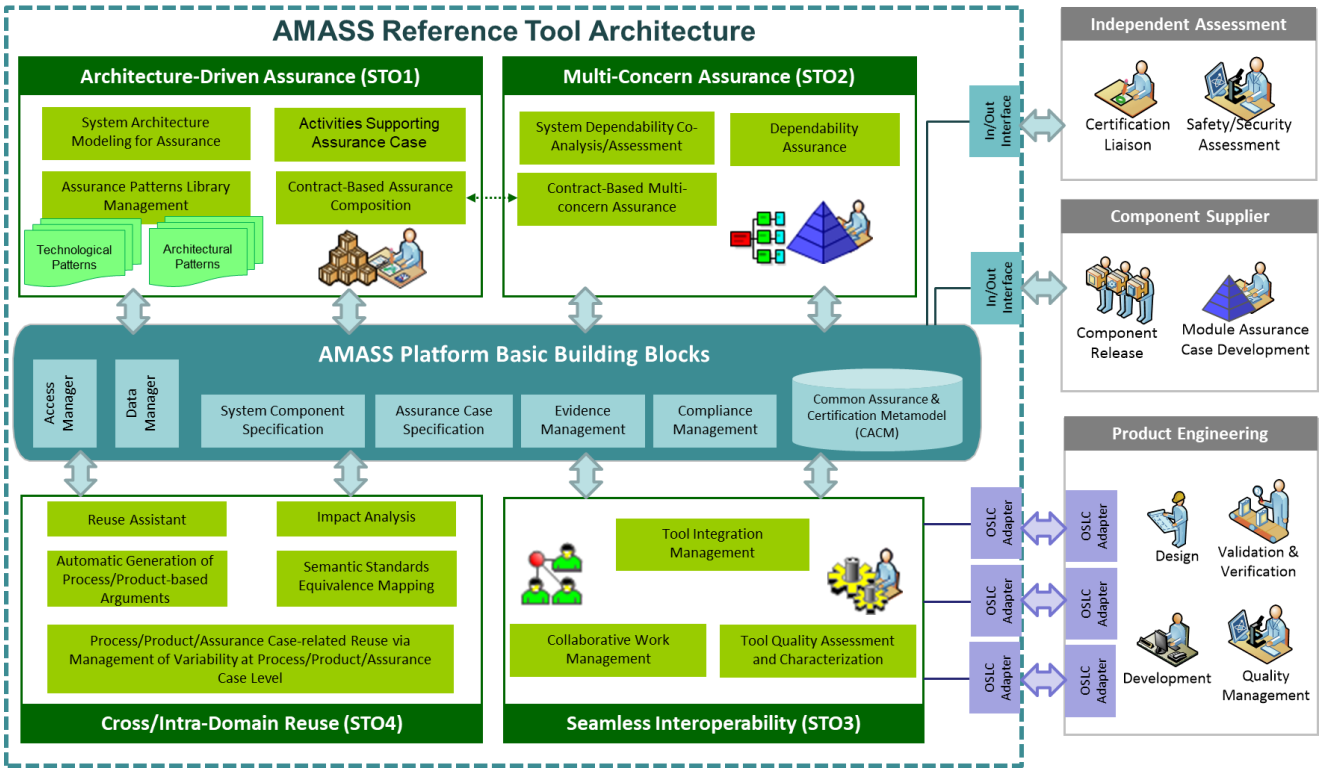
Final Version of the AMASS Reference Tool Architecture

The AMASS consortium has been working on the development of the AMASS Reference Tool Architecture (ARTA) since the beginning of the project. The ARTA is specified as **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, and component/parts supply) into tool chains adapted to the specific needs of the targeted CPS markets.

The final building blocks of the ARTA are:

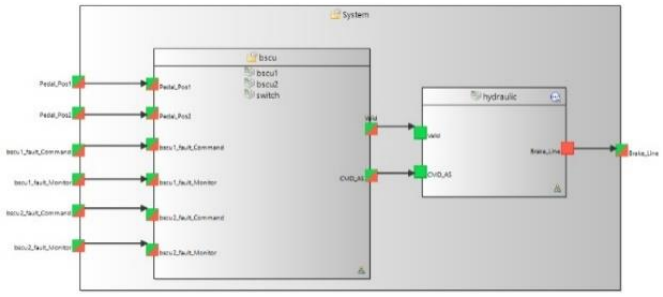
- The basic building blocks are **System Component Specification, Assurance Case Specification, Evidence Management, Compliance Management, Access Manager, and Data Manager**. In addition, the Common Assurance and Certification Metamodel (**CACM**) includes the concepts and data entities to manage in an assurance project according to the AMASS approaches.
- For *Architecture-Driven Assurance*, **System Architecture Modelling for Assurance, Architectural Patterns for Assurance, Requirements Support, Contract-Based Assurance Composition, and V&V Activities** enable the integration of assurance and certification activities with CPS development activities, including specification and design and guaranteeing that emerging behaviour does not interfere with the whole system assurance.
- For *Multi-Concern Assurance*, **System Dependability Co-Analysis/Assessment, Dependability Assurance, and Contract-Based Multi-Concern Assurance** target at supporting the development of assurance cases, co-assessment, and contract-based assurance addressing multiple system characteristics (mainly safety and security, but also other dependability aspects such as availability, robustness and reliability).
- For *Seamless Interoperability*, **Tool Integration Management, Collaborative Work Management, and Tool Quality Characterisation and Assessment** provide and open and generically applicable approach to ensure the joint contribution of different tools and stakeholders towards CPS assurance and certification.
- For *Cross- and Intra-Domain Assurance Reuse*, **Reuse Assistance, Impact Analysis, Automatic Generation of Product- and Process-Based Arguments, Semantic Standards Equivalence Mappings, and Product-, Process-, and Assurance Case-Related Reuse via Management of Variability** aim systematic reuse based on a conceptual framework to specify and manage assurance and certification assets.

The implementation of the basic blocks is mainly based on results from prior projects (CHESS, OPENCOSS, SafeCer…). The functionality for the rest of the building blocks have mostly been developed during AMASS and include both open source solutions (e.g. variability management with BVR) and proprietary tools (e.g. V&V activities with Verification Studio by The REUSE Company). **The AMASS Tool Platform corresponds to the integration of the different open source solutions adopted or developed**, whereas the AMASS ecosystem corresponds to this open source solution together with the commercial solutions built on top of the Platform or that interact with it.



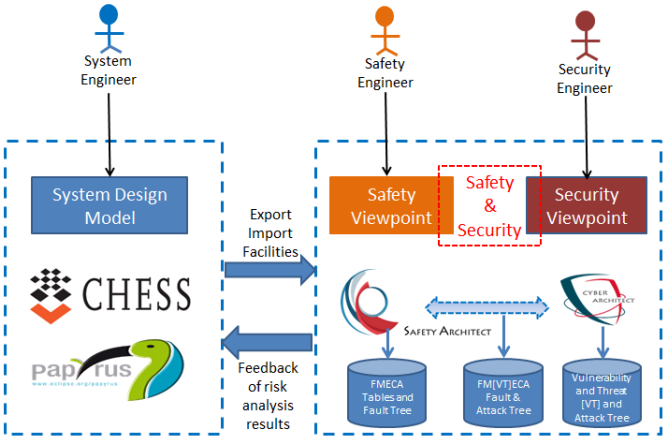
Safety Architect and Cyber Architect in AMASS

The AMASS consortium has chosen to build the AMASS Tool Platform around existing open technologies, e.g OpenCert and Papyrus. The AMASS Tool Platform also provides interoperability features with other tools used by the AMASS consortium to address the project objectives, such as multi-concern assurance. System dependability co-analysis/co-assessment, and particularly **system safety and security co-analysis**, is an integral part of multi-concern assurance aspects.



Safety Architect and Cyber Architect are ALL4TEC tools integrated with the AMASS Tool Platform for system safety and security co-analysis. The tools provide a comprehensive way to **reduce the gap between safety and security analyses and system architecture assurance**. From CHESS models of a system architecture, Safety Architect allows performing a local FMEA of each architecture component and automatically deduces system-global FMEA/FMECA tables and fault trees of identified events. It can be combined with company-dedicated FTA tools, such as FaultTree+ or Arbre Analyste for quantitative risk analysis. In addition, thanks to the security viewpoint in Safety Architect, an assurance engineer can use the results of security analysis realized in Cyber Architect (e.g., vulnerabilities and threats analysis) to co-analyse safety and security risks and to generate merged safety and security artefacts, such as Failure Mode, Vulnerabilities and Effect Analysis (FMVEA).

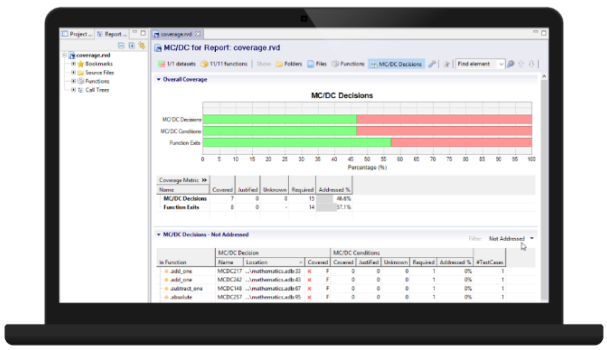
The **integration scenario between the AMASS Tool Platform + CHESS tools and the Safety Architect and Cyber Architect tools** for safety and security co-analysis is presented below.



Collaboration between Rapita and OHB for Code Coverage Analysis

The AMASS partners are collaborating in the execution of activities for CPS assurance and certification. This includes the study of how different technologies can make the activities more efficient. An example is the **work by Rapita and OHB Sweden for code coverage analysis in accordance with DO-178C**.

As part of AMASS, Rapita has worked with OHB Sweden to **improve the efficiency of structural coverage analysis testing for an Attitude Orbital Control System** used in the Electra satellite, while supporting the future adoption of a DO-178C certification processes. OHB Sweden was using an open-source coverage analysis tool to provide coverage data, for which no qualification support is available. Rapita was asked to provide a more efficient coverage analysis solution, also integrated with the existing code generation and test environment and with a tool qualification path already in place.



Rapita has worked with OHB Sweden to integrate RapiCover into the existing build and test environment to collect structural coverage data at DO-178C Level B while tests are run on source library functions. Because of the flexible architecture of both RapiCover and OHB Sweden's development environment, integration was accomplished while making minimal changes to the build system.

The benefits of the solution include a **40% reduction in end-to-end testing time, justifications for tracking manual analysis of coverage, and full support for analysis of C code**.

AMASS Meetings

During the last six months, AMASS partners have participated in the second project review by ECSEL and organised a workshop with the members of the External Advisory Board (EAB).

The **second AMASS project review** was held on June 7th, in Brussels. As in the first review, the expert external reviewers were Philippe Baufreton, from SAFRAN Electronics & Defense, and Christopher Johnson, from the University of Glasgow.

The review team considered that the project is progressing very well. As main recommendations, **special attention must be paid to the industrial case studies** (training needs, inclusion of policy makers, and further consideration of security, of cross-domain, and of cyber-physical aspects aspect)**, tool evaluation criteria for inclusion in the AMASS toolset, and how to facilitate the industrial adoption of the AMASS Tool Platform**.

The **second workshop with the members of the AMASS EAB** was held in Västerås, Sweden, on September 17th, hosted by MDH. This board consists of international experts in critical-system assurance and certification.

The EAB members expressed their vision regarding **how usage scenarios could be improved to get impact in users, how to improve the AMASS user guidance, the conceptual and implementation approach underlying the AMASS Tool Platform, industry usage opportunities for specific features, and the soundness of the AMASS community building, exploitation, and dissemination strategies**.

Last but not least a meeting with the SafeCop ECSEL project (http://www.safecop.eu/) was organised.

SASSUR 2018

The **7th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems**, was held on September 18th, 2018, in Västerås, Sweden, as a SAFECOMP 2018 workshop. SASSUR is one of the key events for scientific dissemination in AMASS, and the project supported the organisation of the workshop.

Over 30 people attended the workshop, including people from academia and from industry. Alejandra Ruiz and Garazi Juez (TEC) and Jose Luis de la Vara (UC3) participated in the workshop as co-organisers, and Martin Skoglund (SPS) presented a paper. Several AMASS EAB members were present too.

The keynote speaker was Thor Myklebust, Researcher and Certification Manager at SINTEF, Norway. With the title **"Evolutionary development and frequent releases of safety systems"**, Thor presented their recent work on the application of agile methods for the development and assurance of software-intensive critical systems. This work includes SafeScrum and the so called agile safety case.

As a novelty for this edition, each paper had an assigned discussant and the time for questions & answers and discussion was extended. The main topics of the six accepted papers are **the comparison of safety analysis techniques, the comparison of safety analysis techniques and security analysis ones, risk estimation for automated vehicles, analysis of generic-component integration in automated driving vehicles, synergies between safety assurance practices and cybersecurity assurance ones, and challenges for assuring complex and large safety-critical systems**.

A panel on trends and needs for future assurance of safety-critical systems was also organised. Laurent Fabre, Thor Myklebust, and Timo Varkoi were the panellists. They are members of the AMASS EAB.

It is expected that **a new edition of SASSUR will be held next year at SAFECOMP 2019** in Turku, Finland.

Recent AMASS Presence at Events (selection)

ECSEL JU Symposium 2018. Brussels, Belgium. June 19-20, 2018

EclipseCon France 2018. Toulouse, France. June 13-14, 2018

EUROSPACE-DASIA 2018 - Data Systems in Aerospace 2018. Oxford, UK. May 29-31, 2018

EuroSPI-2018 - 25th European Conference Systems, Software and Services Process Improvement. Bilbao, Spain. September 5-7, 2018

ICSE 2018 - 40th International Conference on Software Engineering. Gothenburg, Sweden. May 27-June 3, 2018

ICSR 2018 - 17th International Conference on Software Reuse. Madrid, Spain. May 21-23, 2018

INCOSE Symposium 2018. Washington DC, USA. July 7-12, 2018

QUATIC 2018 - 11th International Conference on the Quality of Information and Communications Technology. Coimbra, Portugal. September 4-7, 2018

SAFECOMP 2018 - 37th International Conference on Computer Safety, Reliability and Security. Västerås, Sweden. September 18-21, 2018

SEFM 2018 - 16th International Conference on Software Engineering and Formal Methods. Toulouse, France. June 27-29, 2018

SPLC 2018 - 22nd International Systems and Software Product Line Conference. Gothenburg, Sweden. September 10-14, 2018

Recent AMASS Publications (selection)

Álvarez-Rodríguez, J.M., Mendieta, R., de la Vara, J.L., Fraga, A., Llorens, J.: *Enabling system artefact exchange and selection through a Linked Data layer*. J. of Universal Computer Science (accepted paper)

Adedjouma, M., Smaoui, A.: *Model-Based Computer-Aided Monitoring for ISO26262 Compliant Systems*. Int. Workshop on Software Certification (WoSoCer 2018)

Alaña, E., Herrero, J., Urueña, S., Macioszek, K., Silveira, D.: *A Reference Architecture for Space Systems.* 12th European Conf. on Software Architecture (ECSA 2018)

Bendík, J., Černá, I., Beneš, N.: *Recursive Online Enumeration of All Minimal Unsatisfiable Subsets*. 16th International Symposium Automated Technology for Verification and Analysis (ATVA 2018)

Castellanos Ardila, J. P., Gallina, B., Ul Muram, F.: *Enabling Compliance Checking against Safety Standards from SPEM 2.0 Process Models*. 44 Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2018)

Espinoza, H., de la Vara, J.L., Juez, G., Martinez, C., Gallina, B., Puri, S., Mazzini, S., Blondelle, G.: *Meet the new Eclipse-based tools for Assurance and Certification of Cyber-Physical Systems*. Eclipse Newsletter July 2018

Javed, M. A., Gallina, B.: *Safety-oriented Process Line Engineering via Seamless Integration between EPF Composer and BVR Tool*. 22nd International Systems and Software Product Line Conference (SPLC 2018)

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

ECSEL Joint Undertaking

European Commission

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