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

Newsletter #6 – April 2019 https://amass-ecsel.eu/ @AMASSproject

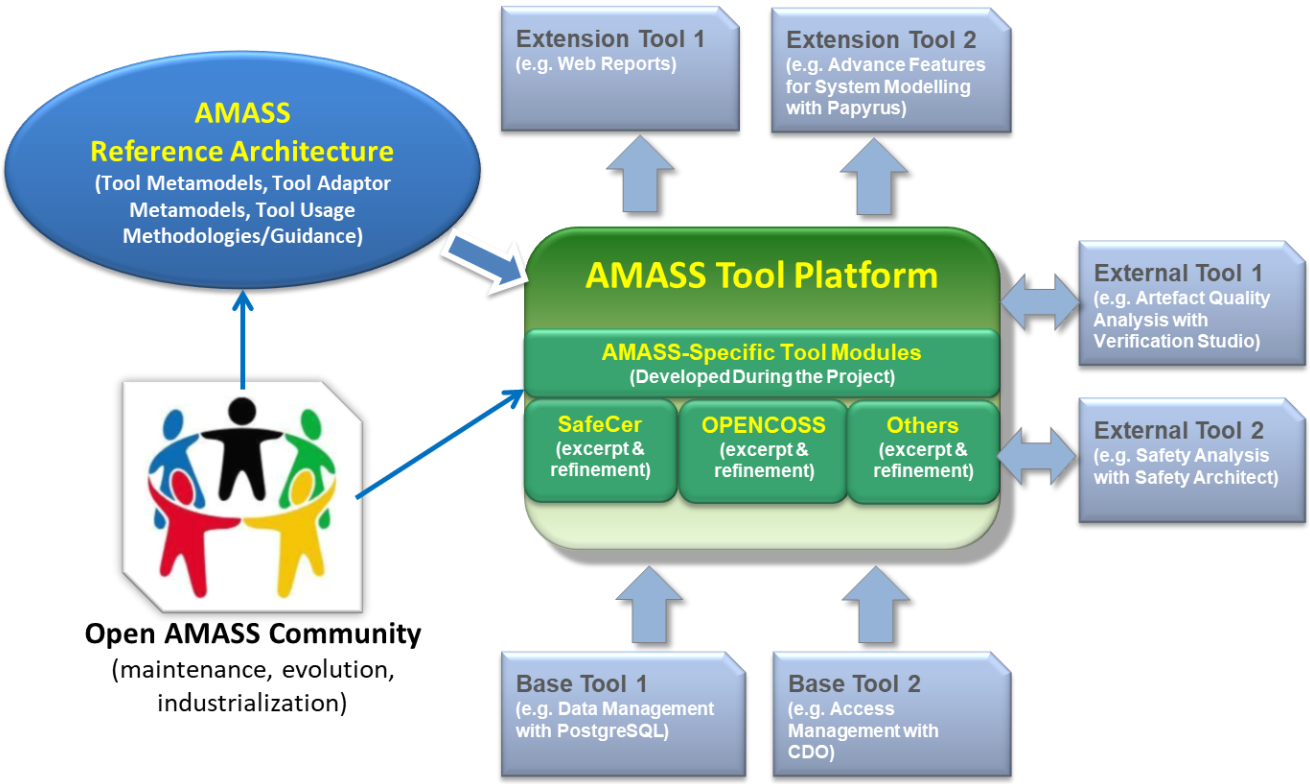
The work on the European-wide open platform and community for assurance and certification of cyber-physical systems has finished!

AMASS is a H2020-ECSEL project that has 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.

The AMASS consortium has included 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 has worked are aerospace, automotive, industrial automation, space, and railway. The AMASS project coordinator has been TECNALIA Research & Innovation and the named Project Manager has been Dr. Alejandra Ruiz from the ICT Division.

The ultimate goal of AMASS was 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.

The AMASS work has built on the **results from previous** successful EU **projects** such as OPENCOSS, SafeCer, CRYSTAL, and CHESS. The Eclipse Foundation, via the PolarSys initiative, has played a major role towards the creation of the AMASS community for maintenance and sustainability of project results.



AMASS Progress during the Last Semester of the Project

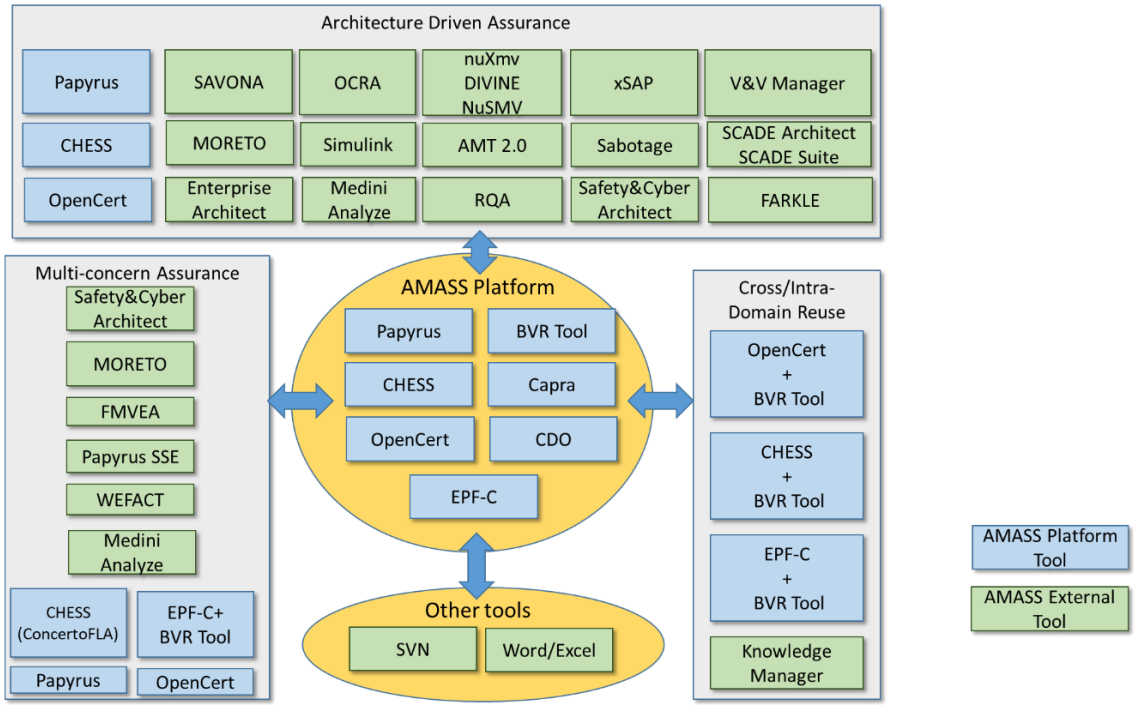
During the sixth semester of the project, the technical work by the AMASS consortium has strongly focused on the validation and finalisation of the final version of the AMASS Tool Platform (Prototype P2) and on the application and evaluation of AMAS results in the different industrial case studies (CS).

The **validation** results have been reported in **D2.8** (Integrated AMASS platform (c)) **and D2.9** (AMASS platform validation). Among these results, all the **test cases** run on the AMASS Tool Platform can be regarded as passed, **tool qualification** aspects have been explained, and the **TRL** (Technology Readiness Level) of the main AMASS tool components has been determined: 7 for Papyrus Modelling, 4 for Papyrus new features, 6 for the CHESS plug-in for Papyrus, 5 for CHESS new features, 4 for OpenCert, 5 for OpenCert new features, 7 for EPF Composer, and 5 for BVR.

D1.6 (AMASS demonstrators (c)) and **D1.7** (AMASS solution benchmarking) present the **application and** the **evaluation** of AMASS results: CS1 - **Industrial and Automation Control Systems** has worked on Managing compliance with IEC 61508 and 62443 and Safety and security co-assessment; CS2 - **Advanced Driver Assistance Function with Electric Vehicle Sub-System** has addressed Reuse of safety artefacts within a product family; CS3 - **Collaborative Automated Fleet of Vehicles** has tackled Safety assessment by model-based safety analysis and contracts and Process for development of collaborative vehicle functions; CS4 - **Design and Safety Assessment of On-Board SW Applications in Space Systems** has dealt with Architectural design; CS5 - **Railway Platform Screen Doors Controller** has focused on Generation of Frama-C asserted C code from B models and System-level modelling; CS6 - **Automatic Train Control Formal Verification** has applied Assurance project creation, System design, V&V and dependability assessment, Evidence and Compliance management; CS7 - **Safety Assessment of Multi-Modal Interactions in Cockpits** has worked on Application of standards for safety assessment, Automation of verification objectives, and Reuse of assurance artefacts from automotive to avionics; CS8 - **Automotive Telematics Function** has studied Multi-concern aspects (assurance cases, assessment, specification, and analysis); CS9 - **Safety-Critical Software Lifecycle of a Monitoring System for Air Traffic Management** has addressed System/software design and safety analysis and Safety case; CS10 - **Certification Basis to Boost the Usage of MPSoC Architectures in the Space Market** has tackled System modelling and Reconfigurable FPGA architectures; CS11 - **Design and Efficiency Assessment of Model-Based Attitude and Orbit Control SW** has dealt with Compliance management.

The corresponding outcomes has allowed AMASS to demonstrate its high-level goals: (1) a potential gain for **design efficiency** of complex CPS by reducing their assurance effort; (2) a potential reuse of assurance results, leading to **cost reductions** for component/product (re)certification/qualification activities; (3) a potential raise of **technology innovation** led by reduction of assurance and certification risks, and; (4) a potential **sustainable impact** in CPS industry by increasing the harmonization and interoperability of assurance and certification tool technologies.

Some of the main **non-technical outcomes** in the last six months have been the Open Industrial Workshop (summary below), new training videos, a new leaflet with usage scenarios, and pagers of the main AMASS tool features.



The Future of AMASS Results

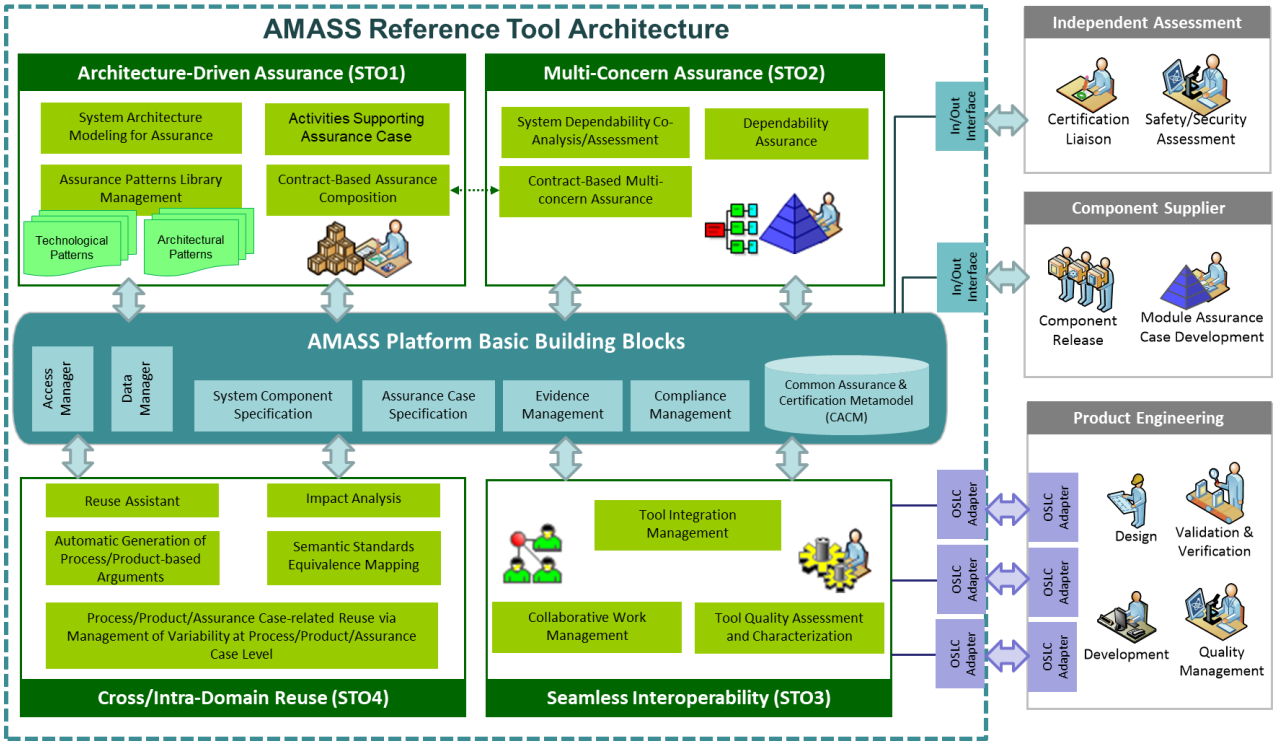
Although the AMASS project has finished, its **contribution to CPS assurance & certification will continue in the future**, both in industrial contexts and in research ones.

From an industrial perspective, the AMASS project provides **a platform that fulfils many requirements**. It is **open, easy to extend, and sustainable** (by means of re-using and recycling knowledge). As with many large applications, companies will likely suffer from drawbacks initially during the phase when the platform is established, similar to enterprises establishing Enterprise Resource Planning systems from Oracle or SAP. We assume though that **once the AMASS Tool Platform is established, it will sustainably contribute and pay off in the long run**. For instance, when employees with expert knowledge leave a company, they can leave valuable information thoroughly categorized behind. Furthermore, the effort to harmonize standards from different domains decreases, and safety and security engineers from one domain find it easier to switch to another domain once they get familiar with similar standards from the same equivalence class. Analogous to the adaptation phase of companies to new ERP systems, it might be interesting to investigate how long it takes until it pays off to replace current V&V efforts with the AMASS Platform.

From an academic perspective, AMASS shows **huge potential as a rich testbed for industrial applications** that now might become more accessible for novel technologies and techniques, arching from testing methods from software engineering to formal verification. Two very interesting domains are: i) **safety impact of security**, and ii) **certification and assurance of multi-critical probabilistic/stochastic processes**. The first point targets assessing (functional) safety and security concerns alike (even in parallel), and the mutual effect one can have on the other. The second point targets the inclusion of reasoning beyond functional safety. When certifying a system, functional properties are important for the industry.

From the perspective of the open source community, the current version of the **AMASS Open Platform website** (https://www.polarsys.org/opencert/) provides: General information about the Polarsys OpenCert Tools Platform; Downloads of the Polarsys OpenCert Tools Platform package (including OpenCert, CHESS, Eclipse Process Framework Composer, and the other integrated open source tools); Support for news and blog posts; Link to Source Code and downloads; Getting Started documentation; User's documentation; Developer's documentation; and Training material linking to videos from the Polarsys OpenCert Tools Platform YouTube channel. More content will be provided to support newcomers, users and adopters in evaluating the AMASS Open Platform. In particular, we plan to publish information about the AMASS industrial case studies and their usage of the AMASS Open Platform.

Last but not least, the AMASS partners have expressed their **intention to exploit tens of foreground items**, e.g.: OpenCert tool, Sabotage tool, V&V Manager, CHESS, OCRA, features to leverage Systems Engineering via TRC tools, OSLC-KM, DIVINE Verification Tool, and other technologies for system modelling, multi-concern system analysis, and for V&V, among others. In addition, **several pieces of AMASS work are being or will be used and extended in other projects** (AQUAS, Arrohead Tools, NewControl…).



Considerations about Open Source and Security

AMASS has addressed a wide universe of application areas while implementing an open collaboration model to develop its technology solutions. It is not surprising that the community would express its **concern on the security aspects and the openness of the AMASS Tool Platform**. But no worries! Security and openness are two orthogonal issues and the AMASS Tool Platform is certainly not a liability for the development of CPS.

No direct relationship between open source and security. It is true that the OSS movement was not designed with security in mind, but also that the OSS community do believe that opening their code up for inspection will increase protection against bugs. When analysing security aspects in open source vs. closed source software, no significant differences in the severity of vulnerabilities have been found.

Closed source solutions are not necessarily more secure. The openness in OSS makes it easier for both the good and the bad guys to find vulnerabilities in the code, since it is available for anyone to review (and to fix!). However, closed models implementing a "security through obscurity" approach are not necessarily better. Security is a holistic concept not only depending on the final result, but also linked to the creation and maintenance process. Open source has the potential to be better because of its available for public scrutiny.

Projection in the AMASS context. AMASS partners and early adopters agree that security is crucial in all tools, systems and platforms, and of course AMASS results are no exception. On the one hand, the Eclipse Development Process covers the traceability of the code published for the AMASS open platform. On the other hand, the platform is supposed to be embedded in a larger environment where additional measures can be integrated to ensure security.

AMASS is about tools for assurance and certification that can be used to improve engineering efficiency, but AMASS is not a CPS core component, and thus its platform by itself is not a liability for the development of CPS. **The AMASS open platform is deployed in the context of a global certification and assurance process that should consider the security risks related to the tools in order to effectively mitigate them**.

TRC results in AMASS

The REUSE Company (TRC) has played the role of a tool vendor in AMASS. The company is specialized in **Semantic Representation and Analysis techniques for systems engineering**. The corresponding tools have been and will be enhanced with AMASS results.

TRC has contributed to solutions that **link (a) system assurance and certification with (b) knowledge-centric systems engineering and quality analysis**:

- **Extended requirements quality analysis**, thanks to the provision of new metrics and procedures to assess requirements specifications.
- **Model quality analysis**, by extending the assessment capabilities to other system artefacts such as SysML diagrams and Simulink models.
- **Quality evolution analysis**, which provides a detailed picture of how system artefact quality has changed during a project.
- **Checklist-based V&V**, in order to extend automatic quality analyses with manual ones.
- **Generic tool interoperability with the OSLC KM technology** for a wide variety of system artefact types and formats.
- **Extended and enhanced ad-hoc tool interoperability**, e.g. for Rhapsody.
- **Automated traceability management**, thanks to the features of the Traceability Studio tool to deal with traceability projects.
- **Evolution management of system and certification information represented as an ontology**, so that a user can first represent e.g. a safety-critical system's design as an ontology and next manage such representation.
- **Data exchange between TRC tools and the AMASS Tool Platform**, to analyse system artefact information managed with the Platform and to enable quality results import into the Platform.
- **Advanced search of system assurance and certification information**, by exploiting TRC suite's semantics-based search features.

Given their great potential, TRC will continue working on these technologies after AMASS.

AMASS Open Industrial Workshop

The AMASS Open Industrial Workshop was held on March 28th, 2019, in Florence, Italy. The event was co-located with the DATE 2019 conference (Design, Automation and Test in Europe; https://www.date-conference.com/).

The workshop was targeted at both practitioners and researchers aiming to gain awareness of **the latest advances on cost-effective assurance and certification of safety-critical systems**, and of how the corresponding solutions work. AMASS partners presented practical aspects and concrete application examples of the main AMASS results.

Twelve people registered for the workshop, including both researchers and practitioners. The speakers from the AMASS consortium were Alejandra Ruiz (TEC), Alberto Debiasi (FBK), and Stefano Puri (INT). The final event agenda included the following topics: Architecture-driven assurance, Architecture-driven assurance workflow and functionalities, Compliance and reuse, Toolchain connectivity, OSLC, Co-engineering as AMASS introduction; Live and video demos; and Exercises

The overall feedback on AMASS results was positive. The attendees had downloaded some of the AMASS resources before the Workshop and were really committed. Questions were asked about installing dedicated servers, how the development will continue after the project, and the role of the AMASS open source community in the future.

SAFECOMP 2018

As reported in the latest newsletter, AMASS contributed to the organization of the SASSUR workshop at SAFECOMP 2018, the **37th International Conference on Computer Safety, Reliability and Security**. In addition, AMASS partners participated in other SAFECOMP events.

SAFECOMP 2018 was organized by Barbara Gallina (MDH). Many other AMASS partners participated in the main conference, including AIT, ALT, SPS, CEA, and TEC. **The conference was co-located with five workshops, including SASSUR, DecSOS** (organized by AIT; co-chair Erwin Schoitsch), **and WAISE** (organized by CEA; co-chair Huascar Espinoza).

The **International Workshop on Artificial Intelligence Safety Engineering** (WAISE) was dedicated to exploring new ideas on AI safety, ethically aligned design, regulations, and standards for AI-based systems. WAISE brought together practitioners, experts, and researchers from diverse communities, such as AI, safety engineering, ethics, robotics, standardization, certification, CPS, safety-critical systems, and application domain communities.

Erwin Schoitsch (AIT) was the chair of the **Multi-concern assurance session** at the main conference, which hosted interesting discussions on safety and security concerns in the automotive domain. The conference featured three keynotes around the conference main theme, which was cross- and intra-domain reuse of engineering and certification artefacts. A panel discussion on the main theme was also held.

AMASS work on **reuse-related results** was also presented at the exhibition by MDH-team members (Irfan Sljivo, Zulqarnain Haider, Faiz Ul Muram, Muhammad Atif Javed, Julieth Patricia Castellanos Ardila). SPS presented a fast abstract.

In summary, SAFECOMP 2018 was a great opportunity to present the progress of AMASS in front of an international audience with more than 180 participants coming from 21 different countries. AMASS partners are looking forward to SAFECOMP 2019 to repeat the large and successful participation.

Recent AMASS Presence at Events (selection)

Ada-Europe 2019 - 24th International Conference on Reliable Software Technologies. Warsaw, Poland. June 11-14, 2019.

ATVA 2018 - 16th International Symposium on Automated Technology for Verification and Analysis. Los Angeles, USA. October 7-10, 2018.

EFECS 2018 - European Forum for Electronic Components and Systems. Lisbon, Portugal. November 20-22, 2018.

embedded world 2019. Nürnberg, Germany. February 25-27, 2019.

HASE 2019 - International Symposium on High-Assurance Systems Engineering. Hangzhou, China. January 3-5, 2019.

ISSA 2019 - International Workshop on Interplay of Security, Safety and System/Software Architecture. Luxembourg. September 23-27. 2019.

MODELS 2018 - IEEE/ACM 22nd International Conference on Model-driven Engineering Languages and System. Copenhagen**,** October 2018.

OSLC Fest. Stockholm, Sweden. November 5-6, 2018.

QUATIC 2019 - 12th Int. Conference on the Quality of Information and Communications Technology. Ciudad Real, Spain. September 11-13, 2019.

REFSQ 2019 - 25th International Working Conference on Requirements Engineering: Foundation for Software Quality. Essen. Germany. March 18-21, 2019.

SAFECOMP 2019 - 38th International Conference on Computer Safety, Reliability and Security. Turku, Finland. September 10-13, 2019.

Recent AMASS Publications (selection)

Adedjouma, M., Yakymets, N.: *A Framework for Model-based Dependability Analysis of Cyber-Physical Systems*. 19th IEEE International Symposium on High Assurance Systems Engineering (HASE 2019)

Bendík, J., Černá, I.: *Evaluation of Domain Agnostic Approaches for Enumeration of Minimal Unsatisfiable Subsets*. 22nd International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-22)

de la Vara, J.L., Jimenez, G., Mendieta, R., Parra, E.: *Assessment of the Quality of Safety Cases: A Research Preview*. 25th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2019)

de la Vara, J.L., Ruiz, A., Gallina, B., Blondelle, G., Alaña, E., Herrero, J., Warg, F., Skoglung, M., Bramberger, R.: *The AMASS Approach for Assurance and Certification of Critical Systems*. embedded world Conference 2019

Haider, Z., Gallina, B., Carlsson, A., Mazzini, S., Puri, S.: *ConcertoFLA-based Multi-concern Assurance for Space Systems*. Ada User Journal 40(1)

Javed, M. A., Gallina, B.: *Towards Variant Management and Change Impact Analysis in Safety-oriented Process-Product Lines*. 34th ACM/SIGAPP Symposium on Applied Computing (SAC 2019)

Nešic D., Nyberg, M., Gallina, B.: *Constructing Product-Line Safety Cases from Contract-Based Specifications*. 34th ACM/SIGAPP Symposium on Applied Computing (SAC 2019)

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