AMASS
ECSEL Joint Undertaking

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

Newsletter #4 - April 2018 https://amass-ecsel.eu/

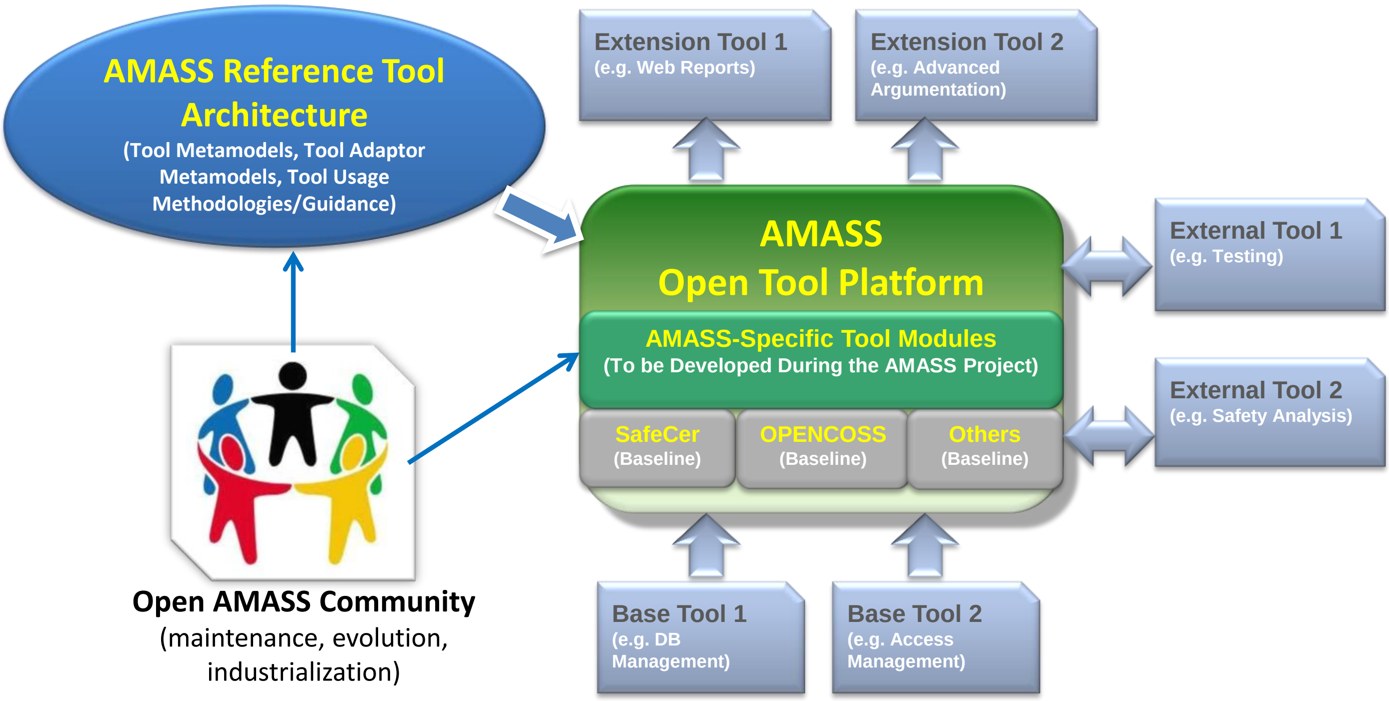
The work on the European-wide open platform and community for assurance and certification of cyber-physical systems is starting its last phase!

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 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 Overall Status after the Second Project Year

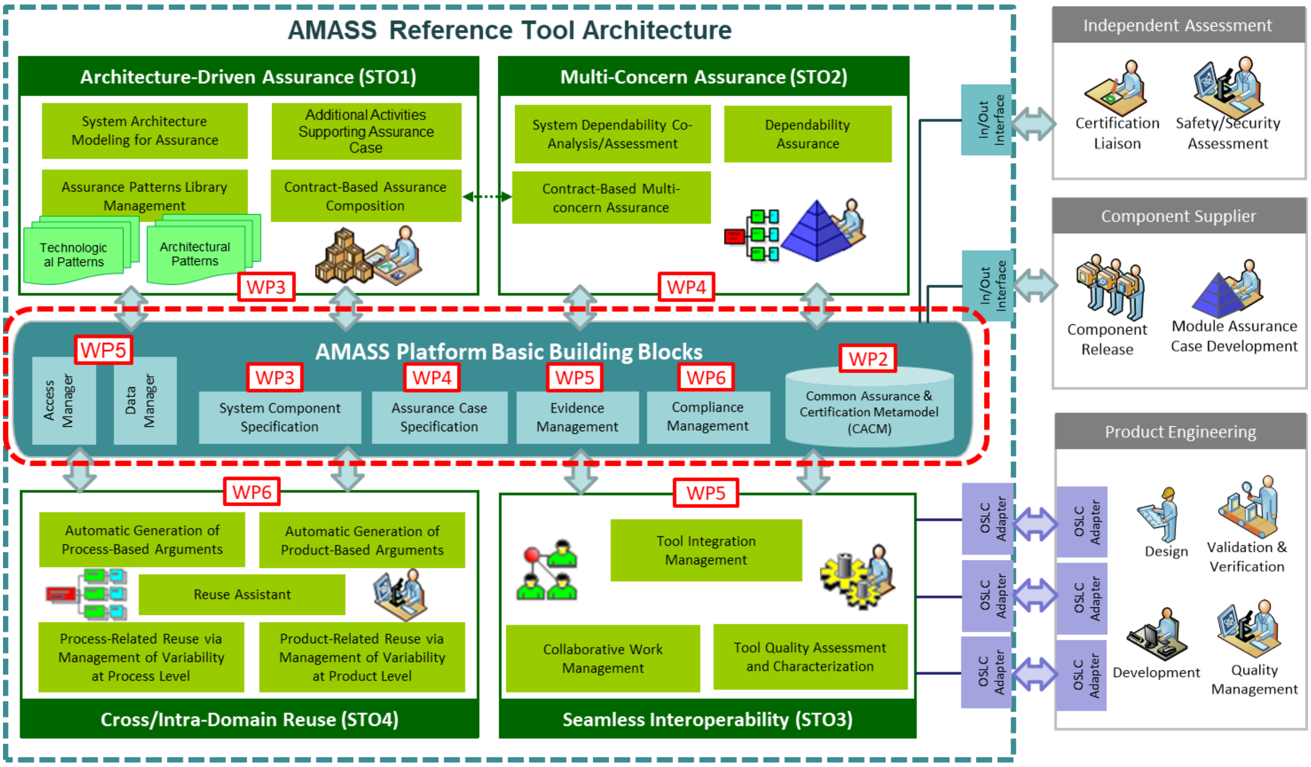
During the fourth semester of the project, the technical work by the AMASS consortium has strongly focused on two main activities: (1) completion of the specification and implementation of the second tool platform prototype (Prototype P1), and (2) evaluation of the implemented tools in industrial case studies.

For Architecture-Driven Assurance, the **AMASS Prototype P1** includes solutions for the left-hand side of the V-model at high- and low-level design (system architecture modelling, architectural patterns for assurance, contract-based design for assurance, requirements support), as well as corresponding V&V activities on the right-hand side of the V-model (i.e. V&V-based assurance). The AMASS partners have developed approaches for Multi-Concern Assurance in relation to dependability assurance modelling, contract-based multi-concern assurance, and system dependability co-analysis and assessment. Further tool interoperability technologies (e.g. OSLC-KM and for V&V tools) and features for collaborative work (e.g. for traceability and data mining) have enhanced Seamless Interoperability. The main new solutions for Cross- and Intra-Domain Reuse are advanced reuse assistance, process- and product-related reuse via variability management, and automatic generation of process arguments and of product-based ones. Deliverables **D3.5, D4.5, D5.5 and D6.5** document the implementation results for Prototype P1, and deliverables **D3.7, D4.7, D5.7 and D6.7** present the methodological guidance to use the results.

The **industrial evaluation** of Prototype P1 has been documented in D1.5. It presents the main outcome from the implementation of the case studies by using the Prototype in the automotive, railway, aerospace, space, and energy domains. Some case studies have also used functionalities of the Core Prototype, e.g. OpenCert or EPF Composer for compliance management. For each case study, the coverage with respect to the AMASS Prototype P1 has been identified and the feedback from industrial partners collected. This feedback is of vital importance and an active proof of the performance of the AMASS platform in the industry.

In addition, different work packages have worked on the **conceptual and design view for the third prototype** (Prototype P2). This conceptual and design work includes: (1) assurance patterns for contract-based design, new means for fault injection, and different ways to assess system artefact quality; (2) concepts for multi-concern contracts, processes, and analyses (e.g. through Failure Modes, Vulnerabilities and Effect analysis); (3) integration of the AMASS Tool Platform with further commercial tools developed by the AMASS partners; and (4) new support for assurance asset search and for analysis of reuse possibilities and consequences.

Last but not least, progress has been made on **non-technical aspects** such as community building and industrial impact, as well as dissemination, training, exploitation, and standardization. This includes the organisation of the second EAB (External Advisory Board) workshop to be held in Västerås, Sweden, in September 2018, together with the SafeComp 2018 Conference. Several AMASS partners participate in the organisation of this conference and of its workshops (DECSoS, SASSUR, and WAISE).


AMASS Reference Tool Architecture
Architecture-Driven Assurance (STO1)
System Architecture Modeling for Assurance
Additional Activities Supporting Assurance Case
Assurance Patterns Library Management
Contract-Based Assurance Composition
Technological Patterns
Architectural Patterns
WP3
Multi-Concern Assurance (STO2)
System Dependability Co-Analysis/Assessment
Dependability Assurance
Contract-Based Multi-concern Assurance
WP4
In/Out Interface
In/Out Interface
AMASS Platform Basic Building Blocks
WP5
Access Manager
Data Manager
WP3
System Component Specification
WP4
Assurance Case Specification
WP5
Evidence Management
WP6
Compliance Management
WP2
Common Assurance & Certification Metamodel (CACM)
WP6
Automatic Generation of Process-Based Arguments
Automatic Generation of Product-Based Arguments
Reuse Assistant
Process-Related Reuse via Management of Variability at Process Level
Product-Related Reuse via Management of Variability at Product Level
Cross/Intra-Domain Reuse (STO4)
WP5
Tool Integration Management
Collaborative Work Management
Tool Quality Assessment and Characterization
Seamless Interoperability (STO3)
OSLC Adapter
OSLC Adapter
OSLC Adapter
OSLC Adapter
OSLC Adapter
OSLC Adapter
Independent Assessment
Certification Liaison
Safety/Security Assessment
Component Supplier
Component Release
Module Assurance Case Development
Product Engineering
Design
Validation & Verification
Development
Quality Management

AMASS Prototype P1

The AMASS consortium has been working on the **second version of the AMASS Tool Platform (Prototype P1)** during the last year. The implementation and its validation have already finished, and the Prototype has been applied and evaluated in the project case studies.

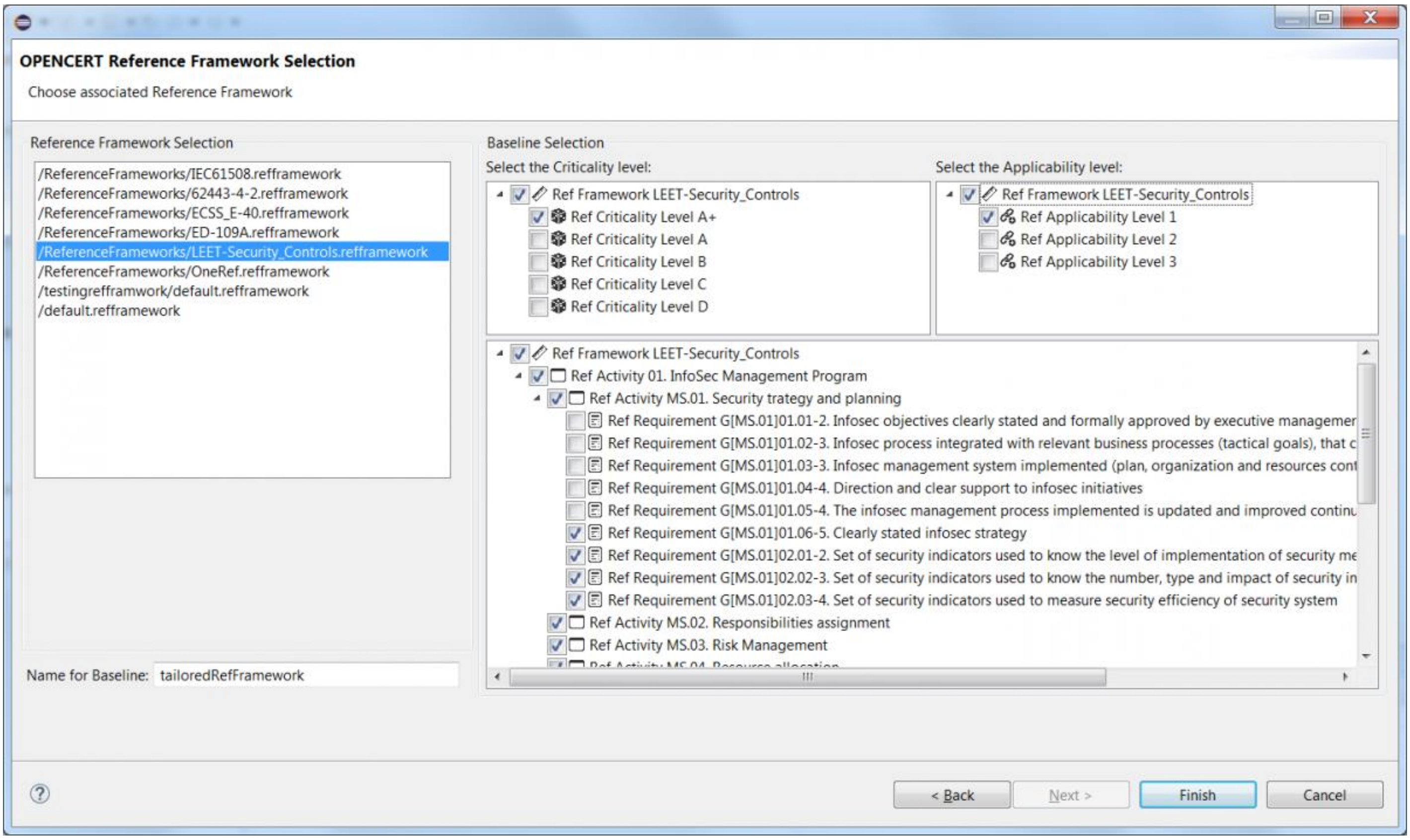
Prototype P1 implementation has been documented in several deliverables in WP3, WP4, WP5, and WP6. Among the **implemented new features**, the Prototype supports:

- For Architecture-Driven Assurance, contract-based validation of component composition, management of contract-component assignments, improved V&V results overview, advanced contract definition, and enhanced requirements quality analysis.
- For Multi-Concern Assurance, argument architecture specification, advanced features for application of argument patterns, argument import and export, generation of compositional arguments, inter-concern relationship specification and analysis, contract-based multi-concern assurance, multi-concern assurance workflow, and co-assessment and cross-concern reuse.
- For Seamless Interoperability, new traceability features, new integration possibilities with V&V tools (V&V Manager and OCRA), implementation of OSLC-KM approach for generic tool interoperability, and preliminary collaborative features by means of web-based technologies and data mining.
- For Cross- and Intra-Domain Assurance Reuse, enhanced compliance management, extended reuse assistance, reusable-artefact search for reuse discovery, semi-automatic generation of process and of product arguments, and variability management from different perspectives.

A major achievement for P1 has been the improvement on the EPF composer tool by MDH. As a result, the EPF team has thanked Muhammad Atif Javed for his contributions to the latest release of the tool, and more concretely for solving some migration fixes (including Java 8/Neon dependencies) and content storage problems, and for providing new combo boxes, rich text editor styles, and export of standalone application.

Prototype P1 validation has been performed in the scope of WP2. The **conclusions from the validation** include that most of the planned functionality for the Prototype has been implemented and successfully tested, that special attention must be paid in future validation activities to the testing of cross-WP requirements, and that there exists room for improvement in the specification of the test cases.

Based on Prototype P1, **the work for the final version of the AMASS Tool Platform (Prototype P2) has also already started**. The main current focus is on its conceptual design, including the necessary approaches to realise the AMASS vision for CPS assurance and certification and tool support design.



OPENCERT Reference Framework Selection

Choose associated Reference Framework

Reference Framework Selection

/ReferenceFrameworks/IEC61508.refframework
/ReferenceFrameworks/62443-4-2.refframework
/ReferenceFrameworks/ECSS_E-40.refframework
/ReferenceFrameworks/ED-109A.refframework
/ReferenceFrameworks/LEET-Security_Controls.refframework
/ReferenceFrameworks/OneRef.refframework
/testingrefframwork/default.refframework
/default.refframework

Name for Baseline: tailoredRefFramework

Baseline Selection

Select the Criticality level:

- ☑ Ref Framework LEET-Security_Controls
  - ☑ Ref Criticality Level A+
  - □ Ref Criticality Level A
  - □ Ref Criticality Level B
  - □ Ref Criticality Level C
  - □ Ref Criticality Level D

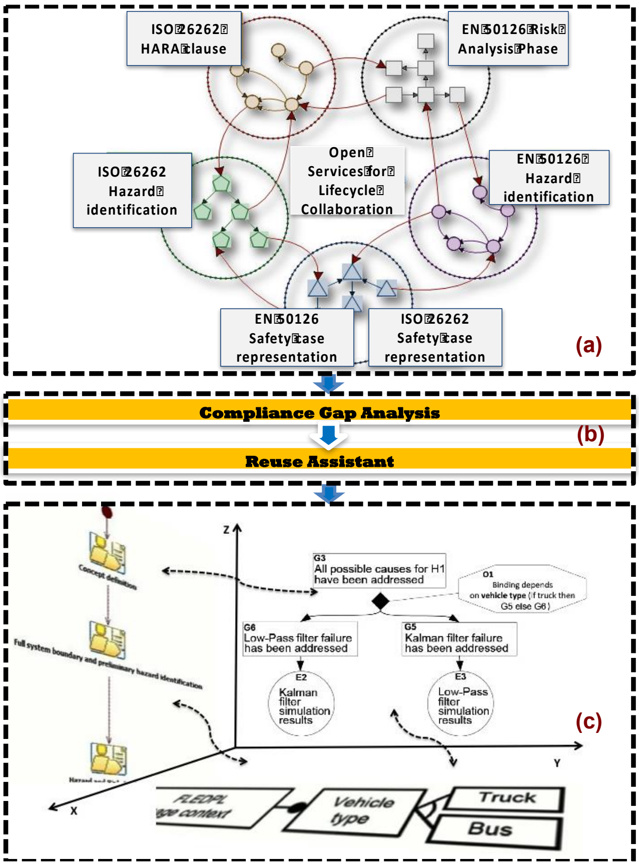
Select the Applicability level:

- ☑ Ref Framework LEET-Security_Controls
  - ☑ Ref Applicability Level 1
  - □ Ref Applicability Level 2
  - □ Ref Applicability Level 3

- ☑ Ref Framework LEET-Security_Controls
  - ☑ Ref Activity 01. InfoSec Management Program
    - ☑ Ref Activity MS.01. Security trategy and planning
      - □ Ref Requirement G[MS.01]01.01-2. Infosec objectives clearly stated and formally approved by executive managemer
      - □ Ref Requirement G[MS.01]01.02-3. Infosec process integrated with relevant business processes (tactical goals), that c
      - □ Ref Requirement G[MS.01]01.03-3. Infosec management system implemented (plan, organization and resources cont
      - □ Ref Requirement G[MS.01]01.04-4. Direction and clear support to infosec initiatives
      - □ Ref Requirement G[MS.01]01.05-4. The infosec management process implemented is updated and improved continu
      - ☑ Ref Requirement G[MS.01]01.06-5. Clearly stated infosec strategy
      - ☑ Ref Requirement G[MS.01]02.01-2. Set of security indicators used to know the level of implementation of security me
      - ☑ Ref Requirement G[MS.01]02.02-3. Set of security indicators used to know the number, type and impact of security in
      - ☑ Ref Requirement G[MS.01]02.03-4. Set of security indicators used to measure security efficiency of security system
    - ☑ Ref Activity MS.02. Responsibilities assignment
    - ☑ Ref Activity MS.03. Risk Management
    - ☑ Ref Activity MS.04. Resource allocation

AMASS Vision for Cross- and Intra-Domain Reuse

The vision of AMASS for cross/intra domain reuse is exemplified in the figure below, which consists of three sub-figures (a, b, and c). The sub-figures are vertically placed and depict respectively the **semantics-based standards mapping, the reuse assistant, and the specification of families of processes, products, or assurance cases**. This vision integrates and extends results achieved by the OPENCOSS and SafeCer projects, and incorporates and cross-fertilizes from-scratch and not-from-scratch reuse.


ISO 26262 HARA clause
EN 50126 Risk Analysis Phase
Open Services for Lifecycle Collaboration
ISO 26262 Hazard identification
EN 50126 Hazard identification
EN 50126 Safety case representation
ISO 26262 Safety case representation
(a)
Compliance Gap Analysis
(b)
Reuse Assistant
Concept definition
Full system boundary and preliminary hazard identification
Z
G3
All possible causes for H1 have been addressed
O1
Binding depends on vehicle type (if truck then G5 else G6)
G6
Low-Pass filter failure has been addressed
G5
Kalman filter failure has been addressed
E2
Kalman filter simulation results
E3
Low-Pass filter simulation results
(c)
Y
X
FLEDPL
ge context
Vehicle type
Truck
Bus

From-scratch reuse is in focus on the top of the figure (subfigure (a)). **Semantics-based automatic identification of commonalities** is proposed as a solution to identify reuse possibilities. This solution builds on top of initial exploration conducted in the framework of SafeCer and it is here empowered by considering recent advances in the semantic web and in tools interoperability.

Once commonalities are identified, the **reuse assistant** (sub-figure (b)) is expected to exploit them **to perform more powerful compliance gap analysis**.

The bottom of the figure (subfigure (c)) focuses on **systematic reuse**. In this case, reuse is not expected to be done from scratch or ad-hoc, but **experience is systematized.** Gathered experience is expected to be derived from the left side of the figure. Systematization is conducted by properly engineering the domain and then by deriving desired processes, products, or assurance cases via valid configuration.

AMASS Meetings

A **workshop on the AMASS automotive case studies** was successfully held at Assystem Germany in January 2018 in Berlin. Fourteen participants from seven different partners attended the workshop. Three case studies were addressed: "DC-Drive Workbench", "Advanced driver assistance function with electric vehicle sub-system", and "Collaborative automated fleet of vehicles". They are demonstrators for the **research and development on autonomous driving**.

Among others, the following **research intentions** were expressed: creation of formalised requirements and contract-refinement, automation of safety analyses (fault injection, model simulation), contract-based safety engineering, assurance case patterns, reuse of safety argument fragments and of monitors, combined safety & security analyses for cars in platoon, assurance cases and patterns, and the automated generation of monitors and verification by simulation.

The AMASS consortium gathered together in Vienna on March 21st, 22nd and 23rd for the **5th General Meeting** of the project. The meeting was hosted by AIT. Forty-six people attended the meeting.

The discussions on technical aspects paid great attention to the **use of Prototype P1 in the project's industrial case studies**. The consortium agreed upon the final research and implementation work for the third prototype of the AMASS Tool Platform (aka Prototype P2). This work includes advanced features for CHESS, new means for co-analysis, co-engineering, and co-assurance of safety and security, finalisation of the features for tool integration and collaborative work of the AMASS Tool Platform, and the enactment of reuse approaches in new scenarios that tackle cross-domain needs.

OpenCert Website

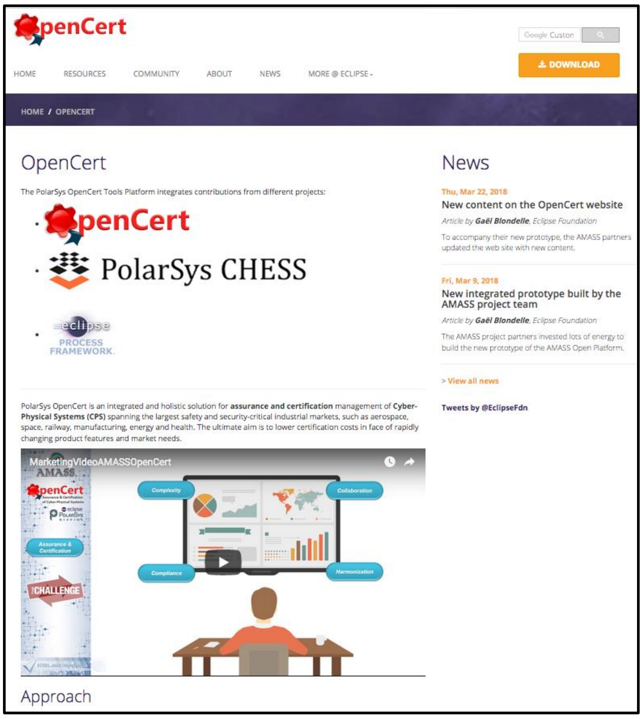
Among the activities for the development of the AMASS open-source community, a new version of the OpenCert website has been released.

The homepage of the OpenCert website has been improved and now lists the different components of the platform upfront, and includes an introductory video of the OpenCert platform. “Getting Started” and “Documentation” have been removed, and the content is now listed with other content like “Training” under “Resources”. More content will be added to this “Resources” page in the coming months to further support AMASS newcomers, users and adopters. The partners have also implemented a more automated mechanism to update the website.

The current version of the AMASS Open Platform website provides:

- General information about OpenCert
- Downloads of the OpenCert platform package (including OpenCert, Chess and Eclipse Process Framework)
- Support for news and blog posts
- Link to Source Code and downloads
- Getting Started documentation
- User’s documentation
- Developer’s documentation
- Training material linking to videos from the OpenCert YouTube channel

In addition to making a continuous effort to improve the content available on the website and keep this up to date, in the future we will focus on **adding more documentation for users and developers, and publishing use cases reports.**



OpenCert

The PolarSys OpenCert Tools Platform integrates contributions from different projects:

- OpenCert
- PolarSys CHESS
- eclipse PROCESS FRAMEWORK

PolarSys OpenCert is an integrated and holistic solution for **assurance and certification** management of **Cyber-Physical Systems (CPS)** spanning the largest safety and security-critical industrial markets, such as aerospace, space, railway, manufacturing, energy and health. The ultimate aim is to lower certification costs in face of rapidly changing product features and market needs.

Approach

News

Thu, Mar 22, 2018
New content on the OpenCert website
Article by ***Gaël Blondelle****, Eclipse Foundation*
To accompany their new prototype, the AMASS partners updated the web site with new content.

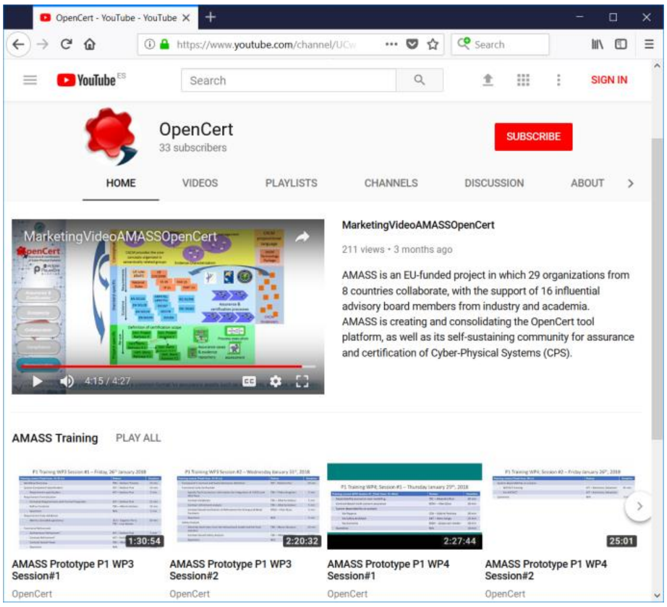
Fri, Mar 9, 2018
New integrated prototype built by the AMASS project team
Article by ***Gaël Blondelle****, Eclipse Foundation*
The AMASS project partners invested lots of energy to build the new prototype of the AMASS Open Platform.

> View all news

Tweets by @EclipseFdn

AMASS videos

A YouTube channel with **videos about the results of AMASS and about the technologies used for their development** has been created. It currently includes a demo of the Core Prototype and videos of the past training sessions.



OpenCert
33 subscribers

MarketingVideoAMASSOpenCert
211 views • 3 months ago
AMASS is an EU-funded project in which 29 organizations from 8 countries collaborate, with the support of 16 influential advisory board members from industry and academia. AMASS is creating and consolidating the OpenCert tool platform, as well as its self-sustaining community for assurance and certification of Cyber-Physical Systems (CPS).

AMASS Training

AMASS Prototype P1 WP3 Session#1
OpenCert

AMASS Prototype P1 WP3 Session#2
OpenCert

AMASS Prototype P1 WP4 Session#1
OpenCert

AMASS Prototype P1 WP4 Session#2
OpenCert

Regarding the **videos** that have been created from the sessions **for training users in the Prototype P1**, for Architecture-Driven Assurance the presenters explained a workflow overview, requirement specification for system component specification, requirements formalization, requirements early validation through metrics, and functional refinement (architectural refinement, contract refinement, contract-based views). Another session addressed components nominal and faulty behaviour definition, functional early verification, safety analysis, safety cases, and upcoming features for Savona, simulation-based fault injection, and requirements early validation.

In the scope of Multi-Concern Assurance, the training content was dependability assurance case modelling, contract-based multi-concern assurance, system-dependability co-analysis (with Papyrus, Safety Architect, and Concerto), and WEFACT.

Partners working on Seamless Interoperability described the integration of the OSLC-KM approach in the AMASS Tool Platform. Other tool integration capabilities were presented in the scope of Architecture-Driven Assurance.

Finally, the features for Cross- and Intra-Domain Assurance Reuse explained were filtering during assurance project generation by criticality/applicability level, reuse assistant, compliance map report, management of families-lines, and semi-automatic generation of arguments.

Recent AMASS Presence at Events (selection)

EclipseCon Europe 2017. Ludwigsburg, Germany. October 24-26, 2017

ER 2017 - 36th Int. Conference on Conceptual Modelling. Valencia, Spain. November 6-9, 2017

ERTSS 2018 - 9th European Congress Embedded Real Time Software and Systems. Toulouse, France. January 31-February 2, 2018

ICRE 2017 - 2nd International Conference on Reliability Engineering. Milan, Italy. December 20-22, 2017

MODELSWARD 2018 - 6th International Conference on Model-Driven Engineering and Software Development. Madeira, Portugal. January 22-24, 2018

PESI day of the Safety Working Group. Madrid, Spain. March 21, 2017

Seminar at City University of London. London, UK. January 29, 2018

Seminars at FBK. Trento, Italy. September and October 2017

TeReCom 2017 - 1st Workshop on Technologies for Regulatory Compliance. Luxembourg. December 13, 2017

TRC Forum. Madrid, Spain. November 30-December 1, 2017

WoSoCer 2017 - 7th IEEE International Workshop on Software Certification. Toulouse, France. October 23-26, 2017

Recent AMASS Publications (selection)

Alajrami, S., Gallina, B., Romanovsky, A.: *Enabling GSD Task Allocation via Cloud-based Software Processes*. International Journal of Networked and Distributed Computing 5(4): 221-232, 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)

de la Vara, J.L., Ruiz, A., Espinoza, H.: *Recent Advances towards the Industrial Application of Model-Driven Engineering for Assurance of Safety-Critical Systems*. 6th Int. Conference on Model-Driven Engineering and Software Development (MODELSWARD 2018)

Gallina B., Haider, Z., Carlsson, A., Mazzini, S., Puri, S.: *Multi-concern Dependability-centered Assurance for Space Systems via ConcertoFLA*. 23rd Int. Conference on Reliable Software Technologies (Ada-Europe 2018)

Gallina, B., Martinez, J.: *Reuse in (re)certification of systems*. 17th International Conference on Software Reuse (ICSR 2018)

Parra, E., de la Vara, J.L., Alonso, L.: *Analysis of Requirements Quality Evolution*. 40th International Conference on Software Engineering (ICSE 2018)

Sljivo, I., Gallina, B., Carlson, J., Hansson, H., Puri, S.: *Tool-Supported Safety-Relevant Component Reuse: From Specification to Argumentation*. 23rd Int. Con. on Reliable Software Technologies (Ada-Europe 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