AMASS
ECSEL Joint Undertaking

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

Newsletter #1 - October 2016 http://amass-ecsel.eu/

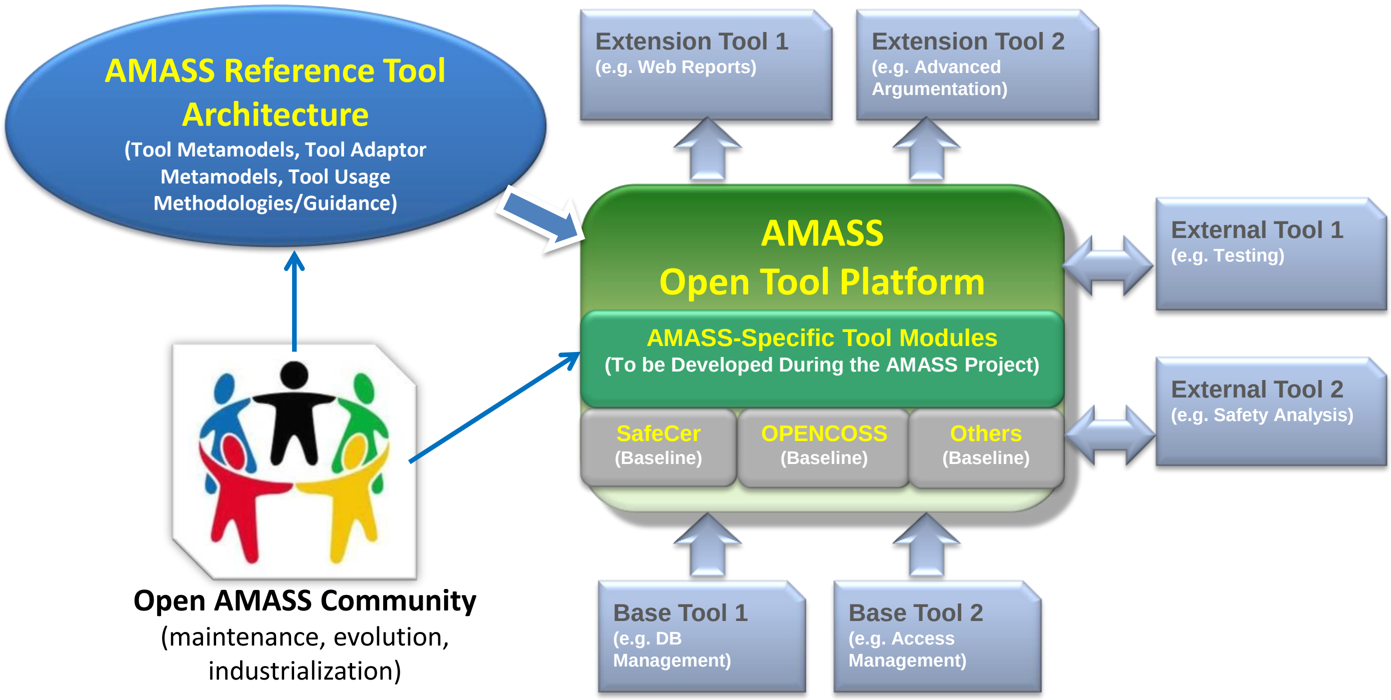
The work on the European-wide open platform and community for assurance and certification of cyber-physical systems has started!

AMASS is a H2020-ECSEL project that will create and consolidate 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 will work 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 will build 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 Goals

1. A potential gain for **design efficiency** of complex CPS by reducing their assurance and certification/ qualification effort by 50%.
2. A potential reuse of assurance results (qualified or certified before), leading to 40% of **cost reductions** for component/product (re)certification/ qualification activities.
3. A potential raise of **technology innovation** led by 35% reduction of assurance and certification risks of new CPS products.
4. A potential sustainable impact in CPS industry by increasing the **harmonization and interoperability** of assurance and certification/qualification tool technologies by 60%.

AMASS results will be validated and their benefits will be evaluated in 11 case studies from Air Traffic Management, Automotive, Avionics, Industrial Automation, Railway, and Space.

AMASS Impact

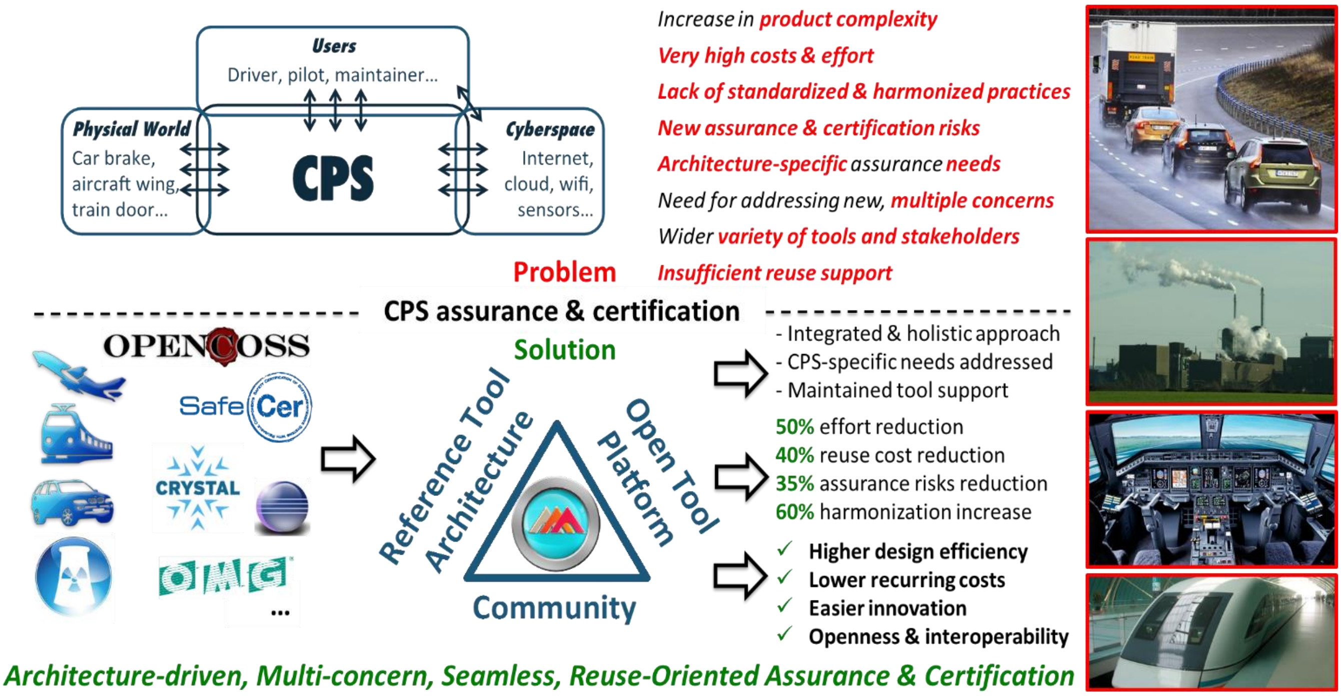
- **OEMs** (including system integrators) **and Component suppliers** will use AMASS results in order to increase CPS design cost-effectiveness, ease innovation, and reduce the costs and risks of CPS assurance and certification.
- **Assessors and Certification authorities** will be able to provide services that better fit CPS-specific needs.
- **Tool vendors** will extend their products with new features and integrate them with the AMASS Open Tool Platform, further benefiting from the openness and interoperability that AMASS will enable.
- **European 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 Excellence Concept

Embedded systems have significantly increased in number, technical complexity, and sophistication, moving towards open, interconnected, networked systems (e.g. "the connected car"), **integrating the physical and digital world**. This “cyber-physical” dimension is exacerbating the problem of ensuring safety, security, availability, robustness, and reliability in the presence of human, environmental and technological risks.

Many CPS further do not have yet standardized and harmonized practices for assurance and certification that ensure safe, secure, and reliable operation with typical system architectures. **The CPS community often finds it difficult to apply existing certification guidance**. The pace of assurance and certification will ultimately be determined by the ability of both industry and authorities to overcome technical, regulatory, and operational challenges. A key challenge is the reuse of CPS products, not only from one application domain in another but also in a same domain.

To tackle these challenges, **AMASS will develop and consolidate an open and holistic assurance and certification framework for CPS**. The technical work has been divided into four Scientific and Technical Objectives: Architecture-Drive Assurance, Multi-Concern Assurance, Seamless Interoperability, and Cross- and Intra-Domain Reuse.



Users
Driver, pilot, maintainer...
Physical World
Car brake, aircraft wing, train door...
CPS
Cyberspace
Internet, cloud, wifi, sensors...
Problem
CPS assurance & certification
Solution
OPENCOSS
SafeCer
CRYSTAL
OMG
...
Reference Tool Architecture
Open Tool Platform
Community

*Increase in **product complexity***
Very high costs & effort
Lack of standardized & harmonized practices
New assurance & certification risks
Architecture-specific** assurance **needs
*Need for addressing new, **multiple concerns***
*Wider **variety of tools and stakeholders***
Insufficient reuse support

- Integrated & holistic approach
- CPS-specific needs addressed
- Maintained tool support

50% effort reduction
40% reuse cost reduction
35% assurance risks reduction
60% harmonization increase

✓ **Higher design efficiency**
✓ **Lower recurring costs**
✓ **Easier innovation**
✓ **Openness & interoperability**

Architecture-driven, Multi-concern, Seamless, Reuse-Oriented Assurance & Certification

AMASS Overall Status

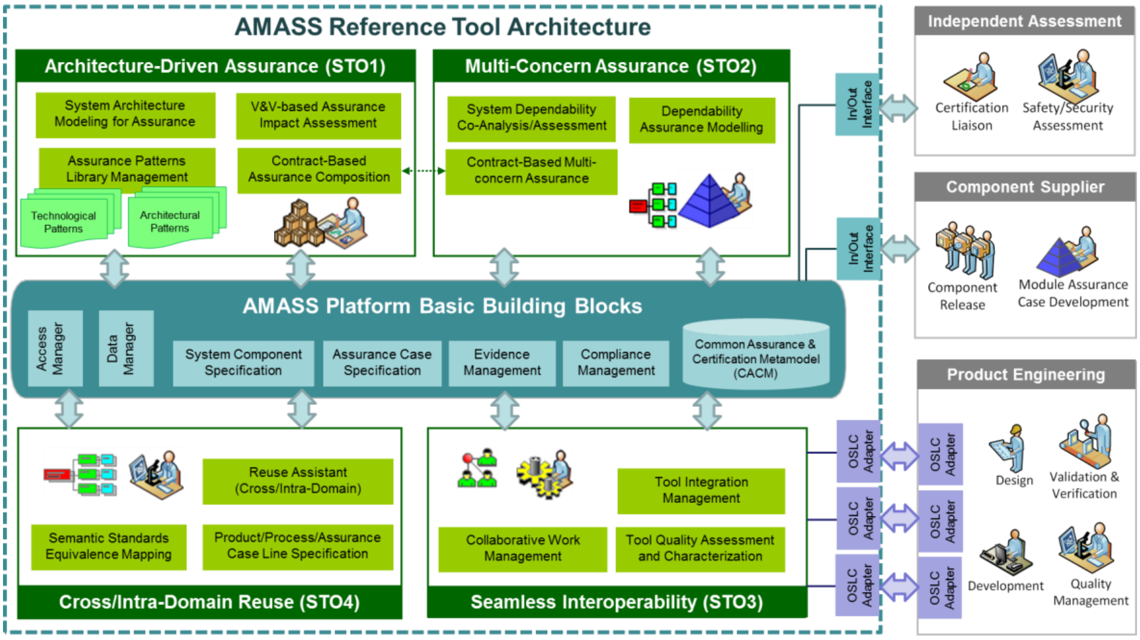
The project started on April 1st and the kick-off meeting took place in Bilbao on April 6th and 7th. Around 50 researchers and practitioners representing the 29 AMASS partners from eight countries attended the meeting and participated in the discussions about the challenges addressed in the project and the ways to maximise its impact.

During the first six months of the project, the AMASS consortium has devoted its technical efforts to both (1) systematically investigate and specify the R&D problems and industrial needs on CPS assurance and certification, and (2) design the basic building blocks of the full AMASS architecture by reusing existing baseline tools.

The first aspect was addressed by different work packages. WP1 was focused on the **particular needs of the project partners concretized on the industrial case studies**. The case studies have been specified by stating the industrial context, the regulatory framework, and the specific needs associated to the AMASS technical objectives and goals. The full consortium has contributed to the definition of industrial usage scenarios. This is part of the deliverable D1.1. WP2 looked at **general needs and requirements for the different industrial domains** targeted by AMASS. WP2 also iteratively revised the specific needs stemming from WP1. The requirements for the first prototype have been brainstormed, collected and formalized in a structured template, and they will be part of deliverable D2.1.

WP3, WP4, WP5 and WP6 focused on a **detailed analysis of the state of the art and state of the practice** for the respective four project objectives. WP3 worked on specifying the background on architecture-driven assurance, including the study of system modelling languages, V&V tools, architectural patterns, and contract-based approaches for compositional assurance. WP4 focused on the survey of multi-concern assurance approaches, including argumentation needs and component contract-related aspects. WP5 was concerned with the related research and industrial work on tool interoperability, data management strategies, UI approaches, and team collaboration features. WP6 conducted a survey of compliance management solutions and process-based and product-based approaches for assurance reuse. These activities have been reported in the deliverables D3.1, D4.1, D5.1 and D6.1. These deliverables provide a straightforward summary of the challenges that AMASS shall face to achieve its goals. They also pave **the way forward towards the achievement of AMASS goals**.

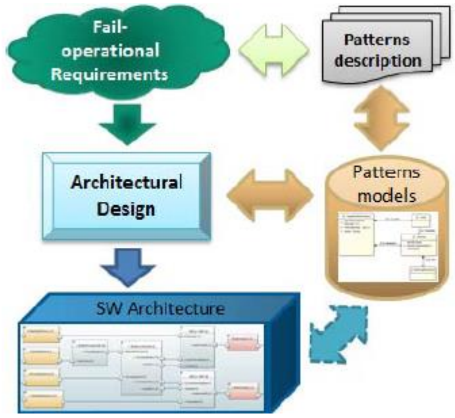
Regarding the second aspect, the consortium started to specify the **AMASS Reference Tool Architecture (ARTA), the Common Assurance and Certification Metamodel (CACM), and the approaches for compliance management, evidence management, assurance case specification, and system component specification**. These are the basic building blocks to develop in Year 1. In-depth discussions took place about the existing solutions that AMASS could reuse, as well as about the challenges to tackle. It was concluded that the results from SafeCer and OPENCOSS can be combined so that AMASS takes advantage of both, and that a deeper analysis of certain modelling languages and metamodels is necessary to determine how AMASS can use them, e.g. the Structured Assurance Case Metamodel (SACM) and the Software and System Process Engineering Metamodel (SPEM). The analysis of the languages, of their metamodels, and of their combination also enables the study of possible solutions for cross- and intra-domain assurance reuse. The result of these activities is part of deliverable D2.2, where three AMASS design perspectives are developed: logical view (functionality concretized in use cases), structural view (how the amass building blocks are composed and connected), and interaction view (the data and control exchange between AMASS tool blocks).


AMASS Reference Tool Architecture
Architecture-Driven Assurance (STO1)
System Architecture Modeling for Assurance
V&V-based Assurance Impact Assessment
Assurance Patterns Library Management
Contract-Based Assurance Composition
Technological Patterns
Architectural Patterns
Multi-Concern Assurance (STO2)
System Dependability Co-Analysis/Assessment
Dependability Assurance Modelling
Contract-Based Multi-concern Assurance
In/Out Interface
In/Out Interface
AMASS Platform Basic Building Blocks
Access Manager
Data Manager
System Component Specification
Assurance Case Specification
Evidence Management
Compliance Management
Common Assurance & Certification Metamodel (CACM)
Reuse Assistant (Cross/Intra-Domain)
Semantic Standards Equivalence Mapping
Product/Process/Assurance Case Line Specification
Cross/Intra-Domain Reuse (STO4)
Tool Integration Management
Collaborative Work Management
Tool Quality Assessment and Characterization
Seamless Interoperability (STO3)
OSLC Adapter
OSLC Adapter
OSLC Adapter
Independent Assessment
Certification Liaison
Safety/Security Assessment
Component Supplier
Component Release
Module Assurance Case Development
Product Engineering
OSLC Adapter
OSLC Adapter
OSLC Adapter
Design
Validation & Verification
Development
Quality Management

Baseline on Architecture-Driven Assurance

AMASS aims to provide a modelling language (metamodel), tools, and techniques to support architecture-driven assurance, i.e., an assurance that exploits and is linked to the system architecture in order to show system dependability.

For **system architecture modelling for assurance**, it appears that there is currently a trend towards extending modelling languages (e.g. SysML) to better and explicitly support the concepts and needs from assurance standards. Concerning **assurance patterns library management**, further investigation needs to be carried out to develop enhanced libraries that cover not only safety argumentation patterns but also some other concerns, e.g. as security. **Assurance of novel technologies** might require the adaptation of standards' requirements to address technology-specific needs. Finally, regarding **contract-based assurance composition approaches**, standard architectures (e.g., AUTOSAR in the automotive industry) require some safety/security architectural patterns definition and application, and auto-generation of platform models and configurations based on these patterns.



Baseline on Multi-Concern Assurance

The review of the state of the art on multi-concern assurance has covered **co-design, co-analysis, co-V&V, and co-assurance of multiple dependability aspects**. Especial attention has been paid to **safety and security co-engineering** and to the integration of these two concerns. The state of the practice has also been analysed for the application domains of the industrial case studies.

The way forward on multi-concern assurance will focus on safety and security, dealing with challenges such as security-informed safety engineering and the creation of assurance cases that jointly justify security and safety. Nonetheless, other concerns (availability, performance, robustness, reliability…) must also be considered for multi-concern assurance, as evidenced by the current industrial practices and standards.

Baseline on Seamless Interoperability

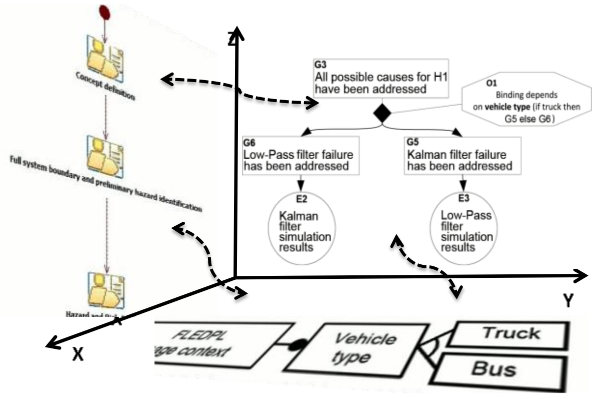
AMASS has analysed the state of the art and the state of the practice related to **seamless interoperability**, especially **on technologies for safety engineering and for safety-critical systems engineering**. It is the same issue that application lifecycle management tools in software engineering have tried to solve for years, with varying success.

Seamless interoperability is a cross-cutting concern across multiple architectural layers, therefore some technologies are orthogonal while others are mutually exclusive. Tool support for systems engineering is usually limited to point-to-point data exchange in some specific data format using import and export functionality. Nonetheless, **recent technologies such as OSLC and ModelBus seem to be promising solutions** to several challenges, e.g. "live" automated collaboration and data exchange. Using modern **web technologies**, it could be possible to close the gaps between tools and allow for a seamless integration.

Baseline on Cross- and Intra-Domain Reuse

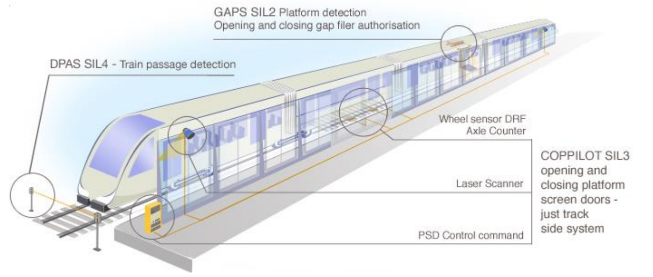
Process-based, product-based, and cross-concern aspects have been considered when analysing the current means for assurance reuse. Different methodological solutions exist to enable **reuse of engineering or assurance artefacts, based on patterns, families, components, and models**.

The proposed way forward consists in a consolidation of existing results from OPENCOSS, SafeCer and other projects, and of some available technology on the market and state of practice. Based on the **three dimensions (process, product, assurance case)**, methods and technologies that could enable systematic reuse include: an EPF Composer-based solution for processes; concerning products, contract-based reasoning, patterns, model-based principles applied to engineering, and variability management; for assurance cases patterns, variability management, contract-based, and module-based argumentation approaches, as well as model-based argumentation.


Concept definition
Full system boundary and preliminary hazard identification
Hazard and Risk
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
Y
X
FLEDPL age context
Vehicle type
Truck
Bus

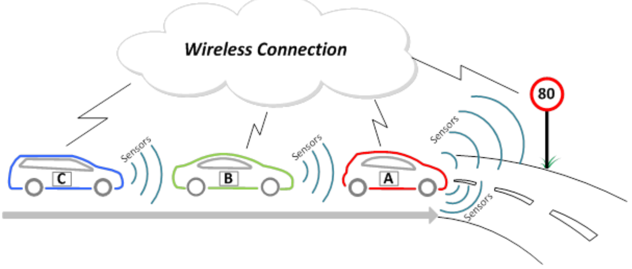
AMASS Case Studies

AMASS will validate and benchmark its results in **11 industrial case studies from six different application domains**: Air Traffic Management, Automotive, Avionics, Industrial Automation, Railway, and Space. The case studies will deal with a variety of system types and with **some of the most novel characteristics and most recent assurance needs of CPS**, e.g. advanced automated and collaborative features of transport systems and the use of new software and hardware technologies in satellites.



Examples of the aspects that will be evaluated in the case studies for each Scientific and Technical Objectives include:

- Architecture-Driven Assurance – link of SysML and Simulink models with assurance models, and application of model- and pattern-based approaches for systematic analysis of functional safety of a cooperative system-of-systems.
- Multi-Concern Assurance – co-analysis of safety and security on the same architectural models of an advanced driver assistance function, and automated support for the creation of assurance cases that address several dependability aspects (safety, security, reliability…).
- Seamless Interoperability – integration of the AMASS platform with commercial engineering tools such as DOORS, IBM Rhapsody, and Matlab, and OSLC-based seamless tool chains.
- Cross- and Intra-Domain Reuse – reuse of assurance information between automotive and avionics, and reuse of qualification dossiers of space components and applications.



The initial validation with the case studies will be conducted at the beginning of 2017, once the first prototype of the AMASS platform is available for its application on case study-specific needs.

AMASS Meetings

In addition to the Kick-off Meeting in Bilbao in April 2016, AMASS arranged a project-wide **Technical Meeting in Vienna in July 2016**.

The overall purpose of the meeting was to discuss the baseline work from which the project needs to develop the AMASS Reference Tool Architecture (ARTA), the Common Assurance and Certification Metamodel (CACM), and the approaches for multi-concern assurance and for cross- and intra-domain assurance reuse. **In-depth discussions took place about the existing solutions that AMASS could reuse, as well as about the challenges to tackle**.

After presenting an overview of SafeCer and OPENCOSS, how to create a first version of the ARTA and the CACM from the results of both projects was discussed. It was concluded that the results from SafeCer and OPENCOSS can be combined so that AMASS takes advantage of both, and that a deeper analysis of certain modelling languages and metamodels is necessary to determine how AMASS can use them, e.g. the current work on the Structured Assurance Case Metamodel and the Common Variability Language. The analysis of the combination and of the languages and metamodels will also enable the study of possible solutions for cross- and intra-domain assurance reuse.

For multi-concern assurance, current standardization work and the basis for security assurance were presented. Several standardization initiatives from different application domains are dealing with both safety and security aspects, and some with the general concern of dependability. A solution for the design of the multi-concern assurance approach was also introduced, focused on argumentation needs and component contract-related aspects.

AMASS Presence at Events (selection)

EclipseCon France 2016. June 7th-9th, 2016, Toulouse (France).

De-CPS 2016: Workshop Challenges and New Approaches for Dependable and Cyber-Physical System Engineering. June 17th, 2016, Pisa (Italy).

INCOSE IS 2016: 26th Annual INCOSE International Symposium. July 18th-21st, 2016, Edinburgh (UK).

IDIMT 2016: 24th Interdisciplinary Information Management Talks. September 7th-9th, Poděbrady (Czech Republic).

ESEM 2016: 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. September 8th-9th, Ciudad Real (Spain).

SASSUR 2016: 5th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems. September 20th, 2016, Trondheim (Norway).

DECSoS 2016: ERCIM/EWICS/ARTEMIS Workshop on "Dependable Embedded and Cyber-Physical Systems and Systems-of-Systems". September 20th, 2016, Trondheim (Norway).

EWICS: European Workshop on Industrial Computer Systems Reliability, Safety and Security meeting. September 20th, 2016, Trondheim (Norway).

SAFECOMP 2016: 35th International Conference on Computer Safety, Reliability and Security. September 20th-23rd, 2016, Trondheim (Norway).

Recent AMASS Publications (selection)

de la Vara, J.L., Génova, G., Álvarez-Rodríguez, J.M., Llorens, J.: *An Analysis of Safety Evidence Management with the Structured Assurance Case Metamodel*. Computer Standards & Interfaces (accepted paper)

Ruiz, A., Gallina, B., de la Vara, J.L., Mazzini, S., Espinoza, H.: *Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems*. 5th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR 2016)

Schoitsch, E.: Autonomous vehicles and automated driving – status, perspectives and societal impact. 24th Interdisciplinary Info. Management Talks (IDIMT 2016)

Gallina, B., Padira, K., Nyberg, M.: *Towards an ISO 26262-compliant OSLC-based Tool Chain Enabling Continuous Self-assessment*. 10th International Conference on the Quality of Information and Communications Technology (QUATIC 2016)

Alajarami, S., Romanovsky, A., Gallina, B.: *Software Development in the Post-PC Era: Towards Software Development as a Service*. 17th International Conference on Product-Focused Software Process Improvement (PROFES 2016)

de la Vara, J.L., Marín, B., Giachetti, G., Ayora, C.: *Do Models Improve the Understanding of Safety Compliance Needs? Insights from a Pilot Experiment*. 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM 2016)

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