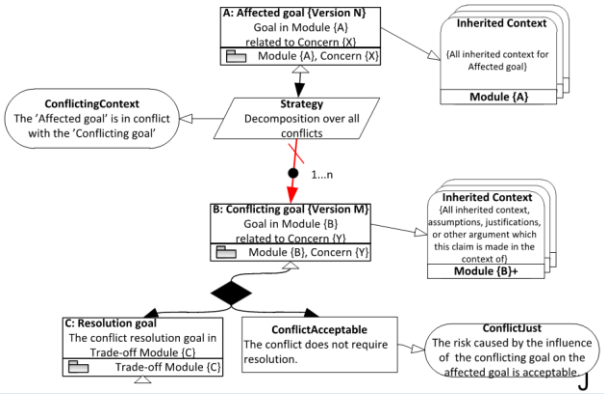
Safety & Security Co-Assessment

When developing a CPS or a CPS component, **the engineers need to ensure the functional safety and the security of the products**. This need affects the following activities for multi-concern assurance:

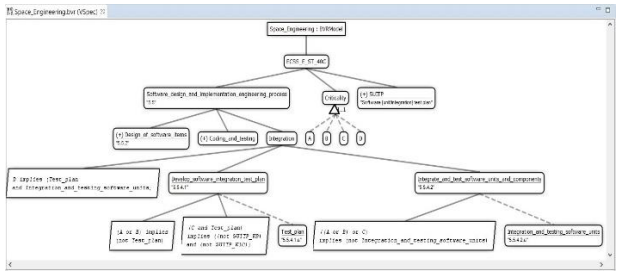
- **Co-Assessment**. Safety and security standards should be digitalised. There are two options in the AMASS Tool Platform: (1) a manager could use the OpenCert tool to model the standards in different reference assurance frameworks and specify the equivalence between them; (2) an engineer could use the EPF Composer to model a combined process of the different standards and next import the resulting model into OpenCert.
- **Co-Design**. The engineers must specify safety and security requirements during product development. These requirements (1) could come from standards and then be refined into technical requirements or (2) could be derived from the design and the risks and vulnerabilities identified. The technical requirements are translated into safety and security properties and mechanisms in the design. To do so, the engineers will include the information into architecture models using the CHESS tool of the AMASS Tool Platform.
- **Co-Analysis**. After design, dependability analyses can be performed, such as model-based or contract-based safety analysis (e.g. using the xSAP feature), safety analysis (e.g. using the ConcertoFLA feature), security analysis (e.g. using the Cyber Architect external tool), and Model Failures Modes Vulnerability & Effects Analysis (e.g. using the FMVEA external tool).

The main decisions and results from these activities can be the basis for assurance case development.



Process & Product Configuration and Compliance

When configuring a new product, e.g. as a product upgrade, **engineers need to comply with both product-related requirements and process-related ones**. Thus, the reconfiguration may affect not only the product but also the process to develop the new configuration. This is particularly evident if a change in the product implies a change in its criticality level. This scenario can be better enacted if systematic reuse support is available.



Variability management at product and process level can support the above situation via the integration of the BVR tool with EPF Composer and the CHESS toolset, all part of the AMASS Tool Platform:

1. An engineer should first investigate if **family-oriented engineering management** is appropriate, evaluating its benefits.
2. If the evaluation is positive, the engineer could use BVR to model a **variability specification** of the product and process dimensions. Next, two new configurations would be generated, for the product and the process, returning a EPF model for the new process configuration and a CHESS component model for the new product architectural specification.
3. Afterwards, **process compliance** could be argued via a new process-based argument, which could be generated automatically from the new process model. Another possibility is to consider the ripple effects of the changes on the corresponding family of arguments. In this case, the engineer should also configure the new arguments. This can be done with the integration of BVR with the Assurance Case editor of OpenCert.
4. **Product safety** could be argued by generating a new argument from the new product specification via the integration of the CHESS, OpenCert, and OCRA tools.

AMASS
ECSEL Joint Undertaking

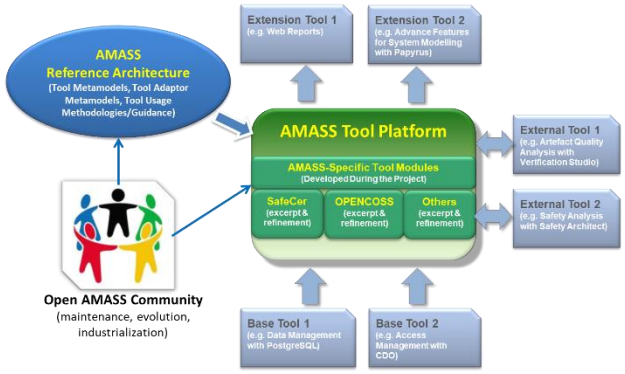
Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

AMASS 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 including automotive, railway, aerospace, space, and energy.

The ultimate goal of AMASS is to **lower 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 seamless interoperability** between assurance and engineering activities along with third-party activities (e.g. external assessments and supplier assurance).

AMASS work has built on the **outcomes from previous successful EU projects** such as OPENCOSS, SafeCer, and CRYSTAL. The results have been validated in **11 industrial case studies** from aerospace, automotive, avionics, industrial automation, and railway.

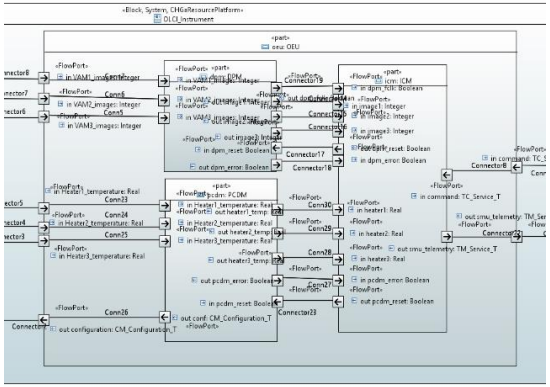
The resulting **open source ecosystem and community** are managed as an Eclipse project.



Architecture Refinement

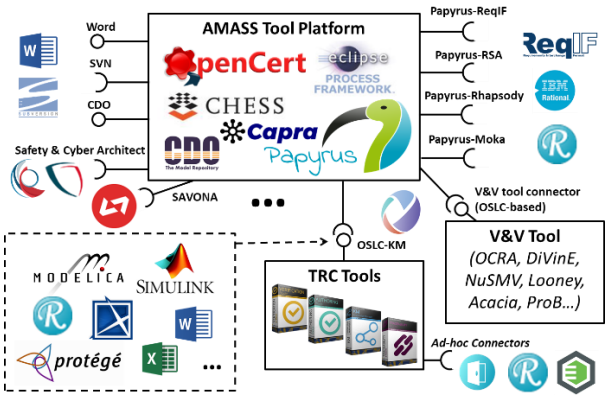
The AMASS Tool Platform supports **system architecture design refinement for reuse and improvement of system assurance**, as a part of architecture-driven assurance. The main steps of this activity are:

1. **System definition**. A system architecture can be modelled by using the Papyrus SysML tool (part of the AMASS Tool Platform) or by using an external tool (e.g. Rhapsody). Components are defined out of context and then instantiated for the target environment.
2. **Requirements early validation**. The engineer can use OpenCert features to analyse system requirements; e.g their quality and their formal properties.
3. **Functional refinement**: Using SysML IBD, requirements are assigned to components and contracts are specified for components as a pair of assumptions and guarantees of formal properties.
4. **Component's nominal and faulty behaviour definition**. This can be specified with state machines or with Simulink models extended with fault injection.
5. **Functional early verification**. The OCRA tool can perform contract-based verification of refinement and state machines, model checking, and contract-based monitoring of Simulink models.
6. **Safety Analysis**. The engineer should perform different safety analyses, such as simulation-based fault injection, model-based safety analysis, and contract-based safety analysis.
7. **Safety case development**. After completing the previous steps, the engineer can generate automatically safety argument fragments that will be part of the whole system assurance case.



Toolchain for System Specification and Quality Assessment

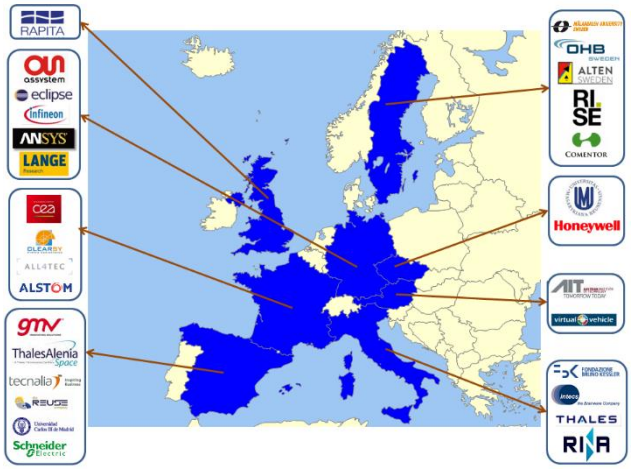
Toolchains play a major role in CPS assurance and certification. CPS engineering is supported by different tools (for system analysis, specification, V&V, etc.). Data from the tools could be necessary in the AMASS Tool Platform for assurance and certification purposes, a tool could need data from another for a different task (e.g. requirements data for quality analysis), and data from a tool can be used as assurance evidence. **Means to enable data exchange between tools, including the AMASS Platform, are necessary** for seamless interoperability.



For example:

- For **requirements specification**, an engineer might use different tools, such as DOORS, PTC Integrity, Excel, and Word, and even Papyrus/CHESS.
- Papyrus/CHESS is the **system modelling** tool proposed by AMASS, but others exist (Rhapsody, MagicDraw, RSA, Simulink, SAVONA…). An engineer might need to exchange model data with them.
- Assurance engineers need to confirm that **artefact quality** is sufficient, thus it must be analysed (e.g. the consistency). The Verification Studio tool supports the analysis based on metrics. The tool exploits OSLC KM as a generic technology for tool interoperability.
- For **traceability management**, the OpenCert Evidence Editor can be used as the default tool, and Capra and Traceability Studio for advanced features.
- OSLC KM supports **data import** into the AMASS Tool Platform, and **data export** can be performed for Word documents and via an API.

AMASS in a Nutshell



H2020-ECSEL-2015 Research & Innovation Action
Apr 2016 - Mar 2019
29 partners from 8 countries
EUR 20.5M budget
EUR 6.2M EU funding
EUR 4.2M national funding
Approx. 2500 persons/month

Web: http://amass-ecsel.eu/
Open Source Project: https://polarsys.org/opencert/
Twitter: @AMASSproject

Coordination
Tecnalia Research & Innovation
Dr. Alejandra Ruiz
Alejandra.Ruiz@tecnalia.com

ECSEL Joint Undertaking

European Commission

AMASS has received funding from the ECSEL JU under the grant agreement No 692474. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and from Spain, Czech Republic, Germany, Sweden, Italy, United Kingdom, and France.