Publishable Summary

Background

Embedded systems have significantly increased in technical complexity towards open, interconnected systems. This has exacerbated the problem of ensuring dependability in the presence of human, environmental and technological risks. The rise of complex Cyber-Physical Systems (CPS) has led to many initiatives that promote reuse and automation of labour-intensive activities. Two large-scale projects are **OPENCOSS** and **SafeCer**, which dealt with **assurance and certification** of software-intensive critical systems using incremental and model-based approaches. OPENCOSS defined a Common Certification Language (CCL), unifying concepts from different industries in order to build a harmonized approach that can reduce time and cost overheads, via facilitating the reuse of certification assets. SafeCer developed safety-oriented process lines, a component model, contract-based verification techniques, and process- and product-based model-driven means for compositional development and certification.

OPENCOSS and SafeCer approaches are largely complementary. SafeCer focused on developing solutions and tool chains for modelling, verification, and certification of critical systems, but a more effective integration for cross-domain reuse can be obtained using OPENCOSS CCL-based approach. On the other hand, the SafeCer solutions can enhance the OPENCOSS tools with the links between the assurance case-centred approach and the modelling and verification approaches for system properties, component contracts, systematization of commonalities and variabilities, model-driven safety certification, and safety analysis.

Both approaches also have some key opportunities to evolve. While the OPENCOSS and SafeCer technological solutions target assurance and certification activities, providing a **seamless interoperability between these activities and engineering activities** (i.e., design, implementation, validation and verification), along with third-party activities (e.g., external assessments, supplier assurance) is of prime importance to lower the threshold of product assurance and certification in face of rapidly changing product features and market needs. Similarly, the standard architectures (such as AUTOSAR in the automotive industry and IMA in avionics) needed to handle these new large, networked systems are only now being equipped with mechanisms to handle dependability-related aspects (including safety, security, availability, robustness and reliability). **OPENCOSS and SafeCer approaches are agnostic regarding system architectural and engineering choices**. This is an intentional feature to meet key requirements about cross-domain harmonization and flexibility. However, the need for more cohesively integrated approaches (assurance/certification versus engineering activities) requires further research and industrial validation with standard and modern engineering practices (e.g., AUTOSAR-driven model-based development). In addition, SafeCer focused on safety aspects in its processes and tools, and only at the end of the project it was envisioned that a holistic multi-concern approach, integrating cybersecurity aspects, should be developed. Finally, the OPENCOSS and SafeCer approaches need a **strong industrial adoption program** to create an open infrastructure and ecosystem in order to facilitate its integration with other ecosystems for CPS development (e.g. other ECSEL platforms).

Technical approach and key innovation

AMASS will **create and consolidate** a **de-facto European-wide assurance and certification open tool platform, ecosystem and self-sustainable community** spanning the largest CPS vertical markets. The project will start by combining and evolving the OPENCOSS and SafeCer technological solutions towards end-user validated tools, and will enhance them and perform further research into new areas not covered by those projects. The ultimate aim is to lower certification costs in face of rapidly changing product 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** (compliance demonstration, impact analyses, and compositional assurance of ***security*** and ***safety*** aspects), and for **seamless interoperability** between assurance/certification and engineering activities along with third-party activities (external assessments, supplier assurance).

The tangible results of the projects will be:

d) ***AMASS Reference Tool Architecture***, which will extend the OPENCOSS and SafeCer conceptual, modelling and methodological frameworks for architecture-driven and multi-concern assurance, as well as for further cross-domain and intra-domain reuse capabilities and seamless interoperability mechanisms (based on OSLC specifications).

e) ***AMASS Open Tool Platform***, which will correspond to a collaborative tool environment that supports CPS assurance and certification. The AMASS Tool Platform is a concrete implementation of the AMASS Reference Tool Architecture, with a capability for evolution and adaptation, and will be released as an open technological solution by the AMASS project. AMASS openness is based on both standard OSLC APIs with *external tools* (e.g., engineering tools including V&V tools) and on open-source release of the AMASS building blocks.

f) ***Open AMASS Community***, which will manage the project outcomes, for maintenance, evolution and industrialization. The Open Community will be supported by governance board, rules, policies, and quality models. This includes support for AMASS *base tools* (tool infrastructure for database and access management, among others) and *extension tools* (enriching AMASS functionality).

These results represent innovative means towards improved assurance of CPS architectural concerns, the development of the multi-concern assurance concept, seamless assurance, further support for assurance reuse, and the enhancement and extension of technologies for CPS assurance and certification. The results will ultimately allow AMASS: (1) to demonstrate a potential gain for **design efficiency** of complex CPS by reducing their assurance and certification/qualification effort by 50%; (2) to demonstrate a potential **reuse of assurance results** (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities; (3) to demonstrate a potential raise of technology innovation led by 35% reduction of **assurance and certification risks** of new CPS products, and; (4) to demonstrate a potential sustainable impact in CPS industry by increasing the **harmonization and interoperability** of assurance and certification/qualification tool technologies by 60%.

Demonstration and use

The achievement of the project's overall goals will be demonstrated through a continuous evaluation of AMASS results over nine industrial case studies in six domains:

- Advanced driver assistance function with electric vehicle sub-system, Collaborative automated fleet of vehicles, Connected hybrid powertrain, and telematics function in the automotive domain
- Safety assessment of multi-modal interactions in cockpits in the avionics domain (also addressing cross-domain reuse with automotive)
- Industrial drive in the industrial automation domain
- Design and safety assessment of on-board software applications in the space domain
- Platform screen-doors controller in the railway domain
- Safety-critical software lifecycle of a monitoring system for radio-navigation equipment in the air traffic management domain

Scientific, economic, and societal impact

AMASS consortium consists of 30 partners from 8 countries with wide experience in critical system assurance and certification. The consortium covers the whole value chain for CPS assurance and certification:

- OEMs (including system integrators) and Component suppliers will use AMASS results in order to increase CPS design efficiency, reduce assurance and certification costs, ease innovation, and reduce assurance and certification risks
- 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
- Research partners will be able to reach a leading position in research on CPS assurance and certification by contributing to the development and assessment of top-notched, flagship solutions

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.