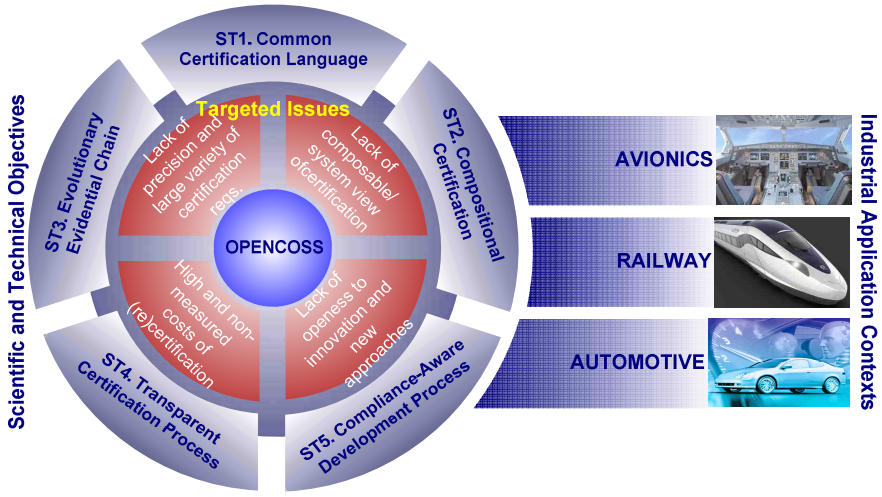
OPEN PLATFORM FOR EVOLUTIONARY CERTIFICATION OF SAFETY-CRITICAL SYSTEMS

OPENCOSS

Key innovation

Safety assurance and certification are amongst the most expensive and time-consuming tasks in the development of safety-critical embedded systems. European innovation and productivity in this market is curtailed by the lack of affordable (re)certification approaches. Major problems arise when evolutions to a system entail reconstruction of the entire body of certification arguments and evidence. Further, market trends strongly suggest that many future embedded systems will be comprised of heterogeneous, dynamic coalitions of systems of systems. As such, they will have to be built and assessed according to numerous standards and regulations. Current certification practices will be prohibitively costly to apply to this kind of embedded systems.

OPENCOSS will devise a **common certification framework** that spans different vertical markets for **railway, avionics** and **automotive** industries, and establishes an open-source safety certification infrastructure. The infrastructure will be realised as a tightly integrated solution, supporting interoperability with existing development and assurance tools. The ultimate goal is to reduce recurring safety certification cost across systems by 40% and across vertical markets by 30%. At the same time product safety will be increased by 20%. Both will boost innovation and system upgrades considerably.



The technical approach

OPENCOSS promotes a **compositional** and **evolutionary certification** approach with the capability to reuse safety arguments, safety evidence, and contextual information about system components, in a way that makes certification more **cost-effective**, **repeatable**, and **scalable**. The technical approach to achieve the project's goals consists of the following key elements:

Contract number

289011

Project coordinator

TECNALIA R&I

Contact person

Dr. Huascar Espinoza

TECNALIA / ESI

Parque Tecnológico Zamudio #202

E-48170 Bizkaia, Spain

Tel: +34 946440400

Fax: +34 94600299

huascar.espinoza@tecnalia.com

Project website

www.opencoss-project.eu

Community contribution

8.44 Mio Euro

Project start date

01 10 2011

Duration

42 months

- Defining a **common safety certification language** to improve mutual recognition of safety approvals based on a shared cross-domain nomenclature.
- Developing rigorous methods for **reuse of safety information**, so that components are easier to certify when integrated into different systems and different application domains.
- Developing an **open-source infrastructure** to facilitate collection of safety evidence, construction of safety arguments based on the evidence, and conducting safety assessments.
- **Benchmarking** the developed tool infrastructure against industrial cases from the railway, avionics and automotive industries.
- **Community building** and **standardisation** of the project outcomes.

We will employ a number of measures to maximize industrial impact, including, most notably: (1) mapping the commonalities and discrepancies between different safety standards (e.g. IEC 61508, DO-178) to improve communication and facilitate **reuse in certification**; (2) bringing together and unifying the "process-based" and "product-based" certification paradigms, with the former drawing on standards, and the latter on the emerging notion of **assurance cases**.

Project partners	Country
TECNALIA R&I	ES
ALSTOM Transport	FR
RINA	IT
TU Eindhoven	NL
AdaCore	FR
Parasoft	PO
Intecs	IT
ATEGO UK	UK
SIMULA	NO
IKV++	DE
ATEGO France	FR
DNV ITGS	FR
Altreonic	BE
HPDahle	NO
University of York	UK
Centro Ricerche FIAT	IT
THALES Avionics	FR

Demonstration and Use

The achievement of the project's key goals will be demonstrated through a continuous evaluation of the developed conceptual framework and tools over three representative use cases:

- In the railway domain, ALSTOM will apply OPENCOSS outcomes for certifying an **on board ERTMS** (European Rail Traffic Management System) in the case of a customer delivery, where the presence of ERA (European Railway Agency) as part of the advisory board will help the approach to be aligned with the strategy of the agency.
- In the avionics domain, THALES will utilize the newly-developed methods to measure the reuse gains in the re-certification of a highly **modular platform onboard aircraft**, composed of both hardware and software.
- Finally, in the automotive domain, FIAT will use the development of an **electric vehicle subsystem** as a context to evaluate the effectiveness of the OPENCOSS outcomes for conducting systematic qualification of safety-critical embedded automotive systems.

Key features:

- Reduction of recurring safety certification costs across systems by 40% and across vertical markets by 30%
- Reduction of product safety risks by 20%
- Increasing product innovation and upgrading by 20%

Scientific, Economic and societal Impact

Scientifically, **universities** and **research institutes** (Simula, TU Eindhoven, University of York, Tecnalia) will be placed at the forefront of research in a very competitive international environment, thus paving the way to improving next generation of safety assurance and certification approaches.

Economically, **industrial contractors** (Thales, FIAT, Alstom) will benefit from the project results by shortened certification cycles, thus lower development cost and faster time to market which are major competitive advantages. **Suppliers** (AdaCore and Altreonic) as well will reduce the time and cost needed to qualify their components and, in addition, will commercialize the same component across different domains which will increase their revenues and competitive position. **Certification bodies** (RINA, DNV) will profit from project results by running certification processes faster and more accurately. **Consultancy organizations** (Intecs and DNV) will be able to apply their safety expertise in a broader spectrum of industrial domains. **Tool vendors** (Atego, Parasoft, ikv+) have an unprecedented opportunity of creating a new breed of tools which supports the safety assurance and certification process, and which is well integrated with other system development tools. To enable rapid adoption, the tools will be **open source** but the tool vendors will create added value services around those tools.

European citizens will benefit from safer and cheaper embedded system devices.