SEVENTH FRAMEWORK PROGRAMME

Proj. N	289011
Kick-Off	Oct 2011
Duration	3 ½ years
Budget	8.4 Meuro

Large-scale integrating project (IP)

OPENCOSS

Open Platform for EvolutioNary Certification Of Safety-critical Systems

Project Motivations and Overview

Paolo Panaroni (INTECS)
Fulvio Taglabo (CRF)
Vincenzo Manni (RINA)

Automotive SPIN, Milan, 1 december 2011

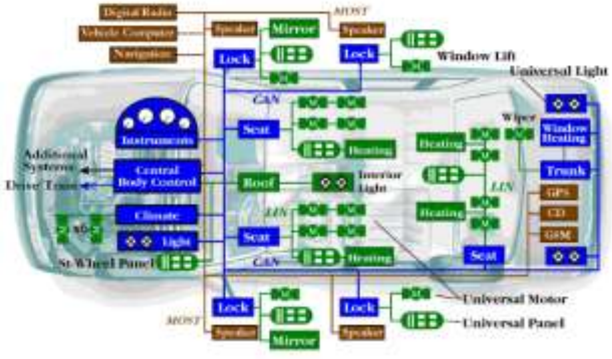
Project partners	Country
TECNALIA R&I	ES
ALSTOM Transport	FR
RINA	IT
TU/e	NL
AdaCore	FR
Parasoft	PO
Intecs	IT
ATEGO UK	UK
SIMULA	NO
IKV++	GE
ATEGO France	FR
Det Norske Veritas	FR, NL
Altreonic	BE
HPDahle	NO
University of York	UK
Centro Ricerche FIAT	IT
THALES Avionics	FR

Background (onboard electronics are pervasive!)

Modern transportation systems are increasingly dominated by electronics /software:

Computers on wheels, Computers that fly

A modern luxury car has more than 80 Electronic Control Units with millions of lines of software code



The electronics are mainly intended to:

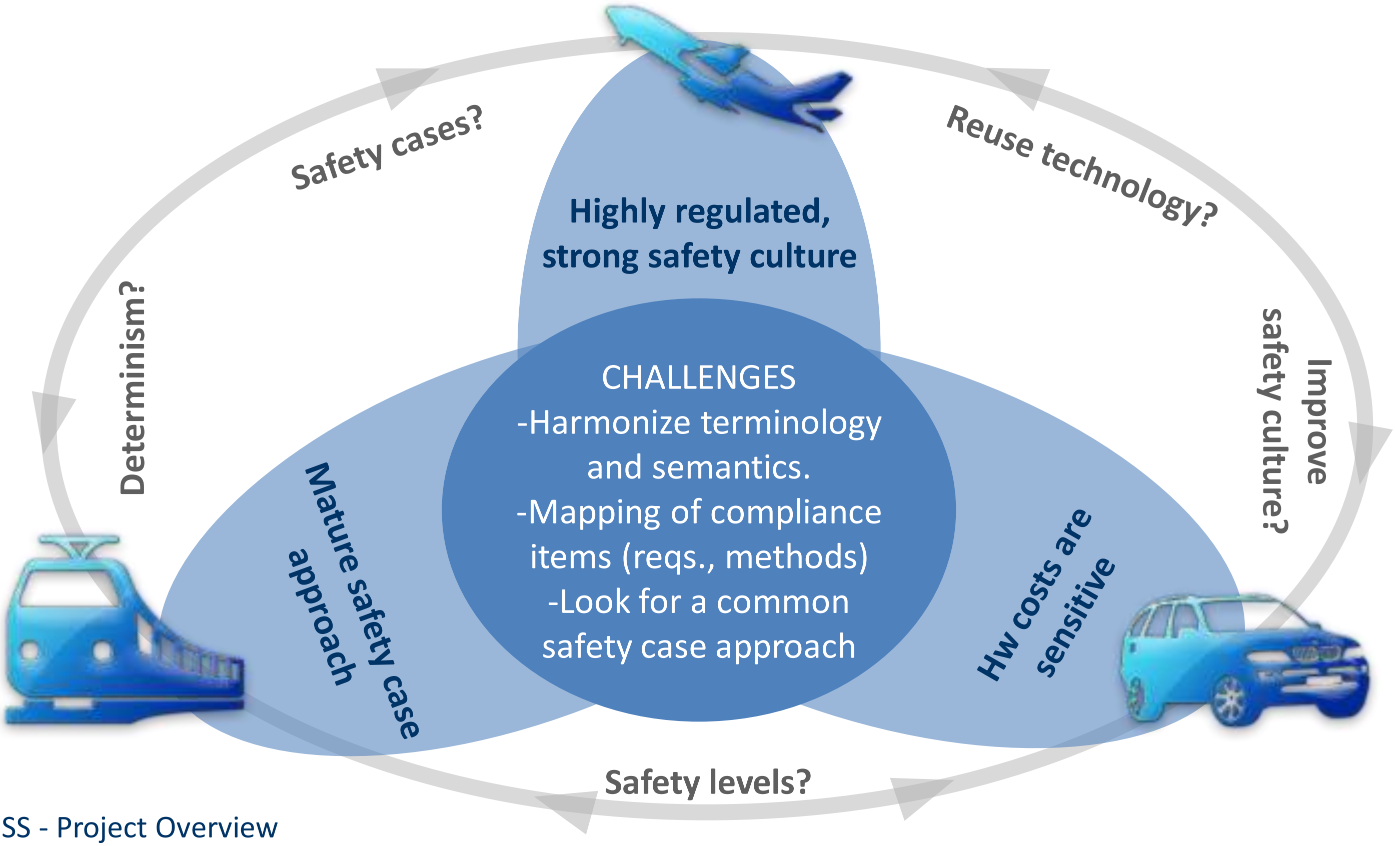
- ***increase passengers safety***
- ***improve comfort, functions, performance***
- ***reduce energy consumption***

The challenge of a cross-domain framework

- System complexity and market demand requires industry to **redefine its reuse strategy**.

- Domain-specific applications are more and more **open to the "external world"**: systems interdependency and Systems of Systems (SoS).

- **Large variety** of definitions/interpretations, technology/architectures and regulation/culture levels.



CHALLENGES
-Harmonize terminology and semantics.
-Mapping of compliance items (reqs., methods)
-Look for a common safety case approach

Strong European Project Team accepting the challenge

tecnalia

ALSTOM

THALES

CRF CENTRO RICERCHE FIAT

simula.

DNV MANAGING RISK

inspearit

atego

PARASOFT

AdaCore
The GNAT Pro Company

intecs
the Brainware company

ikv

Altreonic

HPDahle

RINA
150 YEARS

TU/e Technische Universiteit Eindhoven University of Technology

THE UNIVERSITY *of York*

- *Major transportation industries*
- *Major suppliers*
- *Certification organizations*
- *Consultancy organizations*
- *Tool Vendors*
- *University & Research Institutes*

Supported by (Advisory Board):

European Railway Agency
Cross Acceptance Unit

EUROCOPTER
AN EADS COMPANY

eclipse

Problems and Challenges

- Electronic systems shall not introduce hazards due to possible malfunctions or incorrect specifications
- Society demands adoption of high safety standards
- Different transport sectors (railway, automotive, avionics) have developed their own specific set of standards (a «Babel Tower»)

1. High initial «certification» costs and long schedules
2. High «re-certification» costs when products evolve
3. Difficulty in reusing «pre-certified» components
4. Difficulty in sharing expertise and pre-certified components from different transport sectors (Babel Tower effect)

The Four Pillars of our Approach

1. **Identify a «common safety/certification language» across the different transport sectors (challenge the Babel Tower);**

2. **Identify methods (e.g. safety cases) to better substantiate the satisfaction of safety goals. We will strive to introduce more cost effective and precise «model-centric» approaches in place of current bureauocratic document-centric approaches;**

3. **Develop methods to manage the safety of a complete system built from a set of «pre-certified» components, including those available from different transport sectors (compositional) as well as fast path to re-certification changes to already certified systems (evolutionary);**

4. **Develop an open source platform and a set of tools to support faster and more accurate safety assessment, including «re-certification» after system changes.**

Automotive statement/clarification

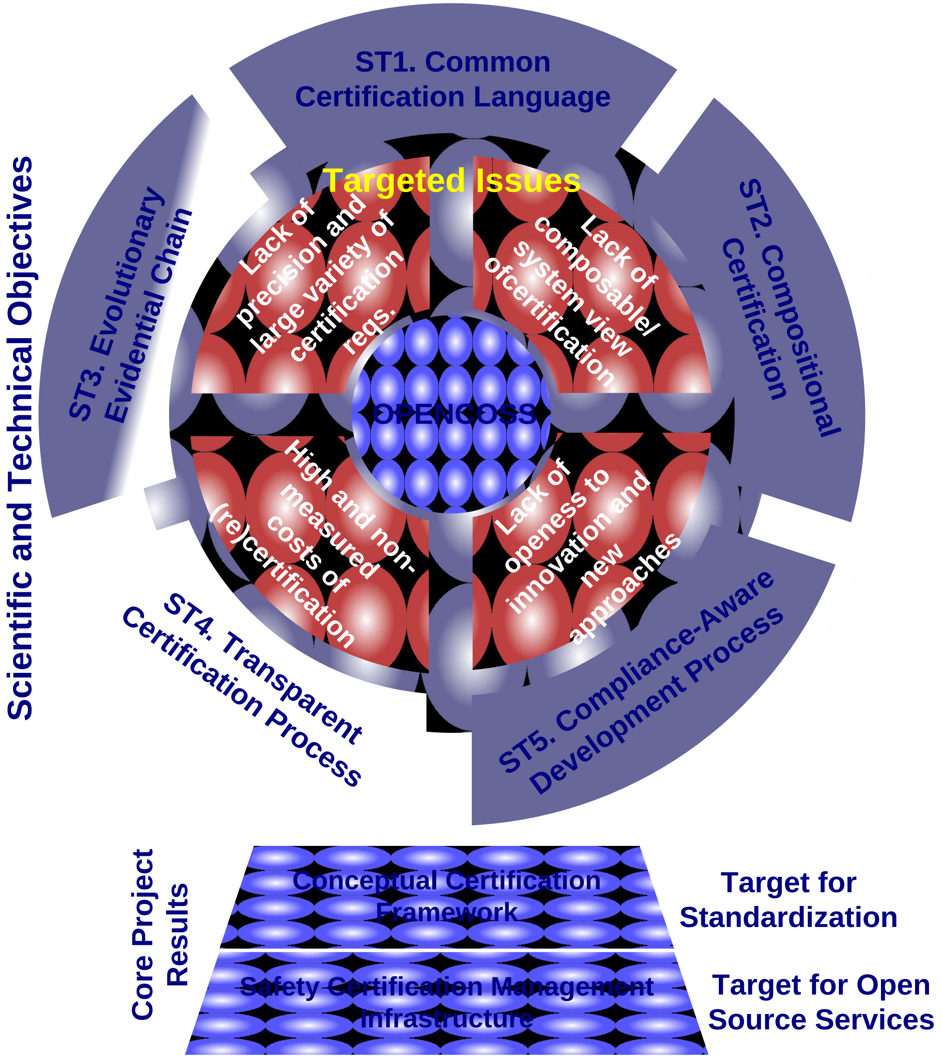
The choice of the automotive field has been to have not a traditional certification approach. It does not exist any certification rule, and consequently any national bodies devoted to accredit companies for the emission of the Certificate.

The standard defines the "Functional Safety Assessment" at the completion of the item development with the scope to assess the functional safety that is achieved by the "item" (item – element under safety analysis).

This conformity assessment shall be performed by an organization independent from the department that has performed the functional safety of the item.

Note: the assessor could be a person of a different department of the same company, i.e. independent from department responsible for the considered work product(s) regarding management, resources and release authority.

OPENCOSS at a Glance



Scientific and Technical Objectives

ST1. Common Certification Language

ST2. Compositional Certification

ST3. Evolutionary Evidential Chain

ST4. Transparent Certification Process

ST5. Compliance-Aware Development Process

Targeted Issues

Lack of precision and large variety of certification reqs.

Lack of composable/ system view ofcertification

High and non-measured costs of (re)certification

Lack of openess to innovation and new approaches

OPENCOSS

Core Project Results

Conceptual Certification Framework

Target for Standardization

Safety Certification Management Infrastructure

Target for Open Source Services

Industrial Application Contexts

AVIONICS

RAILWAY

AUTOMOTIVE

Stay in touch

OPENCOSS

Project Coordinator*:*	*Huascar.Espinoza@tecnalia.com*
Dissemination Mngr*:*	*Paolo.Panaroni@intecs.it*
Visit our web site:	*www.opencoss-project.eu*
Linkedin group:	*opencoss (>120 participants)*

The project is OPEN !!

all results will become public documents and open source software

SafeCer

SAFETY CERTIFICATION OF SOFTWARE-INTENSIVE SYSTEMS WITH REUSABLE COMPONENTS

ARTEMIS

Safety Certification of Software-Intensive Systems with Reusable Components

Advanced Research & Technology for Embedded Intelligence and Systems

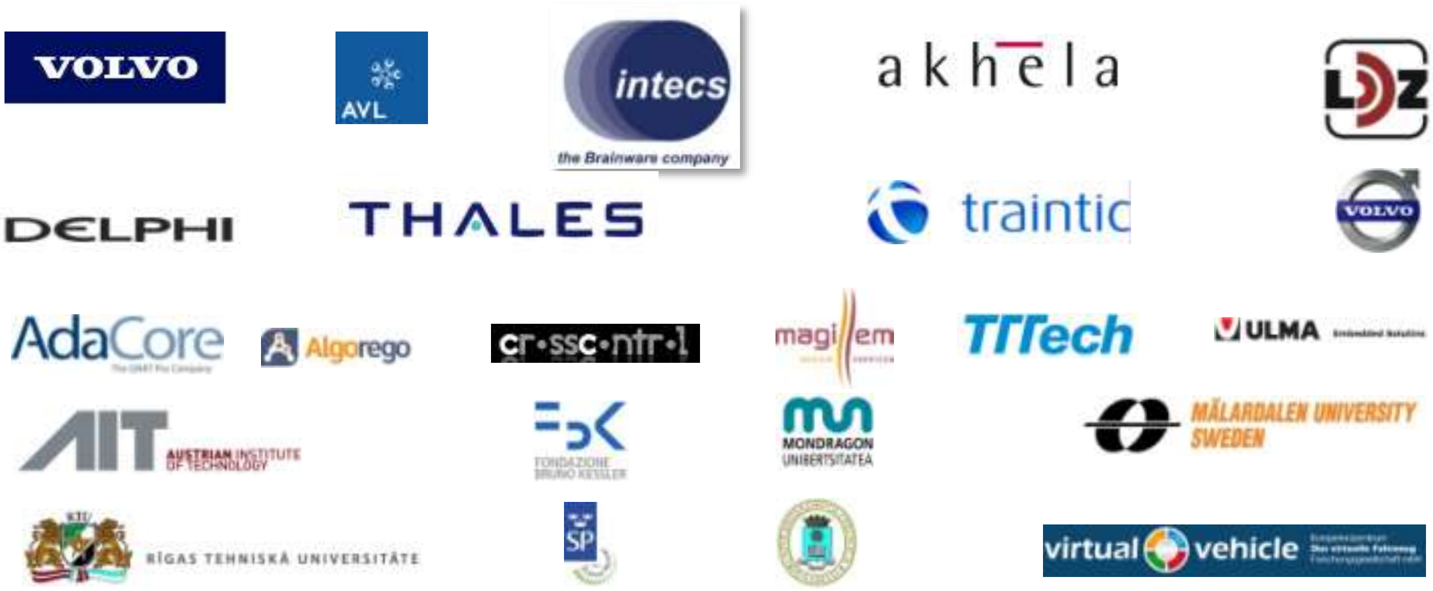
ARTEMIS Joint Undertaking

The public private partnership for R&D actors in embedded systems

Project started April 2011

- ***International research project targets increased efficiency and reduced time-to market by composable safety certification of safety-relevant embedded systems***

The SafeCer consortium



Technological Innovation

- aim is to enhance existing CBD Component Based Development frameworks by extending them to include dependability aspects so that the design and the certification of systems can be addressed together with a manageable amount of work.