NEWSLETTER – N. 1 – April 2012

OPEN PLATFORM FOR EVOLUTIONARY CERTIFICATION OF SAFETY-CRITICAL SYSTEMS

EDITORIAL

OPENCOSS HAS STARTED!

The Babel Tower of the so many different approaches to embedded systems safety is now under attack - at least for the transportation domains including avionics, railway and automotive.

On Monday 3rd to Thursday 6th of October, the Kick-Off Meeting of the FP7 European project OPENCOSS (IP – large scale integrating project) took place at a comfortable conference facility in Bilbao, hosted by TECNALIA/ESI European Software Institute (Spain). The meeting ran for four days, packed with a full schedule of technical and management meetings.

About 40 researchers and practitioners representing 17 European organizations from 9 countries met during the kick off to map out the strategic directions of the project and set up the work plan for the following three and half years. Throughout the meeting, all partners gave presentations about their core areas of competence and current initiatives related to OPENCOSS.

The project consortium includes major manufacturers of transportation systems (ALSTOM, FIAT, and THALES), certification organizations (DNV and RINA), consulting firms and solution providers (Intecs, IKV, ATEGO, AdaCore, Altreonic, and Parasoft), research institutes (TECNALIA and SIMULA), and universities (University of York and Eindhoven University of Technology).

All these organization have joined forces to meet one common objective: reduce certification costs and time while maintaining the highest safety standards.

The existing certification processes are going to be dissected and analyzed in depth, and commonalities across domains will be identified.

A Common Certification Language (CCL) will be defined thus paving the way for certification across transportation domains with only "delta" efforts.

Re-thinking the certification process will allow the stakeholders to minimize rework and to adopt incremental certification running in parallel with the development process. Document-centric will be largely replaced by model-centric certification. Certification costs will be reduced and become more predictable. Subjectivity shall also be reduced by using specific tool support, thus increasing accuracy and auditability. Open-source certification platforms will be set up for a faster and more transparent adoption.

Admittedly, the objectives are ambitious and achieving success will require overcoming a number of roadblocks including, among others, different cultures, different applications domains, consolidated interests in the certification business itself, but the project partners are willing to accept and face the challenge head on.

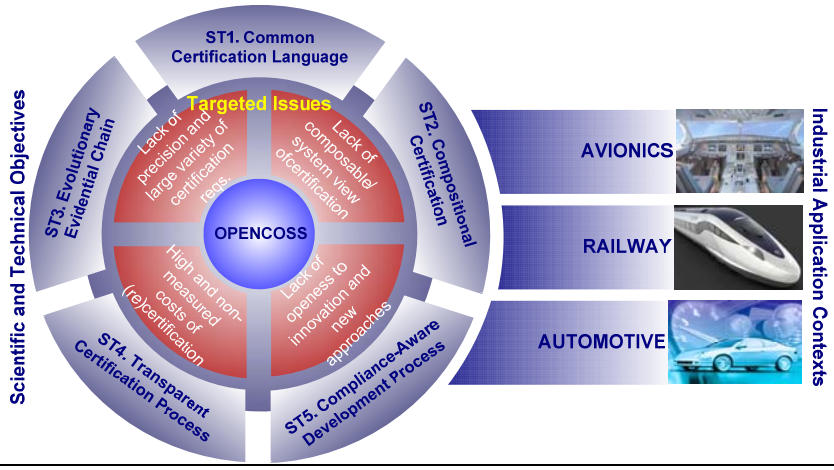
OPENCOSS has been financed by the 7th Framework Programme of the European Commission with a contribution of about 8.4 million Euros for the tenure of the 42-months project (starting date: October 1, 2011).

Visit us at www.opencoss-project.eu, and stay tuned for the project results!

PROJECT OVEVIEW AND GOALS

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.

The OPENCOSS project aims to devise a common certification framework that spans different vertical markets for railway, avionics and automotive industries, and to establish an open-source safety certification infrastructure. The infrastructure is being realized as a tightly integrated solution, supporting interoperability with existing development and assurance tools. The ultimate goal of the project is to bring about substantial reductions in recurring safety certification costs, and at the same time increase product safety through the introduction of more systematic certification practices. Both will boost innovation and system upgrades considerably.



THE CONSORTIUM

A STRONG EUROPEN TEAM

tecnalia	TECNALIA R&I	ES
ALSTOM	ALSTOM Transport	FR
RINA 150 YEARS	RINA	IT
TU/e Technische Universiteit Eindhoven University of Technology	TU Eindhoven	NL
AdaCore The GNAT Pro Company	AdaCore	FR
PARASOFT.	Parasoft	PO
intecs the Brainware company	INTECS	IT
atego	ATEGO UK	UK
simula .	SIMULA	NO
ikv	IKV++	DE
atego	ATEGO France	FR
inspearit Aligning for Customer Value	DNV ITGS => INSPEARIT	FR
Altreonic	Altreonic	BE
HPDahle	HPDahle	NO
THE UNIVERSITY of York	University of York	UK
CRF CENTRO RICERCHE FIAT	Centro Ricerche FIAT	IT
THALES	THALES Avionics	FR

ADVISORY BOARD

EXTERNAL ADVISORY MEMBERS

- Herve Delseny (Airbus, France)
- Ralph Müller (Eclipse Foundation, Europe)
- Luca Trunca (ERA – European Railway Agency, Europe)
- Andreas Keis (EADS / IW)
- George Romanski (Verocel, USA)
- Bert Dexter (Flanders Drive, Belgium)
- Kenji Taguchi (AIST, Japan)
- Eluska Sukia (CAF, Spain)
- Jurgen Niehaus (SafeTrans, Germany)
- Mr. Michael Holloway (NASA, USA)

DOCUMENTS

DELIVERABLES RELEASED (March, 2012)

▪ D9.1 Collaboration Platform	Restricted
▪ D9.2 Dissemination and Training Plan	Public
▪ D1.1 Constraint on the Certification process	Public
▪ D10.1 Project Handbook	Confidential
▪ D4.1 Baselines of the Common Certification Language	Public
▪ D6.1 Baseline of the Evolutionary Evidenctial Chain	Public

PUBLICATIONS

- Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems, Huáscar Espinoza, Alejandra Ruiz (TECNALIA), Mehrdad Sabetzadeh (SIMULA), Paolo Panaroni (INTECS), IEEE ISRE 2012 WOSOCER, Hirosjuma, Japan
- A harmonized multimodel framework for safety environments, Xabier Larrucea (TECNALIA), Paolo Panaroni (INTECS), EuroSPI 2012, Vienna
- Supporting the Verification of Compliance to Safety Standards via Model-Driven Engineering: Approach, Tool-Support and Empirical Validation Rajwinder Kaur Panesar-Walawege, Mehrdad Sabetzadeh, Lionel Briand (SIMULA). Submitted to a Journal, 2012

TRAINING

PROJECT AND RISK MANAGEMENT TRAINING

Tecnalia and HPDahle gave a first internal training on 17 November 2011. Supporting material was provided via the OPENCOSS Subversion repository. The main objective of the training was to familiarize the OPENCOSS consortium with the administrative tasks within the project.

GOAL STRUCTURED NOTATION (GSN) TRAINING

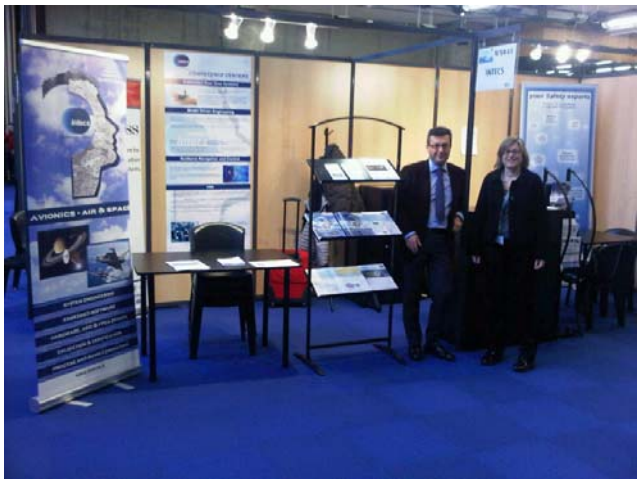
The University of York gave a two-day training on Goal Structured Notation (GSN) at the University of York on 22 and 23 November, 2011. Supporting material was handed out there.

The main objective of the training was to create a common knowledge on the GSN formalism. Numerous participants from OPENCOSS consortium partners attended and feedback was positive.

MODEL-BASED ENGINEERING (MBE) TRAINING

Atego France, Atego UK and Tecnalia gave a training on Model-Based Engineering via Webex on 9 December 2011.

The main objective of the training was to create a common knowledge on model-based engineering and to understand how these concepts can be used in the OPENCOSS project. The training had two main parts. The first one dealt with the basic concepts of MBE (e.g. what is a model, meta-model, profile, modelling language, domain-specific modelling language) and was provided by Atego. The second one dealt with the potential use of modelling and meta-modelling within the OPENCOSS project and was provided by Tecnalia.

MAJOR DISSEMINATION EVENTS	**CONFERENCES**
	The 1st International Workshop on **Software Certification (WoSoCER)** **joined event with IEEE ISSRE Dec 2011, Japan**  The 1st International Workshop on Software Certification (WoSoCER) The WoSoCer'11 deadlines have been extended. Please, see below the new (firm) deadlines. Organizers:
	ERTS Embedded real Time Systems 2012 Toulouse 
	Embedded World 2012 Nuremberg 

COMING SOON

(ORGANISED BY OPENCOSS)

Satellite event of SAFECOMP 2012 Magdeburg 25 Sept

SASSUR (Next Generation System Assurance Approaches for Safety-Critical Systems)

http://www-e.uni-magdeburg.de/safecomp/about-sc-2012/workshops/104-sassur

DISSEMINATION MATERIAL

- Flyer (also called brochure, fact-sheet, leaflet)
- Abstract
- Position Paper (also called white paper)
- Press Release (at project Kick-Off)
- Roll-Up Poster
- Short Presentation
- Long Presentation
- Newsletter (this same document)

OPENCOSS ON THE WEB

PROJECT WEB SITE (www.opencoss-project.eu)

The project community is also visible as a linkedin professional group (> 150 participants), twitter and facebook.

THE LONG TERM VISION

THE SAFETY ASSESSOR DREAM

BACK FROM THE FUTURE !

Disclaimer: *The story presented below is pure imagination, and does not necessarily reflect the position of the whole project consortium nor a commitment. It is intended to speculate about the future of safety certification and foster discussions and new ideas.*

Somewhere in Europe, 21 March **2021**

The context

Joe is a safety assessor. He has a PhD in Safety Engineering awarded at the European Safety Academia and is employed at EuroCERT, an independent and accredited safety assessment organization.
Joe has just been assigned to an innovative project for a new automotive feature called "e-taxi". Basically you drive your car to your chosen destination, get out from the car and, using a mobile phone button, the car autonomously and safely locates the closest authorized parking space. If necessary the car will also autonomously refuel. At any time later, at your convenience, you "recall" the car, that will meet you at a given position at a given time (this is called human-to-car rendez-vous).

The company IntelliCAR is developing the hardware and software system to implement the e-taxi concept. It will soon be marketed as E-TAXI. Joe has to perform the independent safety assessment of the E-TAXI system. He knows it is a tough job and he knows the risks to human lives of authorizing that system on thousands of new vehicles. He also knows the economic cost of a "recall" in case of technical problems. He needs to provide an authoritative statement about the functional risks of that system.

IntelliCAR, is a mature CMMI level 7 organization (CMMI level 5 + safety + security), and is developing the full system using a powerful open source fully integrated system-development tool chain, called OISLC (Open Integrated System Life Cycle). The tool chain includes all tools which support requirements, designing and testing at system, hardware and software level.

The OISLC also has tools to support project management, configuration management, quality assurance and a nice process assistant, that drives the team into a concert of activities along the life cycle, orchestrated by a manager, ensuring proper process execution in the right order and with no omissions.
Moreover, IntelliCAR adopts a reference standard architecture and a large number of both hardware and software building blocks .
Joe needs to ensure that the ISO 26262 "latest edition 5" is fully and adequately applied by IntelliCAR to the system. He will be monitoring the project throughout the life cycle, so as to provide early feedback and recommendations about safety (i.e. *Incremental Safety Assessment*).

The OPENCOSS Safety Navigator

Joe has been using the OPENCOSS platform for 5 years, and is a "satisfied customer" both for efficiency and effectiveness (i.e. more accurate assessments). OPENCOSS is his daily tool. It is called a Safety Assurance/Management Tool.

The E-TAXI project repository is made available to EuroCERT (with a well identified baseline code) and the OPENCOSS tool has immediate access to it (strictly read-only).
OPENCOSS automatically recognizes the E-TAXI repository, its structure and its contents and automatically places all workproducts (evidence) into a "grid" according to the ISO 26262 Edition 5 set of requirements (more than 400, 150 workproducts, 120 tables !).

Joe is not familiar at all with the internal proprietary process used by IntelliCAR to develop the system, but can immediately navigate the repository and identify the document or model which contains the information he has to check.
Traceability is at fine grain to chapter, sections, or even single sentences in a document or model items such as a box, an arrow, etc. OPENCOSS does automatically this "mapping", and highlighted any missing item.

In a sense OPENCOSS acts like a discriminating "lens" that makes it possible to look at the project repository with the "eyes" of the assessor, it provides a repository view called the "safety view". Joe does not have to be familiar with the specific processes and repositories of the various suppliers. It is OPENCOSS that filters out and organizes the information in an appropriate and uniform way.

Joe can then focus only on analyzing the adequacy of workproducts (evidence) in relation to ISO 26262 requirements. All the dirty, expensive and error prone work of collecting and mapping the evidence is done automatically.
OPENCOSS also drives Joe in the systematic and ordered analysis of the evidence, according to a logical workflow. Once items are successfully analyzed, they are marked as "qualified" with a green color. Something wrong is marked as "rejected" with a red color.

A summary is automatically produced in the form of an assessment report.
IntelliCAR has direct access to the assessment report, as it becomes directly visible from its own repository. Issues are connected to evidence and can be managed: the repository is corrected as necessary.

OPENCOSS drives Joe in analyzing the evolution and closing the open issues. Some changes made by IntelliCAR (e.g. a design change) require an impact analysis. OPENCOSS understands the logical connections, dependencies and relationships between evidencs and assists Joe in the ordered impact analysis.

A few days later, after some discussion and effort, the green color pervades the full repository. Everything gets certified and the assessment report is eventually generated with a nicely spelled final sentence like "the system has been successfully assessed in conformance with ISO 26262 Edition 5" and is deemed ready to go into operation.

The OPENCOSS Safety Checker/Validator

Since 2015 the OISLC tool chain supports a full model based approach. Everything in the project repository is a model: requirements, design, test, GANTT, organization charts, etc. The older approach of a huge set of documents has been replaced by a set of coherent and connected **models.**
E.g. Joe does not have to read a narrative textual report to discover that the coverage has achieved 100% on module X, but this information has been automatically loaded by the test tool into an attribute of the module X under test.
The more the information get structured and formalized, the more OPENCOSS can deploy its automatic **safety checking capabilities** and part of the work done by Joe is fully automatized. Joe will focus only on those problems detected by the safety checker.

The safety checker can go beyond: e.g. checking process requirements such as: was this piece of code peer-reviewed ? was the reviewer independent from the tester ? And similar. The safety checker deploy many techniques for model checking, all focused on the safety aspects. It can check safety metrics, validate quantitative safety analysis, etc.
Likewise, the safety checker may verify automatically properly Safety Integrity Level determination and decomposition, leaving Joe to only check adequacy.
Joe is increasingly empowered and involved in highly conceptual tasks rather than checking rules and standards.
As the information is mainly model based, the navigation may take place filtered with a **safety view** (highlight safety relevant information), **product view** (highlight product information) or **process view** (highlight process information, who does, what, when, how). All this information is interconnected. A safety mechanism within the system architecture is highlighted in red. A safety requirement is also highlighted in red within the system requirements. Even a piece of code implementing a safety mechanism is highlighted so as to distinguish it from regular functional code (e.g. with a different red color from source code statements).

The OPENCOSS Evolution Manager (Evolutionary Certification)

IntelliCAR has just launched a new version of its E-TAXI product designed for trucks (called TRUCK-TAXI). As one can imagine TRUCK-TAXI is similar to E-TAXi but a truck poses special challenges and the product is different. IntellCAR decides to apply to EuroCERT for a safety assessment of TRUCK-TAXI as a **derivative** product of E-TAXI.
Once OPENCOSS is informed that this new project is a derivative of a previously analyzed project it is able to identify all the differences and drive Joe in a systematic analysis of impact. Joe is pleased to realize that only 10% of the assessment work has to be re-done and IntelliCAR receives a successful assessment report in just a few weeks.

The OPENCOSS Component Manager (Compositional Certification)

IntelliCAR reuses many elements from previous projects. Most subsystems are the same. They are flagged as "components". OPENCOSS recognizes pre-qualified components and flags them. Joe does not need to analyse those components in detail, but pay attention to the new context in which these components are used. IntelliCAR has sped-up the assessment process by a factor of 2 or more by developing new systems made up of pre-qualified building blocks (components).

The OPENCOSS Cross Domain Manager (Cross Domain Certification)

The E-TAXI solution is getting a great attention on the yacht market and a new version is going to be certified according to maritime standards. OPENCOSS is informed of a derivative project from a different domain and automatically adapts all evidence on the basis of the most recent maritime safety standards.
Joe can now navigate the same project repository using the view of the new standard and any omission will be automatically flagged.

The OPENCOSS Unified Domain Manager (Unified Certification)

However, Joe is not an expert in maritime standards, and he has had to pass the work to Bob.
A recently announced new feature of OPENCOSS however is capable of understanding all the most relevant safety standards and provide a unified (common) safety view. Joe knows this common language (learned at the Safety Academia, developed from an old FP7 project). With this unified approach Joe is able to assess the maritime variants without any trouble.
In fact OPENCOSS automatically verifies the completeness in relation to the many multi domain standards, starting from a common unified model.

Final notes

Over the years the safety standardization community has eventually reached a consensus on a single (cross domain) *unified safety standard* ! Each domain (e.g. automotive, avionics, railway, naval, nuclear, medical, etc.) has occasionally added an *addendum* that provides only specific guidelines for using the *unified safety standard* for that specific domain. The Safety Academia is teaching safety engineering using a single unified safety language (glossary, concepts, patterns, techniques, metrics, etc.). Researchers, practitioners and tool vendors are now converging on this single unified safety discipline. This has led to unprecedented innovation in the technology of safety.

In those rare cases where an accident occurs (in any possible domain) the whole safety community learns from that experience and identifies safety countermeasures applicable to all domains. Not only are accidents analyzed but mainly "near misses", so as to predict and prevent their occurrence.

A **near miss** is an unplanned event that did not result in injury, illness, or damage – but had the potential to do so (wikipedia).

To finish with, the community of **security** has understood the advantage of an Open Platform also for security and they have started a project for an OPENCOSS 2.0 including a **security view** in addition to the safety view. Safety and security mechanisms are highlighted in different colors and tradeoff and balance are made possible.