NEWSLETTER – N. 05 – May 2014

OPEN PLATFORM FOR EVOLUTIONARY CERTIFICATION OF SAFETY-CRITICAL SYSTEMS

The Project in a nutshell	**OPENCOSS** is a European large scale FP7 project (www.opencoss-project.eu). Its objective is to produce the first Europe-wide, open safety certification platform. This is meant to reduce time & cost for (re)certification of safety-critical embedded systems, specifically in the Railway, Avionic and Automotive domains. Want to know more? Choose and download any public deliverable: http://www.opencoss-project.eu/node/7
EDITORIAL **The Tool validated in Case Studies**  **OPENCOSS @ VALIDATION**	The project has been running for two years and half now. Since Newsletter issue 4 (Nov 2013), the project has successfully faced its **3rd EC review**, on mid Jan 2014. As usual, the event represented a valuable opportunity to collect the EC feedback and steer the project where needed. In the period, apart of a general progress on the underlying methodological and conceptual parts, relevant and tangible enhancements have been made on the **Tool Prototype**. This latter, in fact, has been actually utilized (validated) in a number of **Industrial Case Studies**. The resulting feedback has been then returned to the maintenance team, resulting onto tool refinements. The two activities (validation & maintenance) have been carried out in closed loop, and still continues. The chosen case studies are those utilized by the Industrial Partners and cover all addressed domains (Railway, Avionic, Automotive) and their respective safety standards (EN 5012x, DO-178x, and ISO 26262). Three Case Studies have been actually chosen, quite complementary in their cross- or re-certification nature, and thus thoroughly exercising the tool capabilities and providing valuable feedback.

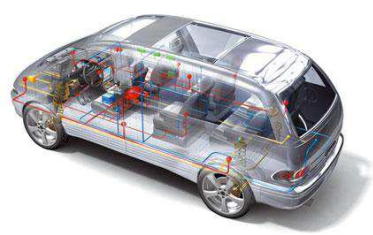
Railway Case Study

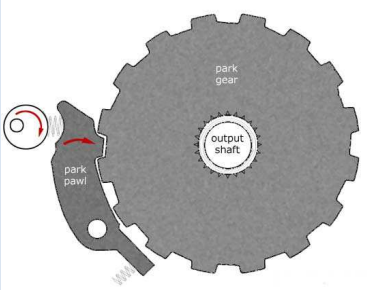
The **Railways-based case study**, developed by Alstom Transport, focused on a part of the European Railway Traffic Management System (ERTMS), On-Board Unit Sub-System (OBU), within the European Vital Computer (EVC). Based on the EN 5012x set of standards, the Opencoss Prototype was thus used to progressively build the Safety Case, assure a Transparent Certification process (e.g. shared view with all stakeholders), and in some extent also the compositional certification, since the OBU hosted some generic products. The Prototype cross features have also been utilized for implementing country-specific requirements, namely the As Low As Reasonably Practicable (ALARP) criteria, as in place in a north European country, and a different Safety Case as desired by a north African country tramway operator. The Opencoss Prototype was successfully used in conjunction with commercial Atego Process Director™.

Avionic Case Study

The **Avionic-based case study**, developed by Thales Avionics, represents a genuine example of cross-certification: an existing Railway product was re-used in the target Avionic domain, with the objective of herein building its Qualification Dossier for certification purposes. This made possible the achievement of concrete cross-domain, objectives compliance, from EN 50128 to DO-178C, according to various, target Design Assurance Levels (A, B, C, D). The technical challenge was to allow the processing platform (processing unit + OS) to be reused from Thales Railway to Thales Avionics, and here within an Integrated Modular Architecture (IMA) compliant framework, including partial/complete certification/safety credits.

Automotive Case Study





The ePARK lock system

The **Automotive-based case study**, developed by Centro Ricerche Fiat (CRF), was based on **SEooC** (Safety Element out of Context), typical ISO 26262 concept, where the "Context" is meant a reference vehicle. The specific SEooC is the **ePARK**, a typical mechatronics device controlling the mechanical locking of the transmission when the Parking mode is selected (by the driver or automatically), thus avoiding undesired vehicle movements. The Prototype has been used for modeling the Automotive Functional Safety process, according to ISO 26262, and for applying a compositional and evolutionary approach through change management, traceability, and tailoring of the safety life-cycle. Indeed the Prototype revealed useful and successful in the general CRF improvement process, resulting onto an enhanced framework organization, standardization, and automated/semi-automated support for ISO 26262 compliance evaluation and evidence reuse.

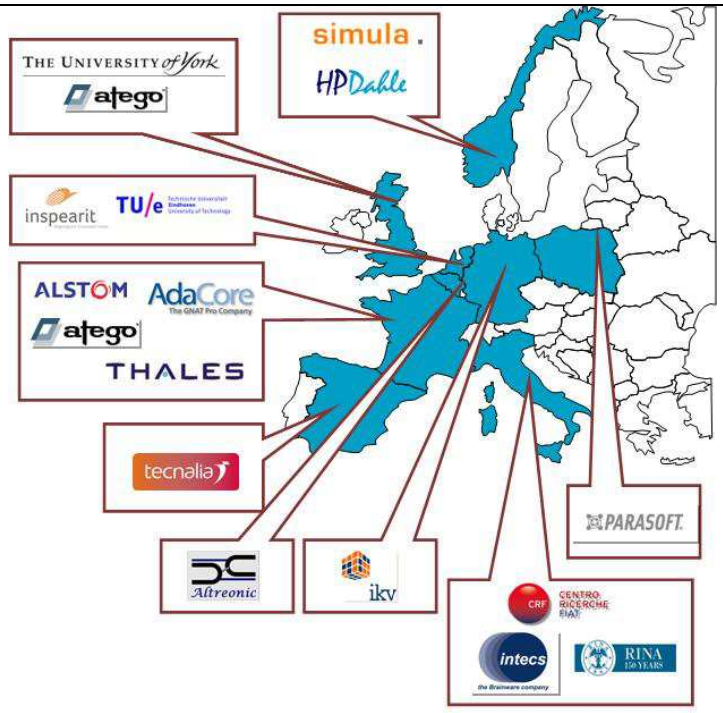
OPENCOSS: the way ahead

Feedback from the Case Studies will continue to be collated and analyzed. Together with the Prototype "technical validation", the Case Studies will also serve a sort of Prototype evaluation or assessment: did/does/will the Prototype bring "measurable" benefits to users, also beyond the Consortium Industrial Partners? Necessary benchmarking will accordingly be defined, with appropriate metrics.

The feedback above, together with running conceptual enhancements (vocabulary and CCL), will be merged and implemented within upgraded Prototypes. A roadmap has already been outlined, moving from current Prototype 1, to next versions 2 and 3. Those will also strengthen the Prototype integration capability with external tools (e.g. Atego Process Director™).

THE CONSORTIUM

A STRONG EUROPEAN TEAM



AdaCore	FR
ALSTOM Transport	FR
Altreonic	BE
ATEGO France	FR
ATEGO UK	UK
Centro Ricerche FIAT	IT
HPDahle	NO
IKV++	DE
INSPEARIT	FR/NL
INTECS	IT
Parasoft	PL
RINA	IT
SIMULA	NO
TECNALIA R&I (Coordinating Partner)	ES
THALES Avionics	FR
TU Eindhoven	NL
University of York	UK

EXTERNAL ADVISORY BOARD (EAB)

The main task of the EAB is to provide strategic guidance and support to the OPENCOSS Consortium in order to ensure that eventually the results will meet the project objectives.

External Advisory Board composition:

- Airbus, France
- AIST, Japan
- BAE Systems, UK
- CAF, Spain
- Deutsche Bahn (DB-Netz), Germany
- EADS/Eurocopter, France
- EADS/IW, UK & Germany
- Eclipse, Europe
- ERA, Europe
- Flanders Drive, Belgium
- NASA, USA
- Renault, France
- RFI – Italian Railway Network, Italy
- Ricardo, UK
- SafeTrans, Germany
- Thalès Railway, Austria
- TÜV Rheinland, Germany
- Verocel, USA
- Volvo, Sweden

More about EAB and its role: http://www.opencoss-project.eu/node/27.

PAPERS AND PUBLICATIONS

PUBLICATIONS

- **Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems**, *Huáscar Espinoza, Alejandra Ruiz, Mehrdad Sabetzadeh, Paolo Panaroni*, IEEE ISRE 2012 WOSOCER, Hiroshima, Japan, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6118522&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6118522
- **A harmonized multi-model framework for safety environments**, *Xabier Larrucea (TEC), Paolo Panaroni (INT)*, EuroSPI 2012, Vienna, http://link.springer.com/content/pdf/10.1007%2F978-3-642-31199-4_11.pdf
- **Towards a Case-Based Reasoning Approach for Safety Assurance Reuse**, *Alejandra Ruiz, Ibrahim Habli, Huáscar Espinoza*, Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR), 31st International Conference on Computer Safety, Reliability and Security (SAFECOMP 2012), September 25th 2012, Magdeburg (Germany), http://link.springer.com/chapter/10.1007/978-3-642-33675-1_3
- **Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards**, *Jose Luis de la Vara, Sunil Nair, Eric Verhulst, Janusz Studzizba, Piotr Pepek, Jerome Lambourg, and Mehrdad Sabetzadeh,* Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR), 31st International Conference on Computer Safety, Reliability and Security (SAFECOMP 2012), September 25th 2012, Magdeburg (Germany) http://link.springer.com/chapter/10.1007%2F978-3-642-33675-1_6
- **A Preliminary Study towards a Quantitative Approach for Compositional Safety Assurance**, *A. Ruiz, H.* Espinoza, *F. Tagliabo, Sandra Torchiaro, Alberto Melzi,* accepted at the 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013, 15-17 October 2013, Radisson Blu, Cardiff (UK), http://tv.theiet.org/technology/manu/16017.cfm
- **A Unified Meta-Model for Trustworthy Systems Engineering**, *Eric Verhulst, Bernhard H. C. Sputh,* Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR), 31st International Conference on Computer Safety, Reliability and Security (SAFECOMP 2012), September 25th 2012, Magdeburg (Germany). http://link.springer.com/chapter/10.1007/978-3-642-33675-1_8
- **Supporting the Verification of Compliance to Safety Standards via Model-Driven Engineering: Approach, Tool-Support and Empirical Validation**, *Rajwinder Kaur Panesar-*

PAPERS AND PUBLICATIONS

Walawege, Mehrdad Sabetzadeh, Lionel Briand, Journal of Information and Software Technology, Volume 55, Issue 05, May 2013 www.sciencedirect.com/science/article/pii/S0950584912002352

- **Nuanced term-matching to assist in compositional safety assurance**, *Katrina Attwood, Philippa Conmy,* 1st International Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2013), www.cs.york.ac.uk/assure2013/Preliminary_Program.html
- **Extracting Models from ISO 26262 for Reusable Safety Assurance**, *Yaping Luo1, Mark van den Brand, Luc Engelen, John Favaro, Martijn Klabbers, and Giovanni Sartori*, accepted to 13th International Conference on Software Reuse, Pisa (Italy), 12-13 June 2013, http://softeng.polito.it/ICSR13/schedule.html
- **Making Software Safety Assessable and Transparent**, *Risto Nevalainen, Alejandra Ruiz, and Timo Varkoi*, accepted at the 20th EuroSPI2 Conference 2013, Dundalk, Ireland, 25-27 June 2013, http://2013.eurospi.net/images/EuroSPI2013/PROGRAM/eurospi2013-program-v1.pdf
- **A Review of Traceability Research at the Requirements Engineering Conference**, *Sunil Nair, Jose Luis de la Vara, Sagar Sen*, accepted at the 21st IEEE International Requirements Engineering Conference, 15-19 July 2013, Rio de Janeiro (Brasil), www.re2013.inf.puc-rio.br/pages/main.php?id=page_welcome
- **On the Use of Goal Models and Business Process Models for Elicitation of System Requirements**, *Jose Luis de la Vara, Juan Sánchez, Oscar Pastor*, accepted at the 14th Working Conference on Business Process Modeling, Development, and Support (BPMDS'13), 17-18 June 2013, Valencia (Spain), www.bpmds.org/program
- **Structuring, and Assessment of Evidence for Safety: a Systematic Literature Review**, *Sunil Nair, Jose Luis de la Vara, Mehrdad Sabetzadeh, Lionel Briand*, presented at the 6th IEEE International Conference on Software Testing, Verification and Validation (ICST 2013), 18-22 March 2013, Luxembourg, www.icst.lu, http://simula.no/publications/Simula.simula.1656
- **SafetyMet: A Metamodel for Safety Standards**, J.L. de la Vara and R.K. Panesar-Walawege, presented at ACM/IEEE 16th International Conference on Model Driven Engineering Languages and Systems (MODELS 2013), September 29 - October 04, 2013, Miami (FLO, USA), www.researchgate.net/publication/257757633_SafetyMet_A_Metamodel_for_Safety_Standards
- **Specifying a Framework for Evaluating Requirements Engineering Technology: Challenges and Lessons Learned**. J.L. de la Vara, D. Falessi, and E. Verhulst, 3rd IEEE International Workshop on Empirical Requirements Engineering (Empire 2013),

PAPERS AND PUBLICATIONS

July 15, 2013, Rio de Janeiro (Brazil) http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6615209&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A6615205%29

- **Dealing with Software Model Quality in Practice: Experience in a Research Project**, J.L. de la Vara and H. Espinoza, 1st International Workshop on Quality and Measurement of Software Model- Driven Developments (QUAMES 2013), July 29-30 2013, Nanjing (China), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6605958
- **Conceptualisation of Industrial Safety Assurance Activities: Towards Computer-Aided Certification**, Katrina Attwood, Fabien Belmonte, Laurent de la Beaujardière and Andrea Palermo, presented at International Workshop on Model-Based Safety Assurance 2013, Paris, March 2013, http://www-users.cs.york.ac.uk/~katrina/publications.html
- **The role of the safety-case lexicon in cross-domain translation: the OPENCOSS project**, Katrina Attwood, presented at the Independent Safety Assurance Group/Safety-Critical Systems Club Workshop 'Transferable Safety - fact or fiction?', London, 5th December 2013, http://scsc.org.uk/file/262/protect_reg_Attwood.pdf
- **Cross-domain systems and safety engineering: is it feasible?**, *Eric Verhulst*, presented at the Flanders Drive seminar: Functional Safety in the Vehicle Industry, Brussels /Belgium), 17 January 2013, http://www.flandersdrive.be/en/about-us/events/functional-safety-vehicle-industry-0 and also at the Flanders' Mechatronics Engineering Centre, Oostende (Belgium), 06 February 2013 http://fmec.khbo.be/events/2013/including-functional-safety-design-mechatronics-and-ict
- **A Preliminary Study towards a Quantitative Approach for Compositional Safety Assurance,** *A. Ruiz, H. Espinoza, F. Tagliabo, Sandra Torchiaro, Alberto Melzi*, presented at the 21st Safety-critical Systems Symposium, 05-07 February 2013, Bristol (UK), www.safety-club.org.uk/e210 and http://scpro.streamuk.com/uk/player/Default.aspx?wid=16017&ptid=1060&t=0
- **A Criterion for Composable Safety and Systems Engineering,** *Eric Verhulst, Bernhard Sputh (Altreonic), Jose Luis de la Vara (Simula), Vincenzo de Florio (Uni Antwerp)*, to be presented at the 2013 Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR), part of the 32nd International Conference on Computer Safety, Reliability and Security (Safecomp), which will be held in Toulouse (France), on 24-27 September 2013, http://conf.laas.fr/SAFECOMP2013/?q=node/26

PAPERS AND PUBLICATIONS	• **From Safety Integrity Level to Assured Reliability and Resilience Level for composable safety critical systems**, *Eric Verhulst, Bernhard Sputh, Jose Luis de la Vara, Vincenzo de Florio*, ICSSEA, Paris, November 2013, www.pats.ua.ac.be/publications/content/publications/2013/ICSSEA_2013_ARRL_final_08102013.pdf • **ARRL, A criterion for compositional safety and systems engineering. A normative approach to specifying components**, *Eric Verhulst, Bernhard Sputh*, Industry session, IEEE ISRRE2013, Pasedena (CA, USA), November 2013, http://2013.issre.net/industry_papers#paper5_3 • **Towards a multi-view point safety contract**, *Alejandra Ruiz, Tim Kelly, Huascar Espinoza*, Proceedings of Workshop SASSUR (Next Generation of System Assurance Approaches for Safety-Critical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, Toulouse (France), 24-27 September 2013, http://hal.inria.fr/docs/00/84/84/96/PDF/5_-_20130042.pdf • **Adequacy of contract grammars for component certification**, *Alejandra Ruiz, Huascar Espinoza, Tim Kelly*, Fast Abstract at the 32nd International Conference on Computer Safety, Reliability and Security, Toulouse (France), 24-27 September 2013, http://conf.laas.fr/SAFECOMP2013/?q=node/10 • **Safety Evidence Traceability: Problem Analysis and Model**, *Sunil Nair, Jose Luis de la Vara, Alberto Melzi, Giorgio Tagliaferri, Laurent de-la-Beaujardiere, and Fabien Belmonte*, 20th International Working Conference on Requirements Engineering: Foundation for Software Quality, Essen (Germany), April 07-10 2014, www.opencoss-project.eu/sites/default/files/REFSQ2014_NairEtAL_CRC.pdf 

ATTENDED EVENTS

OPENCOSS AT THE 4TH EMBEDDED REALTIME SOFTWARE AND SYSTEMS (ERTS²) CONFERENCE IN TOULOUSE (F), 05-07 FEB, 2014

AdaCore, Atego, Intecs, and Parasoft have represented OPENCOSS at the ERTS² Congress (www.erts2014.org), a unique European cross-sector event on Embedded Software & Systems, a platform for top-level scientific information exchange with representatives from universities, research centers and industries. This 2014 edition has gathered more than 100 talks, 500 participants and 80 exhibitors.

NEXT EVENTS	
AESSCS 2014 WORKSHOP **PLANNING THE UNPLANNED EXPERIMENT: ASSESSING THE EFFICACY OF STANDARDS FOR SAFETY CRITICAL SOFTWARE** **AT EDCC CONFERENCE, 13 MAY 2014 IN NEWCASTLE UPON TYNE (UK)**	The main motivation behind this event is that software is frequently judged to be fit for use in safety-critical systems based on conformance to a standard such as RTCA DO-178C, IEC 61508, or ISO 26262., while there is little evidence to either support or rebut claims that conformance actually ensures or confirms fitness for such use. To be sure, software in some domains (e.g. aviation) has an excellent track record, but correlation is not causation.  University of York will participate in this event, and represent OPENCOSS. A paper has already been submitted. More info at www.idt.mdh.se/AESSCS_2014.
19TH INTERNATIONAL CONFERENCE ON RELIABLE SOFTWARE TECHNOLOGIES ADA-EUROPE 2014 **23-27 JUNE 2014, PARIS (FRANCE)**	This conference (www.ada-europe2014.org) will provide an international forum for researchers, developers and users of reliable software technologies all over the world. Presentations and discussions will cover applied and theoretical work currently being conducted to support, the development and maintenance of reliable software systems. Intecs is in the industrial programme committee, and AdaCore will participate to the event.

33RD INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY AND SECURITY (SAFECOMP 2014), FLORENCE (ITALY), 10-12 SEP 2014	An International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR, www.safecomp2014.unifi.it/sassur), organized by Tecnalia, will be co-located within the SafeComp international conference, of which Intecs is in its programme committee. This SASSUR event will also represent the official annual workshop of OPENCOSS. 

DISSEMINATION MATERIAL	
	The following material can be downloaded from the OPENCOSS Web site (www.opencoss-project.eu): • Flyer (also called brochure, fact-sheet, leaflet) • Abstract • Position Paper (also called white paper) • Press Release (issues at project kick-off) • Roll-Up Poster • Short Presentation • Long Presentation • This Newsletter (Nov 2013 to May 2014), and previous ones *In the photo, Alejandra Ruiz, from Tecnalia, while stepping out.*

OPENCOSS ON THE SOCIAL NETWORKS

The project web site is available at www.opencoss-project.eu

The Cordis project page is available at http://cordis.europa.eu/projects/rcn/100775_en.html.

The project is also visible as a LinkedIn professional group (> 180 participants) and on Twitter and Facebook. Join us!

THE TECH CORNER

IN THIS ISSUE: STANDARDS MAPPING AND MIGRATION

Standards Mapping and Migration

There is common agreement that the different safety standards, from respective domains (Automotive, Railway, Avionic, Space), look similar and contain "substantially" equivalent requirements, though stated with different jargons. However, there are always some subtle differences and those have to be faced. This short note focuses on how to practically handle those differences.

Moving ("migrating") a Standard A-compliant system to comply also with Standard-B is a challenging exercise. Let's call this as "standards migration". No exact mapping exists yet between the various standards. Few published works remain only at very high level of comparison. More accurate mappings are required. This is exact in the direction of the OPENCOSS CCL (Common Certification Language), meant as a "lingua franca" for safety requirements.

However, once a mapping is available between any two standards, it is then realized that the two actually differ, and the missing (not mapped) requirements ("delta requirements") have to be covered in the migration. For an available product, this migration typically requires some reverse-engineering activities. The objectives of a migration are therefore:

- Minimize effort to comply with "delta requirements"
- Use proven, agreed and effective approaches to achieve it

The delta requirements may belong to two separated groups: process and product. In the following find a sample of them, together with a survey of possible, solving techniques.

Process requirements:

- Standard B requires that activity X be performed with a certain level of independence, while standard A ignores this. It is impractical and costly to re-execute the activity entirely, and therefore it is recommended to have at least an independent, systematic review of the activity outcome.
- Standard B requires tool X be qualified with a given approach, while standard A ignores this. It would be

STANDARDS MAPPING AND MIGRATION

impractical to change tool (e.g. a compiler) and re-execute corresponding activity, or qualify the tool. Rather think of a thorough verification of the tool output.

- Standard B requires role X to possess a given skill, or seniority, while standard A ignores this. It is recommended to have a systematic review, by an independent skilled and/or senior person, over the artifacts prepared by role X.
- Standard B requires given activity X be performed before Y, while Standard A ignores this, and actually in the project X was performed after Y. Analyze Y dependencies with respect of X, and reconsider potential changes.
- Standard B requires a given test approach, while standard A ignores this. Keep and trust current tests (with related results), and add new tests to achieve compliance with the new approach.

Product requirements:

- Standard B requires the use of a given language subset, while standard A ignores this. Changing the source code may be risk-full and costly at this stage. Remove only true code hazards, and keep not compliant code, provided it is subject to deep inspection or test.
- Standard B requires some code metrics thresholds, while standard A ignores this. Changing the source code may be risk-full and costly at this stage. Keep un-compliant code, provided it is subject to deep inspection or test.
- Standard B requires a given approach to traceability, while standard A ignores this. Improve missing traceability, e.g. define low-level requirements if not available and trace them to tests.

Conclusions

Mapping two standards is a preliminary activity and serves to identify the differences between the two (additions and holes). The challenge is then how to cope with said differences, and to "migrate", in the most efficient and effective way, a given completed project, as compliant with a given standard, to comply also with the other.