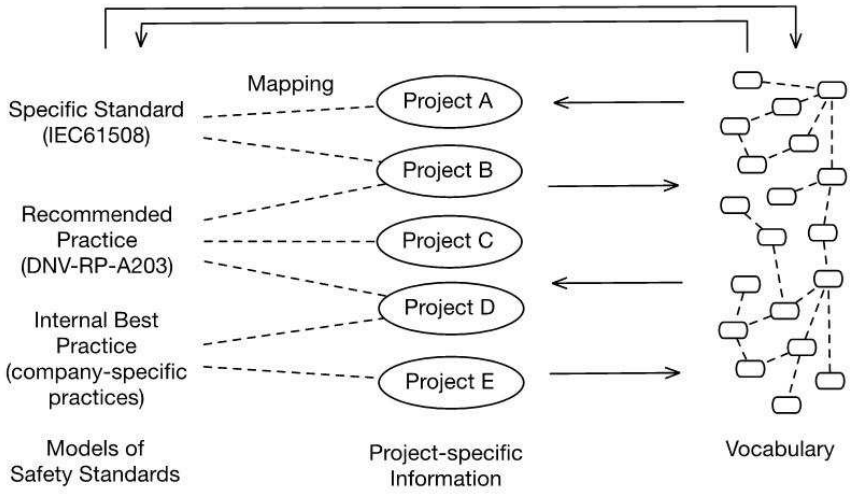
NEWSLETTER – N. 4 – December 2013

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). The objective is to produce the first Europe-wide, open safety certification platform. This platform is meant to reduce time & cost for (re)certification of safety-critical embedded systems, namely for Railway, Avionic and Automotive domains.
EDITORIAL **From Concept to Tool** **OPENCOSS@ WORK**	The project is now two years from start. Since last Newsletter, the project made significant advancements on the **Common Certification Language** (**CCL**) and associated **Prototype Tool**. The **CCL** is quite innovative, and represents the key design strength of the project. **Standardized models** have been defined, addressing safety argumentation, evidence characterization, and compliance management. These models can be characterized for each standard (e.g. DO-178C) or domain (e.g. Automotive). A **vocabulary** has then been prepared, allowing harmonization and comparison of the assurance terminology across domains. Models and vocabulary together represent the CCL.

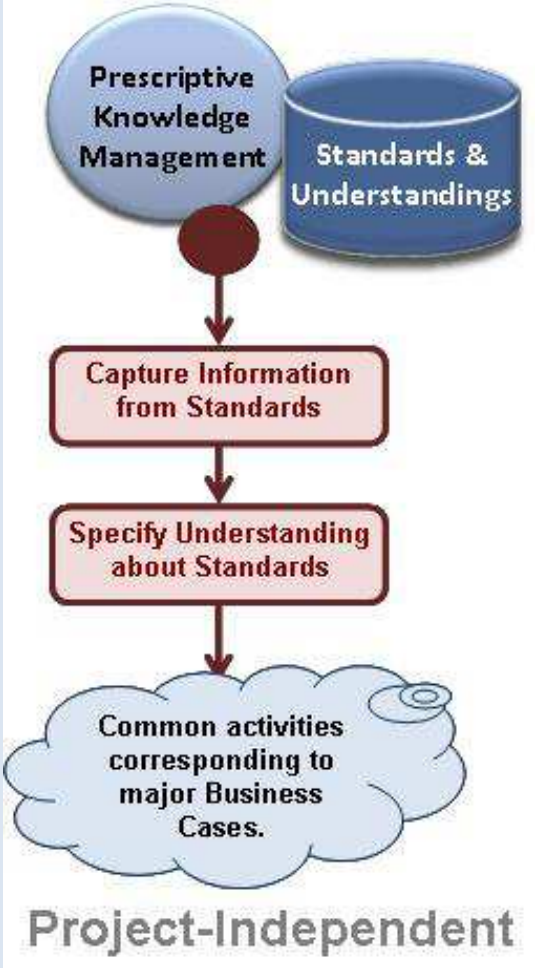


Safety Compliance Models

The CCL

From Concept to Tool

OPENCOSS@WORK



Once finalized the concepts (CCL), the semester has seen the delivery of the first **Prototype Tool**: the concepts at work! Based on the underlying conceptual schema (CCL), the tool is meant to support the work of **safety stakeholders**, the target users of the tool. They are people concerned with the (re) certification process of any software-intensive electronic equipment in any domain (Avionic, Railways and Automotive). These users span several roles (Developer, Safety Manager, Verifier, Validator, QA, Tester, etc.) in several entities (Supplier, Customer, Certification Agency, IV&V, etc.).

The tool allows first the creation of **Reference Frameworks**, i.e. tool-specific representations of Standards and Regulations. It's the project-independent **knowledge base**. In fact, once created, this remains mostly read-only, although they can be enriched from time to time with clarifications, addenda, explanatory notes, FAQ's, either external and coming from standardization bodies or originated internally in users' organizations.

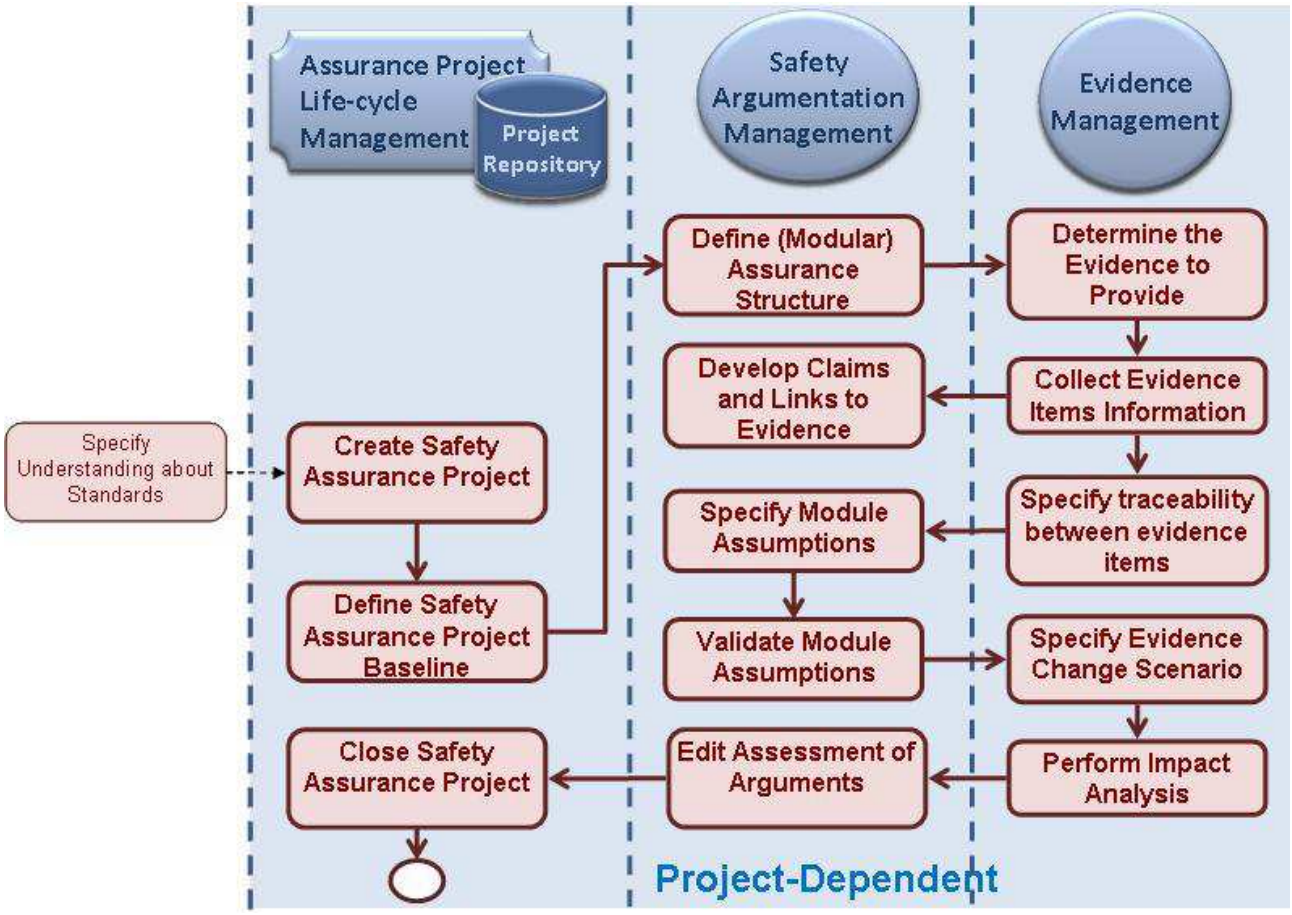
From Concept to Tool

OPENCOSS@ WORK

It then comes the **Project-dependent** part: applying the knowledge in **projects**. In general projects instantiate the knowledge according to unique circumstances. The tool thus lets users create **Assurance Projects** by associating these to a given **Safety Assurance Project Baseline**. This is a **subset** of the **Reference Framework** to be applied in the project. This association may be recurrent or unique, depending on the user organization. For instance, an organizations might consolidate an own Project Baseline for all the required re-engineering activities upon corrective maintenance of level B projects under DO-178C framework.

All along projects duration the tool then allows the modeling of **Evidences** (Artifacts), **Processes** (Activities), **Compliance Maps** (i.e. from Reference Artifacts to actual Artifacts), and **Argumentations**.

A number of representative **use cases** have then been utilized to "validate" the prototype, and next incoming months will see an effective closed-loop between validation and engineering.

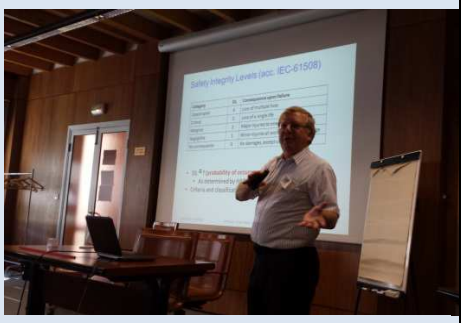


THE CONSORTIUM

A STRONG EUROPEAN TEAM

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

EXTERNAL ADVISORY BOARD (EAB)



EAB MEETING AT SAFECOMP 2013

External Advisory Board current composition:

- AIRBUS (France)
- AIST (Japan)
- BAE SYSTEMS (United Kingdom)
- CAF (Spain)
- Deutsche Bahn (Germany)
- EADS/Eurocopter
- EADS/IW (France)
- Eclipse Foundation
- ERA – European Railway Agency
- Flanders Drive (Belgium)
- Italian Rail Network – RFI (Italy)
- Mr. Michael Holloway (NASA, US)
- Renault (France)
- Ricardo (United Kingdom)
- SafeTrans (Germany)
- Thales Railway (Austria)
- TÜV Rheinland (Germany)
- Verocel (US)
- Volvo (Sweden)

An EAB meeting toke place at SafeComp 2013 conference, in Toulouse (24 Sept 2013). Partners of OPENCOSS answered to some questions of EAB, and a discussion followed. It then resulted a few EAB suggestions, such as:

- Enforcement of usage of standards, and adherence to related efforts, such as OSLC (http://open-services.net)
- Clarification of opensource compatibility and openness of associated results.

These have been taken in consideration by the Consortium, with near-medium term commitments.

DELIVERABLES	**PUBLIC DELIVERABLES** (available for download at http://www.opencoss-project.eu/node/7)
	D1.1 – Constraints of the certification process (report)
	D1.2 – Use cases description and business impact (report)
	D1.3 – Evaluation Framework and Quality metrics (report)
	D2.1 – Business cases and user needs (report)
	D2.2 – High-level requirements (report)
	D2.3 – OPENCOSS platform architecture (report)
	D3.2 – Integration requirements and test plan (report)
	D4.1 – Baseline for the common certification language (report)
	D4.2 – Detailed requirements for the common certification language (report)
	D4.4 – Common Certification Language: Implementation (report)
	D5.1 – Baseline for the compositional certification approach
	D5.2 – Detailed requirements for the OPENCOSS compositional certification approach
	D6.1 – Baseline for the evidence management needs of the OPENCOSS platform (report)
	D6.2 – Detailed requirements for evidence management of the OPENCOSS platform (report)
	D6.4 – Specification of adapters to development and safety assurance tools (report)
	D7.1 – Baseline for the process-specific needs of the OPENCOSS platform (report)
	D7.2 – Detailed requirements for the process-specific needs of the OPENCOSS platform (report)
	D9.1 – Collaboration Platform
	D9.2A – Dissemination Plan
	D9.2B – Training Plan
	D9.4 – First Report of Dissemination, training and exploitation activities (report)

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

PAPERS AND PUBLICATIONS

- **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,* Journal of Information and Software Technology, Volume 55, Issue 05, May 2013 http://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), http://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

PAPERS AND PUBLICATIONS

- **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), 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

PAPERS AND PUBLICATIONS

- **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, http://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 

SOON TO COME RELEVANT EVENTS FOR OPENCOSS	
4TH EMBEDDED REALTIME SOFTWARE AND SYSTEMS ERTS² CONFERENCE IN TOULOUSE (F), 05-07 FEB 2014	 Intecs will represent OPENCOSS at this ERTS² Congress (www.erts2014.org). It is a unique European cross-sector event on Embedded Software & Systems, a platform for top-level scientific with representatives from universities, research centers and industries. Previous editions gathered more than 100 talks, 500 participants and 60 exhibitors.
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 of this event is that software is frequently judged fit for use in safety-critical systems because it conforms to a standard such as RTCA DO-178C, IEC 61508, or ISO 26262. But there is little evidence to either support or rebut claims that conformance ensures or confirms fitness for such use. While software in some domains (e.g. aviation) has an excellent track record, correlation is not causation.  University of York will participate at this event, and representing 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 conducted to support, the development and maintenance of reliable software systems. Intecs will represent the OPENCOSS Consortium at this event.
DISSEMINATION MATERIAL	
	The following material can be downloaded from the OPENCOSS Web site: • 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 • This Newsletter (May 2013 to December 2013), 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), Twitter and Facebook. Join us!

THE TECH CORNER

IN THIS ISSUE: PRESCRIPTIVE VS. GOAL ORIENTED STANDARDS

Prescriptive vs. Goal oriented Standards

In the last issue (May 2013) we hosted a confrontation between product- and process-oriented standards. In this issue a slight variant on the same track: prescriptive vs. goal-oriented standards.

The issue

It is often debated the "prescriptive" approach of some standards vs. the goal-oriented approach for others. It is often argued that goal-oriented are superior as they do allow for more effective and efficient implementation, more easily adapting to emerging technologies. Opponents, however, argue that goal-oriented standards are too vague and subject to interpretation, highlighting its ability to firmly assess the goal achievement.

Prescriptive

Prescriptive means that you are required to perform very precise steps. Little room is left to "interpretation" or to decisions. The standards take the full responsibility to decide what is necessary to perform, and you have just to execute it (more or less) blindly. Two organizations following a prescriptive standard will perform extremely similar tasks and produce similar artifacts. This ensures repeatability of the process and makes it easier to assess compliance.

Actually no standard is truly fully prescriptive. Being "fully" prescriptive means that the entire process could be made fully automatic. Actually, you are always left some room for interpretation. For instance, if a standard were imposing a meeting each week, it would not impose the particular day. If grotesquely it were imposing the Friday, you would still have residual freedom between morning and afternoon.

Goal-Oriented

On the other extreme, goal-oriented standards acknowledge that what is important is just to set objectives (goals) and it is up to the organization, with its own culture and capability, to determine the best steps, in a project, in order to achieve these goals. Although not domain-specific, CMMI® for

PRESCRIPTIVE VS. GOAL ORIENTED STANDARDS

Development (www.sei.cmu.edu/reports/10tr033.pdf) is the leading goal-oriented process improvement standard.

These goal-oriented standards are claimed to be higher level, and they leverage on the competitive ability of organizations to implement their own best steps in order to achieve the goals in a cost/effective way.

No standard is really fully goal-oriented as many of them roll-out into hundreds of low level goals (sub-goals or practices), often prescribing their schedule and associated type of resources (e.g. independence). The same CMMI® states goals and sub-goals, but then it specifies a number of practices that are not mandated, but highly recommended and followed. Actually, when a goal-oriented approach actually identifies a large number of micro-goals, the initial nature of goal-oriented is lost into a prescription to achieve these micro-goals. Your freedom is limited to the implementation of these micro-goals, and you are "prescribed" to achieve them.

Short Discussion

No standard is fully prescriptive and no standard is fully goal-oriented. It is just a matter of degree, intensity. Which is the right balance? Let's try to tackle this with negation reasoning.

When not to prescribe

There is no doubt the prescribing un-influential details (e.g. the day of the week to hold a meeting) is useless, and places un-necessary constraints.

The exact layouts of documents shall also not be prescribed and standards shall discuss only about contents and information, no matter how this is hosted and organized in one document, two documents or into a CAD Model. Whenever there is an objective way to assess goals of one activity (e.g. have you reached 100% MC/DC coverage?), it does not interest the way you achieve that goal. When the state of the art considers different techniques and approaches, having similar value, it is good to leave the organization to choose. For instance, this approach is adopted by EN 5012x standards (CENELEC) that allow for "valid combinations" of techniques.

PRESCRIPTIVE VS. GOAL ORIENTED STANDARDS

When to prescribe

Often there is room of interpretation on the goals to achieve. In these cases it is good to prescribe the steps to be performed. Sometimes it is extremely difficult to assess goals, such as target levels of code defect density. In such cases, it is better to prescribe different steps and associated techniques (e.g. unit test, integration test, validation tests). Moreover, some goals may hide a few risks, and the way these goals are achieved (i.e., methods, tools, staff profile) may influence positively our assurance on their achievement. In this case, prescriptions on qualified tools or personnel, independence on personnel, etc. are appropriate.

Conclusions

There is the need of a wise balance between prescriptive and goal-oriented standards, and it seems that the most practical and cost/effective approach is to prescribe only what is strictly necessary, i.e. when the goal cannot be objectively, consistently and repeatedly assessed.