Collaborative Large-scale Integrating Project

Open Platform for EvolutioNary Certification Of Safety-critical Systems

Report of OPENCOSS standardization activities and follow-up roadmap
D8.4

Work Package:	WP8: Standardisation and Community Building
Dissemination level:	PU
Status:	Ready
Date:	31 March 2015
Responsible partner:	University of York
Contact information:	oleg.lisagor@york.ac.uk

Contributors

Names	Organisation
Oleg Lisagor (ed)	UoY
Katrina Attwood	UoY
Andrea Critelli	RINA
Huascar Espinoza Ortiz	Tecnalia
Ludovic Gauthier	PTC (formerly, ATEGO)
Tim Kelly	UoY
Jerome Lambourg	AdaCore
Xabier Larrucea	Tecnalia
Alberto Melzi	CRF
Jan Mauersberger	IKV
Laurent Pitot De La Beaujardiere	Alstom
Paolo Panaroni	Intecs
Alejandra Ruiz	Tecnalia
Janusz Studzizba	Parasoft
Eric Verhulst	Altreonic

Document History

Version	Date	Remarks
V0.1	2015-03-24	First Draft

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

The present report is produced by task T8.4 (“Standardisation”) of OPENCOSS project. The report consists of two main parts.

Firstly, Section 2 presents the summary of standardisation activities carried out within the project and a plan for outstanding standardisation activities that will be carried out after project completion. The project standardisation activities have focussed on standardising project outcomes, primarily, through System Assurance Task force of the Object Management Group (OMG) and Goal Structuring Notation (GSN) community standard. OPENCOSS is contributing to the revision of OMG’s Structured Assurance Case Metamodel (SACM), the revision of the GSN community standard and OMG efforts to define standardised framework for describing assurance standards based on Common Certification Language (CCL) developed in OPENCOSS. For a range of pragmatic reasons (including dormancy of the relevant groups, maturity of OPENCOSS framework before project completion and standard-agnostic nature of the framework) formal engagement with groups responsible for industrial safety standards has been deprioritised.

Secondly, Section 3 presents a roadmap for the project follow up in areas other than standardisation. This part of the report extends deliverable D9.6 (Final Report of Dissemination, Training, and Exploitation Activities) and presents individual partners follow-up plans in four key areas:

- Research
- Tool development
- Industrial adoption and influencing industrial practices
- Education and professional training

Where possible, a common narrative for activities is presented; however, most of the follow-up plans are presented partner-by-partner in relevant sections.

Abbreviations

Abbreviation	Explanation
ARM	Argumentation Metamodel: a standard developed by Object Management Group; now superseded by SACM (see below)
ARP	Aerospace Recommended Practice: the guidelines for the design and production of aircraft, parts and components published by SAE International.
AUTOSAR	AUTomotive Open System Architecture: a worldwide development partnership of vehicle manufacturers, suppliers and other companies from the electronics, semiconductor and software industry
CCL	Common Certification Language: one of the key concepts developed by OPENCOSS project
CENELEC	European Committee for Electrotechnical Standardization: an European Commission designated standardisation body
CPD	Continuous Professional Development
CPS	Cyber-Physical System(s)
DIA	Development Interface Agreement: a concept introduced in ISO26262 standard
DoW	Description of Work: The main and agreed document describing the project activities.
DSL	Domain-Specific Language
EAB	External Advisory Board of OPENCOSS project
GSN	Goal Structuring Noration: a graphical argumentation notation used to capture the structure of an assurance case
IEC	International Electrotechnical Commission: organization for the preparation and publication of International Standards for all electrical, electronic and related technologies
IMA	Integrated Modular Avionics
ISO	International Organization for Standardization: an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards.
MSc	Master of Science
NLP	Natural Language Procession
OMG	Object Management Group: an international, open membership, not-for-profit technology standards consortium
OSLC	Open Services for Lifecycle Collaboration: an open community concerned with development of specifications for integrating software
Polarsys	An Eclipse Industry Working Group concerned with the creation and support of Open Source tools for the development of embedded systems
R&D	Research & Development
SACM	Structured Assurance Case Metamodel: one of the standards developed and maintained by Object Management Group (above)
SAEM	Software Assurance Evidence Metamodel: a standard developed by Object Management Group; now superseded by SACM (see below)
WP	Work Package

1 Introduction and Overview

Being an integrated project the overarching objective of OPENCOSS is to influence European and wider industrial practices whilst maturing state of research and state of the art technologies and influencing future European research agenda. Pragmatically, this impact cannot be achieved within the time bounds of the project itself. In particular industrial practice in any sector is by necessity conservative and any significant change has to overcome significant 'momentum'. Furthermore, the topic of OPENCOSS and industrial sectors directly addressed by the project (automotive, aviation and railway transportation) are particularly averse to radical change due to regulation and potential (perceived) impact of the safety of the general public.

Recognising this challenge OPENCOSS consortium has developed a roadmap of follow-up activities to ensure that project impact is fostered after completion of research and development activities and to facilitate adoption of the project outcomes. Individual partners have been required to prepare a plan of follow-up activities in five core areas:

1. Further research: the aim of those activities is to investigate more advanced and novel concepts developed by OPENCOSS
2. Tooling: to ensure that maturity and usability of OPENCOSS platform and tool sets continues to improve, to adopt concepts investigated by OPENCOSS in a wider range of industrially mature tools and to enable tool developers that are not part of the consortium to benefit from the project outcomes
3. Training and Education: To support dissemination of OPENCOSS outcomes among current and future safety critical systems engineers and managers therefore facilitating adoption of the key concepts and the overall OPENCOSS framework as part of future industrial practice.
4. Standardisation: comprising standardisation of the OPENCOSS outcomes and framework themselves as well as engagement with industrial safety standards of various sectors; these activities should both ease adoption of OPENCOSS concepts in the context of existing regulatory frameworks and facilitate wider adoption by standardising the outcomes in clear and recognised ways.
5. Industrial practice: these activities are concerned with facilitating direct adoption of the both individual concepts and the framework developed by the project.

It should be noted that whilst activities in the first four categories can be often seen as exploitation of project outcomes in their own right (e.g. training and education is a service provided by a number of project partners) they also provide essential support to facilitating adoption of the project outcomes in industrial safety engineering, management and certification practices and processes (i.e. the fifth category above).

Also, standardisation activities are different from other groups in that those were started during the project and significant progress has already been made.

This report presents a roadmap of the follow up activities for OPENCOSS project. It is based largely on partners individual follow-up plans; however, where appropriate, coordinated actions are highlighted in the text and common / key narrative is presented.

Section 2 of the report focusses on Standardisation activities presenting both the work undertaken during the project and standardisation roadmap. Section 3 focusses on other types of follow up activities as listed above.

Overall the report serves a dual purpose:

- It is a final report for the task T8.4 (Standardisation)
- It extends deliverable D9.6 (Final Report of Dissemination, Training, and Exploitation Activities) by presenting concrete follow-up actions to be taken after completion of the project.

2 OPENCOSS Standardisation Activities

With focus on certification of systems, standardization has been a key support activity of OPENCOSS project. These activities have been carried out in WP8 of the project and, specifically, in Task 8.4.
Initial project plan has focused on work with standardization bodies that publish safety engineering and management standards. These standards include:

- For automotive domain – ISO26262
- For aviation domain – ARP4754a, ARP4761a and DO-178c
- For railway domain – EN50126, EN50128 and EN50129

Similar standards in industrial sectors not directly represented within OPENCOSS consortium include IEC61508 (international domain-independent standard) and DS 00-56 (UK military).

However, many of the groups and working parties related to the above standards are currently dormant having recently completed standards update processes. Furthermore, in the judgment of consortium partners the outcomes of OPENCOSS had insufficient maturity prior to project completion to be usefully formally presented to those standardization groups.

Most importantly, however, the objective of OPENCOSS was to develop a standard-agnostic framework that could be used for modelling any safety engineering standards as well as arguments, processes and work products that are used by companies to demonstrate compliance with standards and satisfaction of their requirements. This means that OPENCOSS framework should require little (if any) modification of the standards.

As a result of these observations, the consortium has decided to focus standardization activities of T8.4 primarily on standardization of the project outcomes – the Common Certification Language (CCL) and its sections developed in WP5, WP6 and WP7 of OPENCOSS. This is being undertaken under the auspices of the Object Management Group (OMG) and GSN Industrial groups as described in Section 2.1 below.

Although engagement with the Working Parties overseeing industrial safety standards have been somewhat de-prioritised by the task T8.4 of OPENCOSS, it has been undertaken by a number of consortium partners as in a form of informal dissemination as well as through the External Advisory Board (EAB) of the project. OPENCOSS framework has a potential for providing useful input into future revisions of these standards. This topic is briefly returned to in Section 2.2 below.

2.1 Standardisation of OPENCOSS outcomes

Standardisation activities, carried out in task T8.4 of OPENCOSS, have focused on standardizing the OPENCOSS framework and influencing the relevant existing and emerging standards. From the perspective of the project outcomes key aspects of the framework that have been addressed by standardization activities are:

- The notion of modular arguments (safety cases / assurance cases) and concepts of safety case interfaces and contracts (WP5).
- Use of structured natural language expressions in structured argument claims (WP4)

- Artefact & Evidence Metamodel (WP6)
- The overarching framework for modelling assurance (including safety) standards encapsulated in CCL (WP4, WP6 and WP7)

These aspects of the OPENCOSS framework have been standardized through influencing two existing standards:

- Goal Structuring Notation (GSN) standard maintained as a community standard by the group of industrial users of GSN. OPENCOSS project partners are contributing to the issue 2 of the standard
- Structured Assurance Case Metamodel maintained by the Object Management Group (OMG) and its Systems Assurance Task Force. OPENCOSS frameworks are providing input into SACM v2.0

Additionally, CCL is forming a basis for a new OMG standard concerned with modelling assurance standards.

OPENCOSS contributions to the above three standardisation efforts is described in the three subsections below.

2.1.1 Influence of the OPENCOSS project on the GSN (Goal Structuring Notation) Standard

The development, review and acceptance of an explicit 'safety case' forms a key component of the assurance and regulation of many safety critical systems, including those in the nuclear, defence, railway, automotive, medical device, and process industries. The incorporation of an explicit safety case has formed part of the OPENCOSS approach (Common Certification Language - CCL) and tooling.

The Goal Structuring Notation (GSN) is a graphical argumentation notation. It explicitly represents the individual elements of any safety argument (requirements, claims, evidence and context) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument). In OPENCOSS we have supported GSN through the incorporation of the Argumentation metamodel portion of the CCL and the provision of Eclipse-based tool support for creating GSN-structured safety case arguments that can reference other assurance artefacts stored and managed within the OPENCOSS platform.

In 2001 an industry group - supported by the University of York - published Issue 1 of the GSN standard[1] to support the now widespread industrial use of the approach. This industry group was formed of representatives from companies including: AACE Ltd, Altran Praxis Ltd, ERA Technology Ltd, Lloyds Register Rail Ltd, RPS Group Ltd, Selex-Galileo Ltd, UK Ministry of Defence, Adelard LLP, BAE Systems Ltd, CSE International Ltd General Dynamics UK Ltd, Thales Ltd. As well as describing 'core' GSN the standard also describes extensions to the notation to support *modular* safety cases (so-called 'Modular GSN'). In OPENCOSS (specifically WP5) we have used this definition of Modular GSN to support our component-based modular certification approach, e.g. incorporating the notion of safety case interfaces, and contracts.

[1] See http://www.goalstructuringnotation.info

The use and development of Modular GSN within WP5 of OPENCOSS has led us to propose some modifications to the definition of Modular GSN defined within the GSN Standard. Specifically, these have addressed the definition of safety case interfaces and contracts. Currently the GSN Community Standard is in a revision cycle (working towards Issue 2) with the aim of having a new issue of standard before December 2015. Partners from the OPENCOSS project (in particular Tecnalia and York) have already contributed to revision meetings. The outputs of OPENCOSS WP5 will be used to propose modifications to Issue 2 of the standard.

2.1.2 Influence of the OPENCOSS project on the OMG Structured Assurance Case Metamodel

The Systems Assurance Task Force within the OMG (Object Management Group) has been working for a number of years on the development of standards to support the assurance community. Of relevance to OPENCOSS is the group's work on standardising metamodels for assurance evidence and assurance case argumentation. Initially, the group's work on these two topics led to the development of two separate standards (published in 2010): The Software Assurance Evidence Metamodel (SAEM)[2] and the ARgumentaion metamodel (ARM)[3]. Following the publication of these two standards, there was an initiative to combine and unify these two standards. This led to the development of Issue 1 of the Structured Assurance Case Metamodel (SACM)[4] in 2013.

The argumentation aspects of SACM were used as a strong influence in the development of the Argumentation aspects of the OPENCOSS metamodel. The evidence aspects of SACM were reviewed when defining the Artefact aspects of the OPENCOSS metamodel but were felt to be too cumbersome for our purpose. In addition, whilst the argumentation model within SACM was known to be based on substantial experience from the development and application of GSN and the Claims-Argument-Evidence Model (from Adelard) there was less evidence to demonstrate the maturity of the evidence model.

SACM has recently been updated to version 1.1 to address minor technical issues. However, a revision task force is currently underway with the aim of producing a substantial revision of the standard for 2016 (SACM 2.0). A number of the objectives for this revision directly relate to areas where OPENCOSS has made significant progress, specifically:

- Support for extending the SACM Argumentation Metamodel to support modular assurance case arguments (relating to the work of OPENCOSS WP5)
- Support for structured natural language expressions being used within the SACM Argumentation Metamodel (relating to the work of OPENCOSS WP4)
- Rationalisation and simplification of the evidence metamodel within SACM (relating to the work of OPENCOSS WP6)

[2] http://www.omg.org/spec/SAEM
[3] http://www.omg.org/spec/ARM
[4] http://www.omg.org/spec/SACM

OPENCOSS partners (specifically Simula, Tecnalia, and York) have officially joined the SACM 2.0 revision task force in order that the outputs of WP4, WP5 and WP6 can be used to influence the revision of the standard. There is already evidence of our success in doing so. The metamodel proposed by WP4 to manage structured vocabulary and expression is forming the current basis of the SACM 2.0 draft for this aspect. The findings from WP5 (as discussed in the section relating to the GSN standard) are being used to inform the modifications of the SACM metamodel relating to modular assurance case interfaces and contracts. Most radically, the CCL artefact model is currently being proposed by the task forces as a complete replacement for the current (SAEM-based) evidence metamodel within SACM 2.0. This has been proposed because it is being seen as a simpler (yet, suitably capable), more rational, and more comprehensible evidence / artefact model. It is hoped that a draft of SACM 2.0 will be available for submission as a RFC (Request for Comment) within the OMG standardisation process by the end of 2015.

2.1.3 Standardisation of the OPENCOSS CCL by the Object Management Group

In addition to influencing the SACM 2.0 revision, there are also plans to standardise the OPENCOSS CCL as an OMG standard. The CCL was presented to the System Assurance Working Group at the December 2014 OMG Technical Meeting in Long Beach, California. It was recognised by the group that the CCL addresses a gap in their current portfolio of standards. They currently have no standardised framework for describing assurance standards (i.e. to model the objectives, artefacts and activities required by a standard). Because of this they are encouraging the submission of CCL as a proposed new OMG standard. As a result of the evaluation of the CCL that has been performed within the course of the OPENCOSS project, it has been suggested that this proposal can proceed direct to the OMG's 'Request for Comment' stage, bypassing the preliminary 'Request for Proposal' stage. The CCL will be brought as a formal proposal to the OMG System Assurance Task Force at the June 2015 OMG Technical Meeting to be held in Berlin.

2.2 Industrial safety engineering and management standards

Although, in consortium judgement, formal dissemination of the project outcomes to industrial standards working parties was premature before conclusion and evaluation of research activities and it was noted that many working parties have been inactive during the OPENCOSS execution period, informal dissemination has taken place through OPENCOSS partners networks of contacts. These activities are expected to continue after completion of the project exploiting partners membership of- or strong links with- various groups as outlined in the following table.

Industrial Sector	Standard(s)	Partners strongly linked with the groups
Automotive	ISO26262	CRF, UoY
Aviation	ARP4754a, ARP4761a	Thales, UoY
	DO-178c	AdaCore, Thales, UoY
Railway	EN50126, EN50128, EN50129	Alstom, RINA

The dissemination activities will also exploit links with standardisation groups from industrial sectors not directly represented in OPENCOSS consortium (including UK Military, Medical Devices, etc.) and utilise connections to a range of standardisation bodies via members of the project's External Advisory Board.

The key objectives of these activities are:

1. To raise the profile of the OPENCOSS framework within communities of practice;
2. To communicate any ambiguities that are detected by OPENCOSS modelling activities in individual standards;
3. To ensure that OPENCOSS approach to cross-domain reuse of certification artefacts is not unduly impeded by the requirements of any emerging standards.

The second objective above warrants some further explanation. The Common Certification Language developed in OPENCOSS provides means for capturing requirements of requirements of individual industrial safety standards in a structured and semi-formal fashion. This modelling (and thus formalisation) activity provides a powerful approach to clarifying standards' requirements and detecting any ambiguities or potential internal inconsistencies. In particular, in our experience, modelling activity highlights issues with standards that are very difficult to detect by mere review of the free text documents.

Although time constraints of the project did not allow consortium partners to model complete standards, modelling of standards segments as part of OPENCOSS case studies has already highlighted some ambiguities and potential for contradiction. This knowledge has a potential for usefully feeding into and adding value to the standard revision processes.

A number of consortium partners intend to continue standards modelling activities after completion of the project. For instance, the University of York intends to model both ARP 4754 & \$761 documents and UK military standards DS00-55 and DS00-56[5]. Consortium members will also advocate use of OPENCOSS modelling framework alongside revision processes (or development of standards) to provide a powerful revision instrument before formal release of new standards versions.

2.3 Summary of certification follow-up activities

As indicated above certification activities, whilst started within task T8.4 of the project, will continue after completion of the project. These will be supported by individual partners actions. Table 1 below summarises actions currently planned by individual partners. It identifies overall objectives that partners will try to achieve along with medium- and long-term goals that are set by partners in order to achieve the objectives and the key risk factors / external dependencies for achieving the goals and objectives (termed "preconditions").

[5] UoY staff provides substantial input to the revision of these standards and intend to maintain involvement in further revision activities.

Table 1 - Planned Standardisation Follow-up Activities

Partner(s)	Long-term objective(s)	Short- & medium- terms goals	Preconditions (incl. resources)
UoY & Tecnalia	Ensure that concepts of safety case interfaces and contracts developed in WP5 are adopted in Issue 2 of Goal Structuring Notation (GSN) community standard.	Continue providing input to and attending meetings of the standardisation group. UoY to consolidate the Issue 2 of the standard	*none* (NB: expect to achieve by December 2015)
UoY, Tecnalia & Simula	Ensure that OPENCOSS outcomes (structured vocabulary and expression metamodel, modular safety cases and CCL artefact [meta]model) are incorporated into OMG's SACM 2.0	Continue providing input to and attending the meetings of SACM 2.0 revision task force. Facilitate publication of SACM 2.0 as Request for Comment (RFC) within OMG standardisation process.	*none* (NB: expect to achieve by end of 2015)
UoY & Tecnalia	Standardise CCL as an OMG standard	Contribute to the drafting of the formal proposal by June 2015. Facilitate publication of Request for Comment (RFC) following OMG Technical Meeting in Berlin.	*none*
UoY	Provide feedback to EUROCAE WG63 on ARP-4754a and ARP-4761a standards	*Within 18 months:* • Model ARPs within OPENCOSS framework. • Consolidate findings and recommendations. *Long-term:* Propose inclusions of standards' models in CCL as annexes to the standards themselves	• Continuous availability and support of OPENCOSS platform tools along with some support from tool partners. • Availability of internal resources. • Willingness of WG63 and the US counterpart committee (S18) to incorporate annex (dependent on visibility of OPECOSS outcomes after project completion)
UoY	Provide feedback to UK MoD on the new DS00-55 standard.	*Within 18 months:* • Model 4+1 principles and other standard requirements within OPENCOSS framework. • Consolidate findings and	• Continuous availability and support of OPENCOSS platform tools along with some support from tool partners. • Availability of internal resources.

		recommendations and provide models to MoD	
CRF	Clarify / develop relation to ISO 26262 standard.	Undertake internal dissemination and carry-out analysis of which relations could influence internal design processes.	Availability of internal and/or external funding.
IKV	Establish AUTOSAR Safety Extensions as main format for exchanging safety related information for AUTOSAR models	*Within 18 months:* work in AUTOSAR WP-A3 as document owner for Safety Extensions. Improve them in order to solve any issues that prevent them from being applied in wider contexts. *Within 36 months:* improve the tool support for AUTOSAR safety extensions. Extend the medina analyse tool as well as AUTOSAR configuration tools of IKV's mother company, KPIT, to support this standard.	Achieving consensus in AUTOSAR consortium on the applicability of AUTOSAR safety Extensions and the further improvement of them.
INTECS	Improve INTECS competence and reputation to provide safety expertise to support standardisation processes.	*Within 18 months:* participate in the definition of the new Motorcycle standards that will be derived from the ISO 26262 Automotive Standard. *Within 36 months:* • To deploy a safety expertise that is largely domain independent and easily deployable on different domains, depending on market opportunities. • To deploy a unique safety expertise that profit from cross-contamination from different domain with focus on automotive, avionics and railway. *General:* To continue advanced research and participation to safety boards to increase	*none*

		commonalities and consistency among safety communities of different domains.	
Altreonic	Follow the evolution of relevant safety and systems engineering standards.	Further refine our Systems Engineering metamodel.	Stable and proven in practice OPENCOSS model

3 External Advisory Board

During the Project execution we have had some meetings with the External Advisory Board which provided us some interesting insights for our project development (see Annex 1).
Once the project has reached its end we have had a Webex meeting where we provided a real demonstration of our Opencoss tools. In order to gather formally their feedback we developed a questionnaire which was answered by them. This questionnaire was structure in two parts: a set of questions which answers are using the following Likert scale:

1. Not at all
2. Not really
3. Undecided
4. Somewhat
5. Very much
6. Other

Q1: Are the implemented functionalities related to your day-to-day safety related engineering activities?

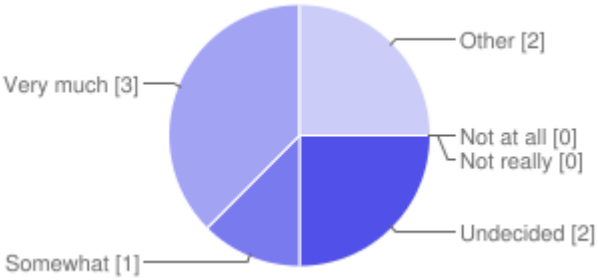


Figure 1: EAB opinion: Implemented functionalities

The majority of respondents consider that the functionalities implemented by the Opencoss project are considered in their daily lives. The Opencoss project consortium is aware of the limitations of our approach, and we need to complete this platform with new functionalities related to code analysis or testing functionalities for example.

Q2: Can you identify opportunities for using the approach ?

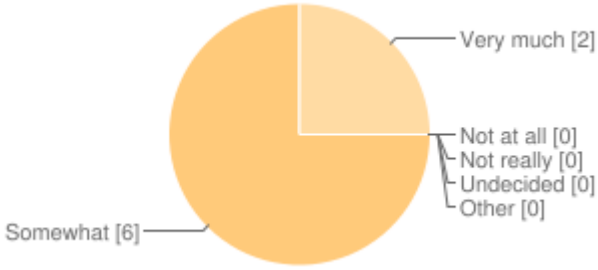


Figure 2: EAB opinion: opportunities

EAB members consider that this platform has several opportunities that can be exploited in a near future.

Q3: Is it methodologically sound?

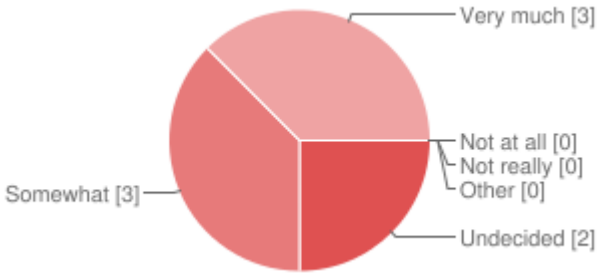


Figure 3: EAB opinion: methodologically sound

EAB members really appreciate the methodology implemented in our platform.

Q4: Are tools contributing to safety engineering discipline?

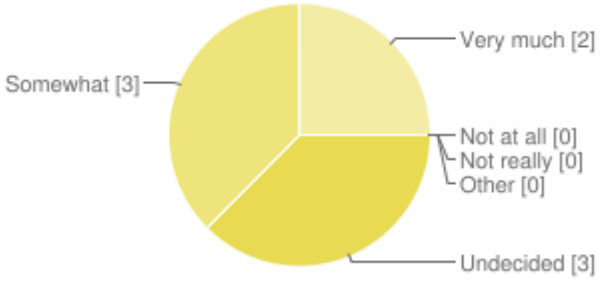


Figure 4: EAB opinion: safety engineering discipline

EAB members consider that the Opencoss platform contributes significantly to the safety engineering discipline.

Q5: Is the approach useful?

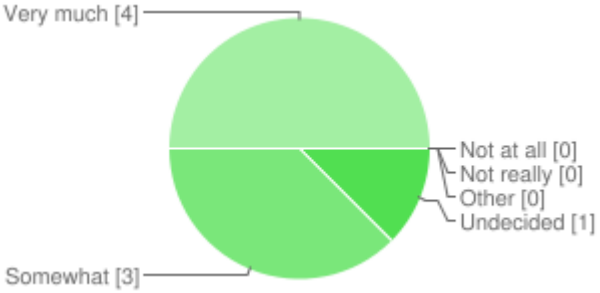


Figure 5: EAB opinion: Usefulness

EAB members consider really useful our approach.

Q6: Is the approach mature?

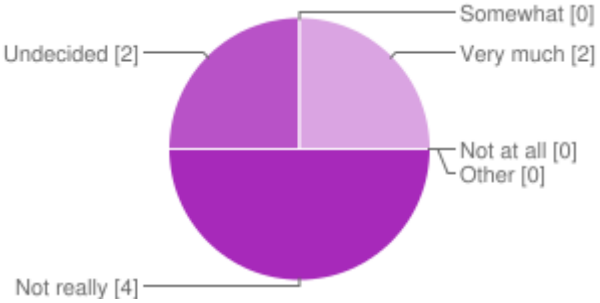


Figure 6: EAB opinion: maturity

Our Opencoss platform requires further developments and EAB members agreed that we need to invest more on the user interface.

Q7: How likely are you to adopt this approach and tools?

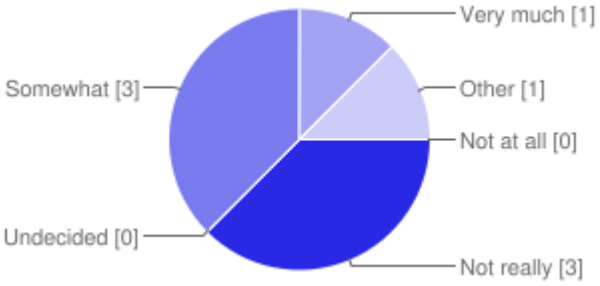


Figure 7: EAB opinion: adoption

This question is tightly related to the previous question (Q6) and obviously we need to invest more time and effort in order to make our platform attractive to be adopted.

In addition we asked to EAB for an informal feedback in a free text with the following questions:

Q8: Which aspects and on what kind of project?

The use of tools in avionics domain is complicated when showing compliance to airworthiness authorities; compliance results shown by the tool have to be error free and potentially cross-checked by other tools (or manually). The Opencoss tool would need stability, maturity and very short access time to be incorporated into a company referential.

Methodology if we run into a safety project (haven't landed one recently)

Medical devices. Managing information and assets in certification processes.

We often develop verification evidence for one system (e.g. an operating system) for several Safety Standards. We develop fine granularity relationships between the artifacts(requirement, test case,design component,code file, test, coverage file etc) and capture the standards requirements in a documents without fine granularity. Your approach does the opposite. Perhaps there should be a way to combine the approaches, so that the evidence can be prepared completely end-to-end covering various standards, and show their compliance. We are looking into this.

The formalism brought to the interpretation of standards.

Q9: Do you believe the approach has the potential to save money? How?

My research is unconcerned with costs, so I don't know.

Using a common language and interfaces for managing compliance between standards and regulations is a key approach to cost savings in cross-domain certification projects. The Opencoss tool would ease this step if implemented into the company referential, but not for a single project; processes are validated by airworthiness authorities on a global aspects across projects.

Managing the detailed certification requirements of a project is a lot of work. Company specific standards introduce a layer of complexity. As standards evolve, and company specific process plans (as well as customer process plans) also evolve, a way of tracking and relating this would certainly ease some of the problems and potentially save money. We do not have enough experience with this to say how much.

I am still not sure it fits well for our industry. Some practices are different. Moreover, it is very software development focused. They are mostly interested in standards for electrical safety. If it works fine for this kind of standards, then it will save money.

Tools could simplify the safety management processes. Applicability of CCL and reuse of safety argumentations and proofs between different areas seem less mature.

Standards and safety issues either are limited to the formulation of a safety functional analysis, and then the interpretation of standards can be very subjective. Further verification si still a major challenge. Solution shall bring order and structure that should assist on achieving coherence on the work by a major state zoned company<

Being able to link evidence etc cross-tools is a potential money saver since it reduces the time to locate, extract and visualize the neeed information.

Yes, not re-inventing the wheel and sharing best practices

The respondents were:

- Paulo Barbosa - State University of Paraiba - Brazil
- Javier Ibanez Guzman Renault S..A.S. France
- inspearit
- THALES AVIONICS
- Angelo Chiappini European Railway Agency
- Cecilia Ekelin, Volvo
- George Romanski - Verocel, Inc.

From the following sectors:

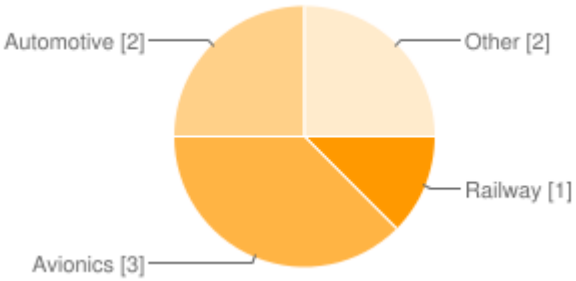


Figure 8: EAB respondent sectors

4 Roadmap

This section of the report presents OPENCOSS follow-up plans of individual consortium partners. Where possible, some common narrative is presented (although this is limited as, in absence of additional funding, it is not pragmatically possible to commit to coordination between partners efforts after the end of the present project). The plans are organised into the following areas:

- *Research:* areas for follow up research to be pursued by partners whether in the form of collaborative or single-partner research and regardless of the funding instruments.
- *Tool development:* Advancement of OPENCOSS tools as well as influence of the project on other tools developed by partners
- *Industrial Practice:* Potential influence of the project and/or the concepts it has explored on future industrial practice in safety engineering, management and certification.
- *Training and Education:* Influence of academic and professional education courses offered by consortium partners.

Partners' follow up plans are presented in the formal similar to that of the certification roadmap above – for each partner, or groups of partners we list the overarching objective, medium term goals and necessary preconditions.

4.1 Research Roadmap

A number of consortium partners (led by Tecnalia) intend to continue research cooperation in area of Cyber Physical Systems assurance and, specifically, on topics of System Architecture Driven Assurance and Multi-Concern Assurance. Another area for longer term collaborative research is concerned with the role of language in safety assurance and, more widely, risk communication.

System Architecture-driven Assurance

The OPENCOSS conceptual approach (concepts and relationships embedded in the CCL) is agnostic regarding system architectural choices. This is an intentional feature to meet OPENCOSS key requirements about cross-domain harmonization and flexibility. However, the characteristics of a CPS' architecture represent a major aspect for ensuring system dependability and for meeting assurance and certification needs and requirements. First, a CPS' architecture corresponds to the realization in the system of the mechanisms necessary to fulfil, among others, safety, performance, security, reliability, and availability requirements. Second, the architecture consists of the components selected for fulfilling such requirements, and these components will have specific dependability characteristics. These characteristics will impose constraints on component reuse, and thus such constraints must be taken into account when analysing this possibility. Reuse constraints can refer to both technical aspects (e.g., a component can only be deemed safe for a given operational context) and economical (e.g., component reuse will have a impact on CPS cost). Thirdly, a CPS' architecture must conform to the applicable standards so that a system complies with them.

There are several architecture-related features that have not been addressed in OPENCOSS but whose explicit consideration can greatly increase the opportunities of cost reduction and of reuse for CPSs, as well as facilitate the analysis of the features' impact on assurance and certification. The architecture-related features that future research will consider are the following ones.

Architectural Patterns for Assurance: OPENCOSS has a straightforward mechanism to specify assurance patterns for argumentation and for compliance with standards. However, further research and case studies are necessary to cohesively integrate these patterns in specific assurance and certification activities. This includes safety architectural patterns definition and application (3-level-monitoring, E2E protection, and partitioning, among others), and auto-generation of platform models and configurations based on these patterns (e.g. for AUTOSAR and IMA). The use of patterns speeds architecture specification and facilitates the (re)use of components targeted at being used in such patterns.

Link to System Models: The existing CCL metamodel corresponds mainly to an assurance metamodel, and should be extended with (or linked to) other modeling formalisms to enable a more detailed analysis of a system's dependability. For example the CCL should be extended with concepts such as fault, error, and failure to allow a better analysis of how these aspects affect assurance activities. In general, OPENCOSS results need to be extended for dealing with the linkage between its assurance framework and system functional property models. This will facilitate a finer-grained management of artefacts, such as those involved in the management of a hazard log in the railway domain: a hazard in a fault tree analysis, a safety requirement in a requirements specification, a block in an architecture specification, an interface in a design specification, a step in a verification report, a test case in a validation report, a section of a safety case, and so on. The current OPENCOSS models allow the treatment of artefacts only at a coarse "black box" level, and OPENCOSS assurance modelling must be linked to modelling formalisms for safety information (information necessary to realize, analyse and verify systems' safety) and to system modelling. We plan to study the relation of the OPENCOSS assurance model with different system modelling languages (e.g. UML, SysML, ADL etc.), safety modelling profiles, and specific platform models and architectures like AUTOSAR for automotive and IMA for avionics. A finer-grained analysis of a CPS and its assurance and certification information will allow industry to make more informed decisions regarding what can be reused between systems (including difference versions of a systems) and reuse consequences.

Assurance of Specific Technologies: Since OPENCOSS results are technology-agnostic, they do not directly support the assurance and certification of many characteristics of the new generations of CPS. Among others, these characteristics include mixed-criticality, the use of multicore technologies, and communication aspects. However, and as indicated for the features above, these characteristics have a great impact on how CPS assurance and certification has to be managed, and thus must be carefully taken into account. For example, the use of some technologies might be allowed for highly-critical CPSs. Therefore, the detailed characteristics of the most recent and future technologies for CPSs will determine under what circumstances they can be reused, assured, and certified. These characteristics should not be disregarded.

Multi-Concern Assurance

The OPENCOSS project has developed an approach for mapping safety assurance artefacts, techniques and requirements across domains, using the OPENCOSS CCL to resolve the inconsistencies in terminology across the target domains and to support informed reuse of

assurance assets. The compositional certification approach developed in OPENCOSS further supports reuse by encapsulating assurance concerns for individual components into reusable assurance argument modules and by providing a mechanism to configure these modules to form an overall system assurance case. In order to leverage the benefits of development methodologies based on the informed reuse of components fully, however, it is important to consider other aspects of the system's design and behaviour a part of the assurance framework. Characteristics such as reliability, availability, maintainability, safety, durability, performance and security also have an impact on safety, and need to be considered in the assurance of mission-critical cyber-physical systems.

In the future projects, we will aim to exploit the existing OPENCOSS approach and extend it to provide a tool-supported methodology for the development of assurance cases which address multiple system characteristics. There are two following aspects to this work.

Extension of the CCL and the compositional certification approach to address multiple concerns: The OPENCOSS CCL metamodel is relatively generic, and its extension to support the reuse of assurance data relating to other characteristics requires considerable further domain modelling, but no fundamental re-engineering of the approach. Similarly, the vocabulary will require the addition of further concepts, but the vocabulary-based and model-based techniques for using mappings between concepts are readily transferable. The contract-based approach to compositional certification developed in OPENCOSS depends, in some respects, on precise mechanisms associated with safety characteristics. In the future we propose to refine this approach to support the management of trade-offs between system characteristics.

Security Assurance: The synergies between safety and security seem to offer clear opportunities for the reuse of assurance assets, although prior research in this area has suggested that the domain-specific standards do not always support such reuse. Our future projects will focus initially on extending the OPENCOSS models and vocabulary to address those aspects of security which impact on safety issues for mission-critical cyber-physical systems, where the potential to save costs through reuse is high.

Language for Safety Assurance

The OPENCOSS project has provided useful insights into the difficulties and desirability of communicating safety concepts across and within domains. Dissemination activities during and surrounding the project have also indicated that there is a large amount of interest in, and traction for, common means of communication within the safety industries. A common safety terminology shared across organisations and domains is, however, still a distant aspiration, for a variety of socio-political reasons. Our future research in this area will therefore focus on extending and refining the translation-based techniques and tooling established during OPENCOSS, to investigate the possibilities for fully-automated comparison of terminology from two project or domain vocabularies. Other possible directions for study include refinement of the contract-generation work in WP5 to include the automated population of argument claims from some system models, the use of language models to provide automated validation for some aspects of argumentation and, potentially, the use of the structured expressions technique developed in OPENCOSS with NLP techniques to detect argument structures in existing free-text arguments and specification documents. Outside the assurance domain, the models and approach developed in OPENCOSS is readily extensible to requirements specification and review:

previous research has demonstrated that considerable cost savings can be made in this area using lightweight techniques, so the potential from the OPENCOSS work is considerable.

The above activities are dependent on availability of appropriate funding instruments under Horizon 2020, Artemis or other European R&D funding initiatives.

Table 2 below presents additional partners plans for the research follow up of OPENCOSS project.

Table 2 - Research Follow-up Activities

Partner(s)	Long-term objective(s)	Short- & medium- terms goals	Preconditions (incl. resources)
Tecnalia	Conduct & participate in collaborative European research to extend OPENCOSS framework; in particular, address issues of multi-concern assurance and system architecture driven assurance.	*Within 18 months:* submit AMASS (Architecture-driven, Multi-concern and seamless ASsurance and certification of cyber-physical Systems) proposal[6] for consideration under ECSEL (project outline stage). *Within 36 months:* • Monitor European collaborative research funding opportunities • Continue networking, consortium building and proposal development activities as appropriate	• Availability of funding in Horizon 2020 and ECSEL programmes for R&D in the areas of CPS assurance, integration of safety and security engineering, integration between design engineering and assurance management; including funding instruments suitable for development of: o Tools to improve reuse opportunities in CPS and to assist users in taking more documented decisions o Data, libraries and patterns to share concepts from various domains in CPS development and assurance
UoY	1. Extending and refining the translation-based techniques and tooling established during OPENCOSS, to investigate the possibilities for fully-automated comparison of terminology from two project or domain vocabularies. 2. Refinement of the contract-generation work in WP5 to include the automated population of argument claims from some system models, the use of language models to provide automated validation for some aspects of argumentation	*Within 18 months:* pump-priming activities including - • Identification of further case studies to facilitate the development of resources such as domain vocabularies • Research into automated comparison, possibly using ontology-based techniques • Dissemination of the techniques, in order to attract interest of partners in the requirements field. • Automated review techniques for	• Case study support from a range of industries • Continued funding from national or European bodies for research in assurance of CPS, contract-based engineering, requirements engineering and use of natural language processing in engineering, assurance and engineering management. • Stability in the assurance domain - i.e. the overriding paradigm of safety assurance to remain reasonably stable.

[6] In addition to Tecnalia, other OPENCOSS partners participating in the AMASS proposal include ikv++, Intecs and RINA; University of York is unable to join the proposal consortium due to limitations of ECSEL funding in the UK.

	3. Use of the structured expressions technique developed in OPENCOSS with NLP techniques to detect argument structures in existing free-text arguments and specification documents. 4. Extension of the models and approach developed in OPENCOSS to requirements specification and review	language aspects of argumentation. *Within 36 months:* preparation of further research grants to refine and automate the comparison of terminology and to investigate the use of structured expressions to detect argument structures in legacy arguments. *General:* Promotion of common assurance language approach in industry, standards bodies, etc. (see also standardisation follow-up)	
CRF	To develop revised version of OPENCOSS framework and platform tailored specifically for automotive domain.	*Within 18 months:* Analysis/specification of possible OPENCOSS automotive tailoring.	Availability of internal and/or external funding.
INTECS	Starting from a consolidated safety culture expand competence on security within embedded systems of automotive, avionics and railway domains. Support an integrated approach to safety and security. Combine the rigour of Safety and Security with the principles of Agile approaches.	• Join Horizon 2020 and/or ECSEL R&D project consortia. • Develop competency for provision of integrated and agile set of services and development addressing safety and security on different domains such as automotive, railway and avionics.	Suitable Horizon 2020 and ECSEL calls and availability of funding instruments
Altreonic	Link the GoedelWorks model with formal methods to be sure the evidence can be trusted.	n/a	*None*
RINA	RINA intends to participate in R&D projects aimed at developing new methodologies and procedures for the management of safety aspects and safety assessment outcomes (Safety Certificates, etc.) and spanning various safety critical business areas with an	RINA is willing to and looking for calls for tenders whose scope of work is in line with the aforementioned objective.	Availability of funding instruments for R&D activities in line with the aforementioned objective.

	emphasis on the transportation domain.		

4.2 Platform and Tools Roadmap

The tool partners of OPENCOSS consortium have developed their individual plans for utilising project outcomes in their current and future tools. These range from continuous improvement of tools developed in the project (Tecnalia) and adoption of some of the safety engineering & certification concepts explored in OPENCOSS within other tools (AdaCore, Altreonic, IKV, Parasoft) to use of technical solutions used by OPENCOSS platform (Parasoft) and monitoring of the developments in the market (Atego). A number of partners are interested in standardisation of OPENCOSS platform and establishing interfaces with other systems engineering tools through initiatives such as Polarsys and OSLC. These follow-up plans are presented in Table 3.

Additionally, in the longer term, OPENCOSS partners are interested in improving **interoperability of the OPENCOSS platform** with tools used in the development of safety-critical systems, whereby evidence can be manually generated or automatically generated by the tools themselves (code generators, testing tools, safety analysis tools, etc.). The challenge is to be able to gather evidence from different types of tools by means of standardized and well-defined adapters or exchange tools. There are some axes in this direction that can considerably improve the opportunities of OPENCOSS adoption:
Tool Integration: How to solve the problem of assurance information present at each development phase (concept, design, implementation, testing, validation) and multiple different tools involved at each phase so that the OPENCOSS tool platform needs to interwork with each of these tools. One promising approach is to use OSLC, by extending it to assurance aspects (safety, security, etc.).
Collaborative work: We mean supply chain and collaborative issues when developing, assuring and certifying cyber-physical systems. For instance, DIA definition (ISO 26262 OEM-Supplier interaction definition), platform to exchange safety related information, potentially as (private) cloud based collaboration service, related compositional, versioning and updating problems, related security and scalability problems, provision of server side services (like intelligent search, cross project consistency checks).
More automated tool support (e.g. what-if/impact analyses): There are a number of tool automation functionalities that will increase the opportunities of cost reductions. For instance, arguments pattern matching: automate the search for compliant arguments in a set of components to define a new safe application that conforms to a set of safety requirements. One typical scenario would be a project (e.g. in railway: segregated safety controller, reduce footprint of hardware, safe communication protocol) starting with several functional and safety requirements (or safety patterns), the OPENCOSS platform looks for adequate component candidates. In addition, there are great opportunities to automate the assurance decisions by informing about various what-if scenarios when changing any engineering feature.

These longer term tool development issues, however, require investment that goes beyond internal funding capability of individual partners and are dependent on availability of external R&D funding (perhaps, as part of a wider research project).

Table 3 - Tooling Follow-up Activities

Partner(s)	Long-term objective(s)	Short- & medium- terms goals	Preconditions (incl. resources)
Tecnalia	Improve OPENCOSS tools and their industrial maturity	*Within 18 months:* • Improve Ref Framework tools GUI and functionality • Improve Assurance Project tools (capability for project management) • Improve Baseline tools • Improve ArtefactModel tools (traceability functionality) • Enhance reporting functionality *Within 36 months:* • Improve information security, encryption and access management. • Introduce profiles management functionality • Improve tools usability • Improve performance characteristics • Introduce integrity control and improve data consistency • Introduce compliance report functionality (artefacts or activities) *General:* participate in Polarsys initiative	*None*
AdaCore	As a tool provider, the objective is to maximize the reuse of our past certification efforts when re-certifying/qualifying a tool for a different usage or a different standard.	*Within 18 months:* Continue investigating the concepts developed within the OPENCOSS project and apply the most interesting ones into the Qualifying Machine, our internal tool used to support certification. *Within 36 months:* to halve the costs needed to re-certify a tool within the same standard, and reduce three-fold the costs needed to certify for another standard.	
IKV	Improve integration with other tools, usually	*Within 18 months:* Support argumentation following	*none*

	used in safety project lifecycle (PLM, ALM, RM, CMS …) based on REST interfaces and (existing) open standards (such as OSLC) or upcoming new standards.	notation standards as GSN to safety cases argument and extensions but also for other places in IKV products (e.g. safety-goal-requirements breakdown). *Within 36 months:* Achieve an acceptable solution in IKV products to support tool based safety case composition for OEM/Tier or Tier/Tier collaboration.	
IKV	Adopt a server based solution based on the OpenCoss architecture and ideas for medini analyze to increase its usage in large distributed development contexts.	*Within 18 months:* Adopt the Argumentation notation extensions and evidence traceability concepts if applicable in the automotive industry. *Within 36 months:* Adopt the contracting/composition concepts if applicable in the automotive industry.	Legal and technical preconditions need to be fulfilled in the industry and a certain acceptance level has to be reached at potential customer sites. (NB: new contracting/composition concepts are rarely adopted by industry due to legal problems in OEM/tier relationships)
ATEGO	Once the OPENCOSS approach gains sufficient interest from our customers and CCL reaches standardisation our objective would be to consider supporting CCL in our modelling environment in addition to the current integration of our process management tool with OPENCOSS. So we have three tools involved: • PTC Integrity Process Director (process management tool) • The integration between PTC Integrity Process Director and the OPENCOSS platform that could be extended. • PTC Integrity Modeler (modeling tool) that could support CCL.	*Within 18 months:* • Provide free access to the integration developed between PTC Integrity Process Director and the OPENCOSS platform. • Enhance the PTC Integrity Process Director API used by the integration. *Within 36 months:* • If there is sufficient customer demand, productize the integration to provide a commercial version. • Keep the integration up to date with potential evolution of the OPENCOSS platform. • Propose as professional services adaption of our relevant off-the-shelf PTC Integrity Process Director process libraries to be aligned with OPENCOSS	Industrial adoption of the OPENCOSS Platform and/or CCL approach, and sufficient demand from our PTC Integrity Process Director customers. Currently CCL has been defined as a domain specific language. The precondition for us to support it in our modelling environment is that CCL reach standardisation at the OMG as an UML profile rather than a DSL. (Report from the last OMG Technical Meeting

		CCL meta-model. If CCL is standardized as an UML profile, we could also support this profile in our modelling environment (PTC Integrity Modeler).	indicated a preference for an UML profile.)
PARASOFT	As certification is becoming a driver of increasing importance for Parasoft products sales, we are going to leverage the certification knowledge gathered during participation in OPENCOSS project in the development of our products.	Incorporate certification aspects/issues into Parasoft Development Testing Platform. (The tool facilitates automated testing, quality policy enforcement, automated defect prevention and some of our customers and prospects pursue various standardisation and certification processes)	*None*
INTECS	Support OPENCOSS integration into Polasys Note: INTECS was *not* a tool developer within the project. However INTECS is committed to the success of the Topcased/Polarsys open platform that will integrate also results coming from OPENCOSS. This platform is aimed at supporting large and safety critical projects not only in avionics (Airbus) but also telecom (Ericsson), Automotive (Continental) and likely also railway (see the OpenETCS initiative from Deutsche Baan).	*Within 18 months:* • Be a visible on the market as a supporter of Polarsys. • Continue using Polarsys. *Within 36 months:* Establish itself as a key Italian stakeholder in Polarsis.	*None*
Altreonic	Expand the GoedelWorks metamodel.	*Within 18 months:* Integrate some of the relevant OPENCOSS, i.e. the arguments based approach, in GoedelWorks model. *General:* • Continue to use and promote the use of GoedelWorks. • Use GoedelWorks internally.	

4.3 Industrial Application and Practices Roadmap

The change of industrial practices is a complex and long process. A single research project, like OPENCOSS, cannot realistically expect to cause a revolution in industrial processes in a short-term. However, the project has demonstrated feasibility of the advocated approach and industrial partners of the consortium are committed to internal dissemination of the outcomes and gradual adoption of individual concepts – if not the entire framework – developed by the project.

It should be noted that one of the secondary, but very important, by-products of the project is establishing of networks between industrial and research, training and consultancy stakeholders. Combined with exposure of industrial partners to cutting edge concepts and principles this will naturally facilitate future smaller-scale collaboration that will, in turn, facilitate adoption of OPENCOSS concepts in industrial practices.

The long-term impact of OPENCOSS in terms of influencing industrial practices can be facilitated by a follow-up adoption program. This will be coordinated by Tecnalia but does, in part, depend on the availability of the external funding.

Table 4 presents follow up plans in this area.

Table 4 - Industrial Application and Practices Follow-Up Activities

Partner(s)	Long-term objective(s)	Short- & medium- terms goals	Preconditions (incl. resources)
ALSTOM	Alstom will integrate the outcomes of OPENCOSS into the development of internal guidelines for the Safety Assurance department (approaches to contract-based compositional certification for example) and into the expression of business needs (by Methods and Tools department) for tools providing engineering support (such as for process and evidence management). (Note: The emphasis will be on concepts rather than using specific tooling developed by OPENCOSS, until such a time as the OPENCOSS platform has been carried forward and industrialsed further.)	*Within 18 months:* Hold internal workshops with stakeholders from engineering and certification communities to disseminate information about the outcomes and elaborate follow-up proposals for concrete applications within our organization (such as elaboration of safety contracts for specific reused components defined at a level of granularity finer than the EN50129 Safety Case). *Within 36 months:* Influence the Methods and Tools department to extend their internal consultation process and the technology watch process, to ensure OPENCOSS outcomes are taken into account.	Support from other OPENCOSS partners in a form of provision of short 2-hour presentations or reports which more clearly summarize the link between business needs of industrial partners and OPENCOSS achievements in terms of new concepts (emphasis on concepts such as vocabulary and mappings in the CCL, not so much in terms of specific tooling, screenshots, architecture).
CRF	To adopt revised version of OPENCOSS framework tailored specifically to the automotive domain.	Tailoring of OPENCOSS framework[7] and platform to specific needs of automotive domain.	Availability of internal and/or external funding. *(See also CRF research follow-up activities)*
Tecnalia	Establish a strong industrial adoption program to create an open infrastructure and ecosystem to facilitate its integration with other ecosystems for CPS development (e.g. ECSEL/Artemis platforms).	More specifically Tecnalia plans: • Consolidation of an OPENCOSS Community (Users, developers, etc.) as part of Polarsys platform. • Eco-system creation: interconnections of different actors though Conferences, Communities, new Projects.	

[7] Editors' note: This involves instantiation of the framework/platform with a complete model of ISO26262 standard and/or local company's procedures designed to conform to the standard. (Consequently, part of this activity can also be seen as standardisation follow-up as described in previous section of this report).

		• Include Industrials from EAB in the new community. • Create Rules, Policies, Board of the community within Polarsys • Link with other platforms (ECSEL: ex-Artemis, etc.) • Industrial demonstrators in real environments, within new innovation projects • Work on socio-technical barriers for industrial adoption	
INTECS	Deploy a safety expertise that is largely domain independent and easily deployable on different domains, depending on market opportunities. Deploy a unique safety expertise that profit from cross-contamination by different domain with focus on automotive, avionics and railway.	*Within 18 months:* • Develop capability to move safety staff easily across safety projects from multiple domains. • To become more flexible in managing safety related projects in automotive, railway and avionics domains. *Within 36 months:* • Deploy a safety culture largely independent from the specific domain, providing unique and added value against our competitors. • Enter into new safety domains such as agriculture machines, medical devices, etc. *General:* develop internal knowhow, templates, methods and standards largely cross domain.	*None*

4.4 Training and Education Roadmap

OPENCOSS project has developed some innovative safety management and certification concepts and has increased maturity of some pre-existing state of the research & state of the art concepts. These outcomes embedded in the OPENCOSS framework and platform can be utilised in training (both academic and professional) of the future and current engineers and managers.

Within the project consortium a number of partners offer training and education services in areas covered by OPECOSS. For instance, the University of York (UoY) offers a comprehensive portfolio of both postgraduate and Continuous Professional Development (CPD) courses in high integrity systems engineering, safety management and certification. UoY clients include key industrial stakeholders in a number of industrial sectors in the UK, Europe and Worldwide whereas the MSc in Safety Critical Systems Engineering Course is internationally recognised as one of the strongest academic program in this area. Other consortium partners also offer relevant high-quality professional education services whether associated with respective partners 'core' consultancy and/or tool services or as a product in its own right.

Table 5 presents partners plans for exploitation of OPENCOSS outcomes in the context of academic and CPD training.

It is important to stress that those plans are not just a pathway of exploitation of OPENCOSS outcomes in their own right, incorporation of OPENCOSS concepts in training and education will provide a useful basis for other types follow-up activities (see sections above) and in particular would facilitate both research and industrial adoption of the OPENCOSS framework outside by stakeholders outside of the project consortium.

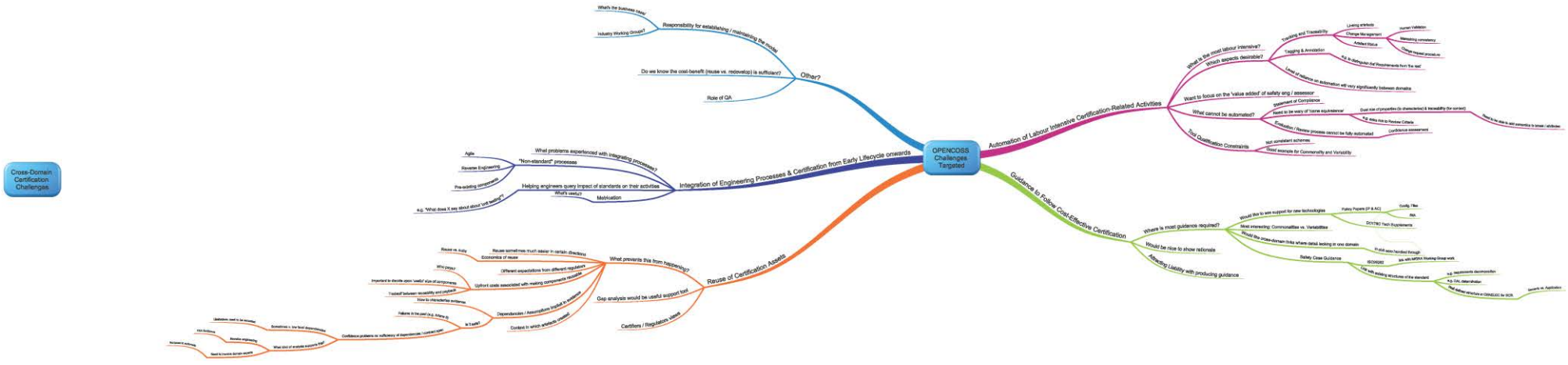
Table 5 - Training and Education Follow-up Activities

Partner(s)	Long-term objective(s)	Short- & medium- terms goals	Preconditions (incl. resources)
UoY	Incorporate OPENCOSS outcomes into (existing) MSc / Diploma / Certificate programme in Safety Critical Systems Engineering	*Within 18 months:* • Review current modules of the MSc programme to identify opportunities for inclusion of references and examples of OPENCOSS framework. (Candidate modules include, Foundations of System Safety Engineering [FSSE], Safety Case Development and Review [SCDR] and Computers and Safety [CASA]). • Develop models of key standards to be handed out. *Within 36 months:* • Undertake full revision of MSc curriculum • Consider feasibility of inclusion of a new module (e.g. model-based approaches to safety engineering or reuse of safety engineering and certification assets) that heavily draws from OPENCOSS outcomes.	*none*
UoY	Incorporate OPENCOSS outcomes into industrial Continuous Professional Development courses on Safety Engineering and Management.	*Within 18 months:* • Develop standard models that can be used in slides and hand-outs *(see UoY standardisation follow-up plans).* • Develop standard slide-packs on aspects of OPENCOSS framework that are most closely related to the more specialised CPD courses currently delivered by	The achievement has no strong dependencies and activities are planned already. However the following conditions would facilitate more timely achievement: • Demand from industrial clients on more advanced CPD provision in Safety Engineering and Management • Recognition of OPENCOSS concepts and outcome within industry and

		UoY. These are modular GSN, safety case module interfaces and contracts on the one hand and use of controlled expressions and vocabulary within safety cases on the other. *Within 36 months:* Develop standard slide-packs on other key aspects of OPENCOSS framework to be used on relevant CPD courses whenever an opportunity arises: • Artefact Models • Standard / Reference Framework Modelling • Cross-domain reuse of certification data	regulatory bodies • Standardisation of OPENCOSS outcomes • Availability of external (partial) funding for pilot course development and delivery The extent of coverage of OPENCOSS outcomes within CPD courses is also dependent on continuous availability of mature prototype tools.
ATEGO	If PTC Integrity Modeler were extended to support CCL and/or the integration between PTC Atego Process Director and the OPENCOSS platform new training courses could be developed or existing training courses extended.	n/a *(see ATEGO tooling follow-up plans)*	Industrial adoption of the OPENCOSS Platform and/or CCL approach, and sufficient demand from our customers. *(see ATEGO tool follow-up plans)*
INTECS	Extend existing and marketed training courses on safety (DO178C, CENELEC and ISO 26262) taking into account the acquired cross-domain expertise.	*Within 18 months:* • Develop a motorcycle safety course. • Develop a new CENELEC course. *Within 36 months:* become the Italian leader on professional training on E/E/PE safety with a focus on ISO26262, DO178C and CENELEC jurisdictions. *General:* Encourage cooperation with Universities and Research Centres to create a larger base of safety competence within Universities, with a cross-domain focus. This	

		includes support to define specific safety syllabus at the Universities as well as participation and organisation of safety related events and seminars.	
Altreonic	Organise workshops that promote a coherent and unified systems engineering approach.	Integrate the extend metamodel in the GoedelWorks literature.	n/a
RINA	Implementation of an efficient and straight forward process adopted by RINA personnel for the management of certification information and communication with the customers and the standardization of the safety assessment process.	*Within 18 months:* RINA personnel directly involved in the project will perform an internal workshop and training session in order to present the challenges that were faced by OPENCOSS project. In addition to this, they will describe the results achieved and the methodologies adopted within the OPENCOSS platform and considered as relevant for the achievement of the aforementioned long term objective. *Within 36 months:* RINA will try to tailor the assessment procedures currently in force for the safety assessment services, in order to capture the lesson learned and the feedback resulting from the internal analysis of the outcomes of the OPENCOSS project.	None

Annex 1:


Cross-Domain Certification Challenges
OPENCOSS Challenges Targeted
Automation of Labour Intensive Certification-Related Activities
Guidance to Follow Cost-Effective Certification
Integration of Engineering Processes & Certification from Early Lifecycle onwards
Reuse of Certification Assets
Other?
Responsibility for establishing / maintaining the model
Industry Working Groups?
Do we know the cost-benefit (reuse vs. redevelop) is sufficient?
Role of QA
Helping engineers query impact of standards on their activities
"Non-standard" processes
Agile
Reverse Engineering
Pre-existing components
Motivation
What's useful?
What problems experienced with integrating processes?
What prevents this from happening?
Economics of reuse
Different expectations from different regulators
Upfront costs associated with making components reusable
Dependencies / Assumptions tracked in evidence
Context in which artefacts created
Gap analysis would be useful support tool
Certifiers / Regulators aware
Tool Qualification Constraints
Statement of Compliance
Confidence assessment
Tagging & Annotation
Traceability
Change Management
Artefact Status
Where is most guidance required?
Would be nice to show rationale
Affecting Liability with producing guidance
Safety Case Guidance
Safety Patterns (SP & AC)
Config. Files
AMA
DO178C Tech Supplements
IEC61508
Would like cross-domain links where detail lacking in one domain