Collaborative Large-scale Integrating Project

Open Platform for EvolutioNary Certification Of Safety-critical Systems

Business Cases and User Needs

D2.1

<table>
<thead>
<tr>
<th>Work Package:</th>
<th>WP2: Business cases and user needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination level:</td>
<td>PU</td>
</tr>
<tr>
<td>Status:</td>
<td>Final</td>
</tr>
<tr>
<td>Date:</td>
<td>01 June 2012</td>
</tr>
<tr>
<td>Responsible partner:</td>
<td>Martijn Klabbers (TUE)</td>
</tr>
<tr>
<td>Contact information:</td>
<td><a href="mailto:martijn@laquso.com">martijn@laquso.com</a> <a href="mailto:M.D.Klabbers@tue.nl">M.D.Klabbers@tue.nl</a></td>
</tr>
</tbody>
</table>

PROPRIETARY RIGHTS STATEMENT
This document contains information, which is proprietary to the OPENCOSS Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the OPENCOSS consortium.
Contributors

<table>
<thead>
<tr>
<th>Names</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Giorgio Tagliaferri, Vincenzo Manni</td>
<td>RINA Services SpA</td>
</tr>
<tr>
<td>Martijn Klabbers, Joost Gabriels, Luna Yaping Luo</td>
<td>Eindhoven University of Technology</td>
</tr>
<tr>
<td>Janusz Studziszba</td>
<td>Parasoft SA</td>
</tr>
<tr>
<td>Mireille Larnac, Florent Pages, Michel Ilkiewicz</td>
<td>Inspeart (before DNV ITGS)</td>
</tr>
<tr>
<td>Katrina Attwood, Oleg Lisagor</td>
<td>University of York</td>
</tr>
<tr>
<td>Fulvio Tagliabò, Alberto</td>
<td>Centro Ricerche Fiat S.C.p.A.</td>
</tr>
<tr>
<td>Cedric Chevrel</td>
<td>THALES Avionics</td>
</tr>
</tbody>
</table>

Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>2011-12-01</td>
<td>ToC</td>
</tr>
<tr>
<td>V0.2</td>
<td>2011-12-16</td>
<td>First draft version</td>
</tr>
<tr>
<td>V0.3</td>
<td>2012-03-11</td>
<td>First full version</td>
</tr>
<tr>
<td>V0.4</td>
<td>2010-03-12</td>
<td>Ready for core group review</td>
</tr>
<tr>
<td>V0.5</td>
<td>2012-04-30</td>
<td>Ready for internal review</td>
</tr>
<tr>
<td>V0.9</td>
<td>2012-05-29</td>
<td>Ready for PB review</td>
</tr>
<tr>
<td>V1.0</td>
<td>2010-05-31</td>
<td>Approved by PB</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1 Executive Summary ........................................................................................................... 7

2 Introduction ......................................................................................................................... 9

3 OPENCOSs mission and vision .......................................................................................... 11
   3.1 Introduction .................................................................................................................. 11
   3.2 Vision and Scope ......................................................................................................... 11
   3.3 Mission and objectives ............................................................................................... 13
   3.4 Relation with other OPENCOSs work packages and tasks ........................................... 14
       3.4.1 Relation with work package 1 (WP1) ................................................................. 14
       3.4.2 Relation within work package 2 (WP2) ............................................................. 15
       3.4.3 Relation with work packages 4 through 7 (WP4–WP7) ...................................... 15

4 The general OPENCOSs business case ............................................................................... 16
   4.1 Introduction ................................................................................................................ 16
   4.2 BOAT framework ....................................................................................................... 16
   4.3 The Business Model Canvas ....................................................................................... 18
   4.4 e² Value Models ........................................................................................................ 19
       4.4.1 Introduction ....................................................................................................... 19
       4.4.2 Methodology .................................................................................................... 20
       4.4.3 Example e² value model in the safety assessment context .............................. 20

5 Domain related OPENCOSs Business Cases ................................................................... 22
   5.1 Introduction ................................................................................................................ 22
   5.2 Approach ................................................................................................................... 22
   5.3 Avionics domain ........................................................................................................ 23
       5.3.1 Business cases: Avionics domain ...................................................................... 25
   5.4 Railway domain ........................................................................................................ 31
       5.4.1 Business cases: Railway domain ....................................................................... 32
   5.5 Automotive domain .................................................................................................. 43
       5.5.1 Business cases: Automotive domain ................................................................. 44
   5.6 Conclusion ................................................................................................................ 55

6 Stakeholder goals and user needs ..................................................................................... 57
   6.1 Stakeholders ............................................................................................................. 57
   6.2 Stakeholder Analysis ................................................................................................. 59
       6.2.1 Avionics Stakeholders for the OPENCOSs Platform ......................................... 60
       6.2.2 Railway Stakeholders for the OPENCOSs Platform ........................................... 61
       6.2.3 Automotive Stakeholders for the OPENCOSs Platform .................................... 63
       6.2.4 General Stakeholder Model for the OPENCOSs Platform ............................... 63
   6.3 User Needs .............................................................................................................. 66
       6.3.1 User Needs for the Avionic Domain ................................................................. 66
       6.3.2 User Needs for the Railway Domain ................................................................... 67
       6.3.3 User Needs for the Automotive Domain ........................................................... 68

7 Conclusion ......................................................................................................................... 69

8 Appendix: Commonalities ................................................................................................. 71
   8.1 Cross domain business processes ............................................................................. 71

9 Appendix: Abbreviations and Definitions ........................................................................ 74
   9.1 Abbreviations .......................................................................................................... 74
9.2 Definitions ........................................................................................................................................ 74
10 Appendix: References ......................................................................................................................... 76
11 Appendix: Relations between WPs and Deliverables ........................................................................ 77
12 Appendix: a BOAT framework view on OPENCOSS ....................................................................... 78
  12.1 Introduction .................................................................................................................................. 78
  12.2 Phases of the BOAT framework ................................................................................................. 78
  12.3 Business aspect ............................................................................................................................ 79
    12.3.1 Reach and Richness .............................................................................................................. 80
    12.3.2 Reorganisation in business chains ....................................................................................... 80
    12.3.3 Business direction ................................................................................................................ 81
    12.3.4 Business structures .............................................................................................................. 81
    12.3.5 Business model .................................................................................................................... 81
  12.4 Organization aspect ...................................................................................................................... 82
  12.5 Architecture aspect ...................................................................................................................... 82
  12.6 Technology aspect ....................................................................................................................... 82
13 Appendix: A Business Model Canvas view on OPENCOSS ................................................................. 83
  13.1 History .......................................................................................................................................... 83
  13.2 The Canvas .................................................................................................................................... 83
  13.3 Customer segments ...................................................................................................................... 84
  13.4 Value proposition .......................................................................................................................... 85
  13.5 Channels ........................................................................................................................................ 85
  13.6 Customer relationships ................................................................................................................ 85
  13.7 Revenue streams .......................................................................................................................... 86
  13.8 Key resources .............................................................................................................................. 86
  13.9 Key activities ............................................................................................................................... 86
  13.10 Key partners .............................................................................................................................. 86
  13.11 Cost structure ............................................................................................................................. 87
  13.12 The resulting Canvas .................................................................................................................. 87
14 Appendix: e³ value model elicitation steps ......................................................................................... 89
15 Appendix: European projects related to OPENCOSS ....................................................................... 91
16 Appendix: The Volere Stakeholder Template .................................................................................... 99
17 Appendix: a cross domain high level scenario .................................................................................. 101
  17.1 Purpose of scenario ..................................................................................................................... 101
  17.2 Background: The OpenComRTOS .............................................................................................. 101
List of Figures

Figure 1: The Business Model Canvas for OPENCOSS ................................................................. 19
Figure 2: Simple example e3 value model (from [1]) ................................................................. 20
Figure 3: Example of a general e3 value model of the safety assessment field .................................... 21
Figure 4: Safety assessment business process for the avionics domain ........................................... 24
Figure 5: The Business Model Canvas for avionics ....................................................................... 25
Figure 6: Unification of the certification dossier by introducing the OPENCOSS platform/community ...... 27
Figure 7: Unification for working group improvement by introducing the OPENCOSS platform/community ................................................................. 28
Figure 8: Improved insight in data through traceability overview ................................................... 29
Figure 9: Reuse of certification dossier .......................................................................................... 30
Figure 10: Safety assessment business process for the railway domain ......................................... 31
Figure 11: The Business Model Canvas for railway ........................................................................ 32
Figure 12: Assessment of a system made up of two sub-systems, each assigned to a specific ISA .......... 36
Figure 13: Sequence diagram related to delta-assessment ............................................................... 37
Figure 14: Delta-assessment e3 value model .................................................................................... 38
Figure 15: Avoid complete recertification for products entering another country market .................. 41
Figure 16: e3 Value Model on Better view on relation between requirements and system ................... 42
Figure 17: Safety assessment business process for the automotive domain ..................................... 43
Figure 18: The Business Model Canvas for automotive .................................................................... 46
Figure 19: e3 value model in automotive maximise safety (and reuse) ............................................. 50
Figure 20: e3 value model for automotive marketing ........................................................................ 53
Figure 21: e3 value model on decrease claims .................................................................................. 55
Figure 22: Generic Onion Model of Stakeholder Roles (from [6]) ................................................... 58
Figure 23: ‘Onion Model’ of OPENCOSS Platform Stakeholders .................................................... 64
Figure 24: General safety assessment business process ................................................................. 72
Figure 25: Business aspects for e-business models (the BOAT framework) ...................................... 79
Figure 26: Reach and richness ........................................................................................................ 80
Figure 27: Disintermediation in a business chain of activities ......................................................... 81
Figure 28: Reintermediation in a business chain of activities ........................................................... 81
Figure 29: The Business Model Canvas ......................................................................................... 84
Figure 30: The Business Model Canvas for OPENCOSS ................................................................. 87
List of Tables

Table 1: OPENCOSS’ BOAT Business model .......................................................... 17
Table 2: OPENCOSS’ BOAT Business model for avionics ........................................... 25
Table 3: OPENCOSS’ BOAT Business model for railway ........................................... 33
Table 4: OPENCOSS’ BOAT Business model for automotive ....................................... 46
Table 5: OPENCOSS’ BOAT Business model .......................................................... 82
1 Executive Summary

This document represents the first deliverable of OPENCOSS WP2. This deliverable aims at specifying business cases and user needs. The intention is to provide a definition of the first common vision of the scenarios in which the OPENCOSS platform will be implemented and fully operational.

This deliverable provides a systematic analysis and formulation of the meaningful business models for the OPENCOSS platform and captures the needs of the different types of OPENCOSS stakeholders, including tool vendors, embedded systems developers, integrators, system and system of systems providers, certification entities, governmental agencies, regulation bodies, and standardization bodies.

The main topics of this document are:

1) description of business case scenarios for the proposed platform, for each domain of application of OPENCOSS approach itself (i.e. automotive, avionics, railway);
2) identification of the parties benefitting from the whole project and their characteristics, in order to establish stakeholder needs referred to the proposed scenarios.

Before describing the business case scenarios, the deliverable introduces for each application domain in OPENCOSS a business case using three business modelling frameworks, the Business Model Canvas, the BOAT framework, and the e³ Value Models in order to show respectively the general context of the business case, specifically the e-business opportunities, and the specific value exchanges between the stakeholders.

The latter method, e³ Value Model, originally aims to quantify the value exchanges. In this document we have mainly used these models to detail the business cases and relate them to the other frameworks. The reason for that is that in the context of safety and the involved trust issues, there are a number of intangibles that make a hard to quantify the effect of the introduction of the OPENCOSS platform. Finally, a domain independent view for these frameworks is described with the aim of describing the added value for certification of safety critical systems in general and in finding commonalities between and overlapping business targets in the application domains in OPENCOSS.

This deliverable, D2.1, summarises the purpose of every other relevant work package (WP) in OPENCOSS and its relation with WP2. D2.1 establishes the foundations from which part of the future work in WP2 will be performed. In particular, D2.1 will mainly serve as input for D2.2, which will specify high-level requirements for the OPENCOSS platform. D2.1 will also have an impact on the other deliverables of this and other work packages.

Conclusions of this deliverable are that the business cases for all of the domains which have been analysed share common themes. We see unification, innovation, and reuse as common denominators for all domains included in the OPENCOSS project:

- Unification helps the common understanding between assessors and manufacturers, but also between stakeholders in different domains. Provides a faster assessment process and a safer product by increased understandability.
- Innovation will be based on cross-over effects between application domains and applying theoretical knowledge in practice. Dependent on the innovation, it will result in a faster assessment process, a safer product, etc.
- Reuse of the assessment data of already approved systems or system component. From a development perspective, we expect the OPENCOSS platform to minimize development activities where possibilities, time and cost by facilitating the reuse of components. This also holds for the certification perspective in the reuse of assessment information, possibly even across domains.
Additionally, these denominators can also be combined. We expect OPENCOSS to minimize certification effort by streamlining the certification argument through unification.

Finally, the OPENCOSS business cases provide enough support to claim that the future OPENCOSS platform has, from a business perspective, a clear and feasible goal.
2 Introduction

Safety assurance and certification are among the most expensive and time-consuming tasks in the development of safety-critical embedded systems. European innovation and productivity in this market is curtailed by the lack of affordable (re)certification approaches. Major problems arise when evolutions to a system entail reconstruction of the entire body of certification arguments and evidence. Further, market trends strongly suggest that many future (embedded) systems will comprise of heterogeneous, dynamic coalitions of systems of systems. As such, they will have to be built and assessed according to numerous standards and regulations. Current certification practices will be prohibitively costly to apply to this kind of embedded systems.

The OPENCOSS project aims to devise a common certification framework that spans different vertical markets in, first of all, the transport sector and facilitates the reuse of assurance assets across and between domains, and to establish an open-source platform or safety certification infrastructure. The infrastructure is being realised as a tightly integrated solution, supporting interoperability with existing development and assurance tools. The ultimate goal of the project is to bring about substantial reductions in recurring safety certification costs, and at the same time to increase product safety through the introduction of more systematic certification practices. Both will boost innovation and system upgrades considerably.

Note that the OPENCOSS platform is currently under definition. The partners included in the OPENCOSS consortium are the first to start the OPENCOSS community and contribute to the future platform. After the project, this community and platform will continue to develop and mature. The goal of OPENCOSS is to produce a proof of concept, beyond the proof of principle, in order to demonstrate that a prototype OPENCOSS platform can support safety assessments based on real data in a tractable way. With this concept in mind, we will look at the relevant respective business cases. The business cases described in this document are aimed at the community and platform in the years after the project has ended successfully.

We will call the community contributing to the platform the OPENCOSS community and its product the OPENCOSS platform. Note that the community probably will include the users of the OPENCOSS platform.

The objective of this deliverable is to provide a systematic analysis and formulation of the meaningful business models of the OPENCOSS platform and capture needs of the different types of OPENCOSS stakeholders including tool vendors, embedded systems developers, integrators, system and system of systems providers, certification entities, governmental agencies, regulation bodies, and standardization bodies.

This document specifies business cases and user needs. The OPENCOSS partners have described the overall environment targeted by the OPENCOSS project in order to define a common vision of the scenarios in which the OPENCOSS platform will be implemented and will become operational. The first stage towards the architectural definition is the description of business case scenarios for the proposed platform. Business cases provide a description of the target markets, technology enablers, system boundaries, regulatory context, safety certification scenarios, costs, and metrics to measure the degree of success. This description must be understandable by stakeholders outside the project but also must be a reference point within the project, expressed in a uniform language. OPENCOSS will evaluate the use of sequence diagrams (e.g., UML sequence diagrams) to specify the interaction between stakeholders and the OPENCOSS platform, and experiment with this rather unique value models (e³-value approach developed by Jaap Gordijn and Hans Akkermans) to attempt to specify the value exchange between stakeholders.

The identification of the parties benefiting from the whole project (tool vendors, embedded systems developers, integrators, system and system of systems providers, certification entities, governmental agencies, regulation bodies, standardization bodies, but also civilians or the transportation users, and the European committee as a representative group, and their characteristics will be the first step to establish
the stakeholder needs and to detail the proposed scenarios. An economic assessment will also be provided to show what solutions are most likely economically feasible. However, in the context of safety and the involved trust issues, there are a number of intangibles that make a hard to quantify the effect of the introduction of the OPENCOSS platform. The feasibility of the project goals' has been substantiated by validating them in a comparison with the other business frameworks and by verifying the achievability of the economic savings for the platform’s users.

In Chapter 3, the mission and vision describe the goals of OPENCOSS and the landscape it is operating in. This chapter also describes the relations within OPENCOSS between this deliverable on the one hand and the activities in the other tasks and work packages. Chapter 4 continues the general OPENCOSS business case and the approaches to describe the business cases. In Chapter 5, the business cases for each domain included in the OPENCOSS are discussed and the specific business cases analysed. Chapter 6 then deepens the understanding of the business case actors in the stakeholder goals and user needs. Chapter 7 describes the conclusion of this document.

Chapter 8 through 17 are the appendices for the document. The commonalities described in Chapter 8 tackle the differences and similarities of the concrete business cases described in Chapter 5 and the goals and needs in Chapter 6. Chapter 9 describes the concepts and abbreviations used in this document, Chapter 10 provides the references to supporting literature. Chapter 11 describes the relationships with other tasks and work packages.

Chapter 12, 13, and 14 explain the approaches for describing business cases, respectively the BOAT framework, the Business Modelling Canvas, and the e3 value model. Chapter 15 lists an overview of related European projects, Chapter 16 describes the Volere Stakeholder Template and Chapter 17 describes a more detailed cross domain scenario.
3  OPENCOSS mission and vision

3.1  Introduction

Innovation and productivity in the adoption and development of safety-critical embedded systems, in, for example, the transportation sector in Europe face many challenges related to the safety certification of systems and their component parts. In particular, safety critical system’s industry finds it hard to reap the benefits afforded by incremental- and reuse-based approaches to the development of systems in other sectors (e.g. modular and component-based design, the use of pre-existing, off-the-shelf components, product-line development and so on), due to the need for the expensive repetition and reconfiguration of the entire safety certification information – arguments and supporting evidence – for each system variant. The OPENCOSS (Open Platform for Evolutionary Certification Of Safety-critical Systems) project has as its main objective to reduce both the time and the cost overhead inherent in the safety (re)certification of safety critical systems. The project aims to achieve this by the development of compositional and evolutionary techniques for certification and by realizing open-source safety certification platform for different system markets, facilitating the reuse of certification assets. The techniques are intended to target the railway, avionics, and automotive domains, in first instance.

Section 3.2 introduces the overall vision and scope statements for the OPENCOSS project, in order to contextualise the wider business and stakeholder objectives outlined in Chapters 4 through 6. Section 3.2 also gives further details of the vision, scope and contribution of OPENCOSS, in the light of recent discussions and renewed understanding of the state of safety (re)certification activity across the target domains. The general objectives of the project, as presented in the ‘Definition of Work’ presented in Annex A of the original grant proposal document [8], are described in Section 3.3. Section 3.4 details the means by which the project seeks to address the business and stakeholder needs, giving a detailed breakdown of the concerns of the various work packages in fulfilling the overall project objectives.

3.2  Vision and Scope

At the heart of OPENCOSS is the aim of enabling (component) manufacturers of embedded systems in safety-critical domains to leverage the benefits of modern reuse-centric development techniques – such as the use of off-the-shelf components, the incremental development of systems using product-line techniques and the use of modular approaches to software integration. The project is focussed not on the technical challenges of applying such techniques in real-time, safety-critical embedded systems development, but on the integration and management of the regulatory aspects of the development: how these systems receive approval for operation in specified contexts-of-use.

In order to gain approval from the relevant authorities and regulatory bodies, the developers of a safety-critical system need to demonstrate that the system is acceptably safe to operate in its intended, clearly-defined, context. Conceptually, this means that all of the potential system hazards – operational misbehaviour or conditions which might lead to an accident leading to injury or loss of human life or to damage to the environment – are either prevented or mitigated in the design of the system. Rigorous analysis, checking, and testing is carried out to ensure that the design demonstrates an absence of hazards and that the system-as-built meets its requirements.

In most industries, manufacturers are required to produce an explicit safety case, in order to demonstrate that all of the hazards have been prevented or mitigated and that the system is acceptably safe to operate in its intended context of use. A safety case, in this context, is a structured argument, supported by a body of evidence that provides a compelling, comprehensive and valid case that a given system is safe for a given application in a given operating environment. The nature of the support offered to the argument by
the test and analysis results typically appealed to as evidence should also be demonstrated, in terms of the argument developer’s degree of confidence in the strength of the argument. Part of the argument presented in a safety case of this kind will also aim to show that the system-as-built conforms to the relevant safety and development standards.

In some sectors, an explicit safety case is not required. Rather, manufacturers are required to demonstrate compliance to a particular safety standard, guidance document or company practice statement, which will provide an account of the required development processes, analyses and testing to be performed, and will mandate a particular level of rigour of adherence to be shown. Note that complete systems require safety compliance, whereas system components need assurance for the relevant properties. The relationship between the component’s assurance properties and the system’s safety case are provided in the argumentation of the safety case.

The OPENCOSS project adopts the position that, even in this compliance-focused, standards-based approach to safety demonstration, the safety engineer will need to adopt the kind of thinking required to produce the explicit argument-based approach, albeit without the need to make it explicit. In order to claim safety compliance, it will be necessary for him/her to consider the relationship between the analysis and test artefacts produced during the development and the requirements laid down by the standard/guidance or best practice document. He/she will have to persuade him or herself of the adequacy of the results, in order to determine that the processes and analyses that have been carried out are sufficient to make the claim of the adequate safety of the system which is implied by his presentation of the compliance documentation for final scrutiny.

This kind of thinking about the justification of safety is central to the OPENCOSS project. The project aims to develop technology to support the reuse of safety evidence artefacts – test and analysis results, associated with particular reusable system components – across system development projects within and across safety-critical domains. In principle, such reuse should reduce the recertification effort, although this might not be completely true for cross domain certification assessment. In order to carry out the reuse – and to ensure that it does not in itself introduce potential hazards into the target system –, and to leverage its benefits, it is necessary to understand the explicit reasoning about the nature of the safety claims made about the component or system in the original context, and how the evidence presented there supported those claims. This “safety argument thinking” – at the abstract level – is essential to ensure that compliance with standards is demonstrating safety in this new context as well. This subject is further tackled in the technical work packages, and WP5, Compositional Certification, in specific.

The safety demonstration by a safety case will therefore be a central concept in the OPENCOSS Platform.

The platform will be released as an open-source tool infrastructure for safety assessments where the development and progress of the safety case will have a central role. The platform will basically consist of a set of tools that:

1. Interface with existing tools (open- and closed-source) in order to avoid new and possibly unstable implementations, while reuse of proven technology has as advantage reliable, trusted, compliant, possibly certified software that is broadly accepted by industry and regulators. The existing tools need to provide additional value to the development of the safety case;
2. Could be created from or based on the building blocks from OPENCOSS partners (Qualifying Machine from AdaCore, Tecnalia tools for Compliance Management, etc.), which provide additional value to the development of the safety case;
3. Are created from scratch and provide new functionality to the development of safety cases.
4. Support the demonstration of compliance to a defined standard, guidance document or checklist, with an informed understanding of the implications of the requirements and the nature of the ‘proof of compliance’ offered by the evidence artefacts.
The biggest challenge of the platform is to provide functionality that supports the reuse of safety cases. Several types of reuse might be envisaged:

a) reusing evidence for a next version of a safety critical system, within a project or organisation
b) reusing a safety case for a component or a subsystem of a new system, possibly across domains,
c) reusing (part of) a safety case in order to show compliance to another standard,
d) reusing and improving a safety case in order to regain confidence, for example after a catastrophic accident,
e) reusing a safety case for a system in another domain.

The platform must exceed the functionality of a checklist, but will never generate the safety case completely automatically; the user, either an assessor, developer, or a safety manager must always have control over the judgements included in the safety case, because these persons need to be informed about and in control over the overall safety case, no decisions or judgements may be kept outside the awareness of the user. The tool may provide tips to the user to improve the safety case by means of suggesting proven solution patterns, and may also provide guidance on the implications of particular ways of phrasing claims, in terms of the nature of the support they require from the evidence.

One of the techniques by which the OPENCOSS approach will facilitate the reuse of reasoning (implicit or explicit) and evidence relating to compliance is called the Common Certification Language (CCL). This technique, which is detailed in work package 4 (WP4), enables the OPENCOSS platform to be released without any specific data of standards, knowledge on standards, or specific expertise of the partners, unless partners are willing to share this information, of course. Future users must provide the data for the safety demonstration, for example: the safety requirements from standards, evidence, safety arguments, etc. Whether the interpretation of the standard can be shared openly is at this moment still under debate: it is important to note that standards are not free and are generally only available under license, so it is potentially the case that making interpretations of the standards freely available would bypass these licences.

In this document we initially maximize the scope in order to maximize the number of profitable business cases. We will look at the domains included in the OPENCOSS project in more detail. The aim is to provide a platform that is domain independent.

3.3 Mission and objectives

The OPENCOSS Description of Work [8] states that the overall mission or goal of OPENCOSS is to improve the current situation relating to the costs of certification in safety-critical systems development. The improvements are intended:

- to demonstrate a potential reduction of recurring costs for component/product safety certification across systems by 40% and across vertical markets by 30% (G1)
- to demonstrate a potential reduction of product safety risks by 20% (G2)
- to demonstrate a potential gain for product innovation and upgrading by 20% (G3)

The OPENCOSS main objective and overall goals will be achieved by means of the following project objectives:

- Define a common conceptual safety certification language to improve mutual recognition agreement of safety approvals and to be employed to discuss abstract notions from different industrial markets. (O1)
• Define a compositional and evolutionary approach that reuses safety arguments, in a way that it is easily certifiable and that such certification is re-usable when integrating the product in higher level systems and interconnected systems. (O2)

• Develop a fully-fledged open-source tool infrastructure that will allow developers and other safety assurance stakeholders to:
  - Reduce uncertainty and (re)certification costs by following a measurable and auditable process (O3.a)
  - Assess their compliance with safety standards and practices (O3.b)

• Benchmark the tool infrastructure against real industrial cases from railway, avionics and automotive. (O4)

• Support the OPENCOSS community building and standardization of:
  - The common conceptual safety certification framework as a “de-jure” standard. (O5.a)
  - The open-source tool infrastructure as a “de-facto” standard. (O5.b)

3.4 Relation with other OPENCOSS work packages and tasks

The relationships between work packages and tasks are visually represented in Appendix A. Below is the explanation of this picture.

3.4.1 Relation with work package 1 (WP1)

Work package 1 (WP1: Use Case Specification and Benchmark) will quantify the effect of the OPENCOSS platform on the effectiveness and efficiency of the chosen business use cases or demonstrators. The overall degree of achievement of the project goals will be assessed by comparing the results from the use cases in terms of improvements in safety, costs, and speed with the original way of working before OPENCOSS.

This deliverable will benefit from the WP1 results by understanding the constraints of the practical use cases and demonstrators and to refine the vision and scope based on these constraints.

The first deliverable of WP1, D1.1, contributes to the inputs for the definition of the overall project architecture and of the basic approach to a general requirements framework among the various domains (Automotive, Avionics, Railway), from which derive the guidelines for the design of the common certification platform and its integration and validation.

The aim of D1.1 is to identify in the certification processes from the different domains the constraints and requirements that are to be considered by the project as target for the development of the general framework supporting the design of the common certification platform. The applicable legislative background, the standards and the best practices used in order to deliver products to a customer have been considered. The voluntary and regulatory actions in the development of a certified product in each domain have been also taken into account.

As a consequence, D1.1 is a collection of information - in particular task, activities, documents - from the three domains, focused on the creation of a list of requirements for certification processes in each domain and then on the selection of those requirements useful for the OPENCOSS framework. The document reports what shall be done for obtaining a safe system in each domain, and how it could be done (also what artifact has to be produced during the different steps of the development process). Neither business aspects nor possible stakeholders involved are considered.
D2.1, on the other hand, provides a systematic analysis and formulation of the meaningful business models of the OPENCOSS platform across domains and captures the needs of different types of OPENCOSS stakeholders, including tool vendors, embedded systems developers, integrators, system and system of systems providers, certification entities, governmental agencies, regulatory bodies, and standards organizations. The intention is to aggregate the results over domains, starting with the three OPENCOSS domains individually.

This deliverable focuses on business models and stakeholders, and the value exchanges between them. These value exchanges are reported in detail for each of the stages in the e³-value model in Chapter 5. The model of each domain focus on the scenarios listed in Chapter 5, trying to detail values for stakeholders.

### 3.4.2 Relation within work package 2 (WP2)

This document, as it contains the business cases and user needs, will describe the drivers for the requirements and the architecture, which will be developed in tasks 2.2 and 2.3 respectively. The most influential elements in this document are the summary of the scope and vision of the OPENCOSS project, which form the boundaries for the requirements and architecture, and the focus that the business cases will present, which will inform the development of the requirements.

### 3.4.3 Relation with work packages 4 through 7 (WP4-WP7)

The business cases and user needs presented in this document establish the vision and scope for the technical work packages (4-7). They are also the source for the priorities of the requirements and design rules generated in these work packages. From the more technical implementation of work packages 4 to 7, Compositional Certification (WP5), evolutionary evidential chain (WP6), Transparent Certification and a Compliance-Aware Process (WP7), business cases and user needs can also be refined and updated.

Because of the preliminary nature of WPs 1, 2, and 3, and the dissemination or administrative nature of WPs 8, 9 (except D9.3 about exploitation), and 10, we will mainly consider WP 4, 5, 6, and 7 for relations with stakeholders.

In WP4, the common safety assessment metamodel (also known as the common certification language) will be developed. This metamodel is the language which will bind requirements, standards, evidence and argumentation. In WP5, the focus is on component based certification. WP6 addresses evolutionary certification. The transparent certification and compliance-aware process (WP7), has an important role in the remainder of the project. The better and more transparently structured the process, the easier it is to assess.

The Consumer stakeholder group relates to all WP’s, because the individual results from all of the work packages, and the sum of their parts will ultimately provide the consumer with a safer and cheaper product.
4 The general OPENCOSS business case

4.1 Introduction

The OPENCOSS project aims to provide a platform and community that is self-sustainable and aims at supporting the safety assessments required for certification or compliance assurance. The core activities of the community in terms of their reason for existence will be in information technology. Activities will be IT-enabled and used in an integrated fashion for both the processing and the communication of information. The platform and its community can, therefore, be considered as an e-business project; it conducts core business activities in a way that is enabled by the integrated use of information technology for processing and communication of information.

However, the context of the certification activities is still grounded in more conservative, safety-related, government-controlled environments. The assessment process and manufacture of safety-critical systems is embedded in a risk-avoiding culture, and therefore innovations are scrutinized in detail and held back if the consequences of their contribution is unsure or introduces new uncertainties. OPENCOSS provides the opportunity to try and demonstrate improvements and to create innovations that have been proven to increase the system’s safety and to speed up the safety assessment process. For that reason we have chosen to describe the business cases using a more general approach that can be applied to businesses other than those focussed on e-business.

Section 4.2 describes the e-business oriented BOAT framework and formulates the general OPENCOSS business case according to that framework. Because not everything is directly related to the e-business aspects, section 4.3 depicts a more general approach; the Business Model Canvas. It also describes the OPENCOSS general business case. Section 4.4 concludes with a description of the e³ value models, which in a sense form the organisational content for the BOAT framework.

4.2 BOAT framework

The BOAT framework and approach assists in developing new e-businesses by integrating several development stages into one spiral model. BOAT is an acronym consisting of the four consecutive development stages or aspects: Business aspect, Organisation aspect, Architecture aspect, and Technology aspect (BOAT). The framework supports working in cycles. After the last step (Technology), a next review round starts in order to demonstrate the impact of the previous choices and to increase the added value of the business proposition. Thus, the approach prescribes a continuous business development. If used rigorously, BOAT can support opening up completely new business opportunities and a big change in existing market value chains, especially in more conventional oriented markets. A more detailed description of BOAT can be found in Chapter 12.

In OPENCOSS we have already made a first iteration through business, organisation, architecture, and technology aspects. The OPENCOSS DoW [8] describes most of the aspects quite clearly from business goals, to architecture and technology solution directions. In this document we analyse the business to a more refined level, taking the existing definitions of the four aspects into account.

In the BOAT framework, the business is described in terms of parties, objects and time scope. There are three types of e-business parties: business party (B), consumer party (C) and government party (G). The business objects that can be exchanged between the partners can be categorised as physical goods, digital goods, services, financial goods and hybrid objects. Moreover, in the e-business collaboration scenarios, four types of time scope are represented: static, semi-dynamic, dynamic and ultra-dynamic.
To apply the BOAT framework in OPENCOSS, we begin with the business aspect. This describes the business goals of OPENCOSS in terms of business drivers, reorganization in business chains, business directions and business structures.

There are a number of concepts in which the business aspect is described:

- **Drivers**: mainly include reach and richness.
- **Chains**: mainly include disintermediation and reintermediation.
- **Directions**: used to conduct business from the viewpoint of one party.
- **Structures**: used to organize the collaboration of parties in a scenario.
- **Model**: summarizes the observations made on the different items of the business aspect.

The last step of the business aspect is to build the BOAT business model for OPENCOSS. In Table 1 the concepts for BOAT, like parties included, objects, etc., are listed in the first column. The second column describes the categories, like B2G – business to government – for the parties concept. If necessary, a number of additional explanations are added in the last column, called details. A more elaborate description of the BOAT concepts can be found in Appendix 12.

### Table 1: OPENCOSS’ BOAT Business model

<table>
<thead>
<tr>
<th>Business model: OPENCOSS platform</th>
<th>Categories</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concepts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parties</td>
<td>B2B, B2G</td>
<td>G2B is also possible</td>
</tr>
<tr>
<td>Objects</td>
<td>Digital goods</td>
<td>Safety case, arguments, evidence</td>
</tr>
<tr>
<td>Time scope</td>
<td>Static/semi-dynamic</td>
<td></td>
</tr>
<tr>
<td><strong>Drivers</strong></td>
<td>Increasing reach</td>
<td>More companies will be able to certify their safety critical systems and stored and reusable safety cases will enrich the relationships and result in repeat sales.</td>
</tr>
<tr>
<td></td>
<td>Increasing richness</td>
<td></td>
</tr>
<tr>
<td><strong>Chains</strong></td>
<td>By reintermediation enabling disintermediation</td>
<td>Unification of safety cases and enabling reuse allows for skipping (part of) the certification of already assessed (complete/sub)systems.</td>
</tr>
<tr>
<td><strong>Directions</strong></td>
<td>Time compressed business</td>
<td>Time advantage through reuse of safety cases. Increased safety is a second important direction.</td>
</tr>
<tr>
<td>Structure</td>
<td>Uniform and reusable safety cases.</td>
<td></td>
</tr>
</tbody>
</table>

The organization aspect describes how organizations are structured and connected to achieve business goals. It includes business processes and business functions. Since the e³ value models describe the actors and their value exchange, and, with that, the functions and processes involved in the OPENCOSS business, this forms an excellent description of the organisational aspect of BOAT. The organisational aspect of OPENCOSS is sufficiently covered in the e³ Value Models in 4.4.

The architecture aspect covers the conceptual structure of automated information systems used to enable organisational structures. It includes information system structures between organizations and within organizations. The architecture aspect will be fully covered in deliverable D2.3: Design of the OPENCOSS platform architecture.

The technology aspect describes the technological realization of the systems of with architectural structures. The technology aspect describes software, languages, communication protocols, and hardware.
This subject is covered in the implementation of work packages 4 to 7, dealing with the common safety assessment metamodel (in WP4, also known as the common certification language), Compositional Certification (WP5), evolutionary evidential chain (WP6), and the Transparent Certification and Compliance-Aware Process (WP7).

The business model canvas (from the business model generation) describes the overall context of the business case in the next section, Section 4.3.

4.3 The Business Model Canvas

The Business Model Canvas is a strategic management template for developing new business models or documenting existing ones. In addition to the BOAT framework, the Business Model Canvas (the Canvas in short) includes the value proposition, cost structure, and revenue streams. Together with the BOAT framework and e³ value models, the canvas covers all business aspects and the details to analyse the business case. The Canvas summarizes these results in one overview.

In other words, the Canvas is a visual chart with elements describing a firm's value proposition, infrastructure, customers, and finances. It assists firms in aligning their activities by illustrating potential trade-offs. It helps analysts to discuss, organize, design and invent a new business model by describing it in 9 basic business blocks: customer segments, value proposition, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, cost structure. The details of these building blocks are described in Chapter 13.

With the business model canvas, the OPENCOSS business model can be managed just in one image. Using the Canvas to design or develop a business model, each block can be clarified by the following steps:

1. Customer segments: defines all the people and organizations for which OPENCOSS wants to create value.
2. Specific value propositions: describes the various products/objects and services that create value for the customer segments.
3. Channels: describes how OPENCOSS intends to deliver value to its customers.
4. Customer relationships: the types of relationships established with the customers should be outlined in the customer relationships block.
5. Revenue streams: its purpose is to make clear how the business model captures the value.
6. Key resources and key activities: The key resources show indispensable assets in the business model, while the key activities represent which things are needed to help OPENCOSS perform well.
7. Key partners: the people who will provide the knowledge, basic functionality, social networks, for the OPENCOSS platform to run smoothly.
8. Cost structure: describes the most important monetary consequences while operating under different business models.
Figure 1 shows general Business Model Canvas for OPENCOSS. The canvas for each domain will be provided in Section 5.3 through 5.5.

**Figure 1: The Business Model Canvas for OPENCOSS**

### 4.4 e³ Value Models

#### 4.4.1 Introduction

There is a risk that constructing the business cases might remain as a theoretical exercise if there is no connection to the real added value of the new business. Failing to produce a realistic estimate of the added value, could result in a sudden end of the new venture. For this reason we have included the e³ value model to create a better understanding and estimate of the added value of the OPENCOSS platform in the years after the OPENCOSS project has ended.

In a market of safety and trust, it is impractical to give an estimate of the numerous intangibles. Examples of such intangible values being exchanged in a safety market business case could be: Safety Measures (issued by Governments), Votes (issued by Consumers for Governments), Safety Hazard Reports (issued by Component Manufacturer). They are exchanged in a complex environment, between various stakeholders, hence trying to quantify each value and calculate the overall gains would be very far from precise.

This section therefore describes the value exchange between stakeholder, both tangible and intangible, but will not include an estimate of the value in money. For the numbers we rely on the fact that the OPENCOSS goals will be achieved. Demonstration of the economic viability of the OPENCOSS platform will presently rely on the cost reduction and the face-validity of the e³ value models.
4.4.2 Methodology

The e³ value methodology helps you to explore your innovative e-business idea - starting from understanding which enterprises and actors are actually involved, to an assessment of profitability for each enterprise [1]. Other models are not as rich or focussed on business value as the e³ value model, since they either miss the crucial information required to give a complete picture on a business case level, or they have to include too many details, which makes things more complicated or insecure because of a great number of assumptions need to be made.

As a methodology, e³ value is a graphical approach: you can create your business idea using a number of pre-defined visual elements. Furthermore, e³ value modelling explicitly recognizes that most e-businesses are networks of enterprises. Typically, you develop your e-business idea as an e³ value model in a short timeframe; the methodology has been developed to be tractable and lightweight.

![Figure 2: Simple example e3 value model (from [1])](image)

Figure 2 displays a simple e³ value model showing the value exchange between a customer and a supplier, where the customer pays money in order to get a good. Note that the Customer has the start node (single circle) because he/she takes the initiative in the value exchange. The Supplier is responding to this initiative and because at this level we are not interested in the details of delivering the goods, the activities are represented in an end node (double circle).

In appendix B the steps for constructing a correct e³ value model are provided.

4.4.3 Example e³ value model in the safety assessment context

Based on the context provided by the BOAT framework and the Business Model Canvas, we have already identified the process context, the stakeholders, the goals and the added value. Figure 3 depicts an overview of the cross-domain e³ value model of the field of safety assessment. It shows the current value exchange starting from the Transport Consumer to the Vehicle Manufacturers, Component Suppliers, Tool vendors, and the Safety Assessors, and last but not least, the OPENCOSS Consortium. Each block represents a (group of) stakeholder(s) in the value chain. Each stakeholder has a value interface and communicates with the outside world by means of value exchanges. The line between start and end, is the value chain and can continue through each stakeholder. Within each stakeholder, the value chain can fork or join. The square around the stakeholders shows the focus of the OPENCOSS project. Each block represents a (group of) stakeholder(s) in the value chain. Each stakeholder has a value interface and communicates with the outside world by means of value exchanges. The line between start and end, is the value chain and can continue through each stakeholder. Within each stakeholder, the value chain can fork or join. The square around the stakeholders shows the focus of the OPENCOSS project. Note that, at this moment in the OPENCOSS project, the OPENCOSS consortium and platform do not provide a direct added-value to the safety assessment stakeholders. However, in the next chapters, this document will describe the future situation, where the OPENCOSS platform will generate such value to the stakeholders.
Figure 3: Example of a general $e^3$ value model of the safety assessment field

$e^3$ value models for each of the domains specifically will be provided in Section 5.3 through 5.5.
5 Domain related OPENCOSS Business Cases

5.1 Introduction

In order to maximize the added value for the OPENCOSS platform, in this chapter we model the domain-related business cases for the OPENCOSS platform. We describe our approach in Section 5.2, identify the most interesting business cases per domain in Section 5.3, 5.4, and 5.5, and conclude with an aggregated, cross domain observation in section 5.6. We describe the complete context in terms of a highly aggregated safety assessment process and the business modelling approaches as described in the chapter above: the BOAT framework, the Business Canvas Model, and the e³ value models.

5.2 Approach

To understand the OPENCOSS business better, more specifically, to understand the safety assessment process, we have interviewed a number of stakeholders, manufacturers to be precise, in the various domains of the OPENCOSS partners. A summary of the semi-structured open interviews with these manufacturers is available within the OPENCOSS project D2.1 repository.

Based on these interviews, we have constructed a number of highly aggregated BPMN (Business Process Model Notation) models, verified them with the interviewed stakeholders and identified a number of business cases for these domains. BPMN is a standard language for business process modelling; it provides a graphical notation for specifying business processes in a Business Process Diagram (BPD), based on a flowcharting technique. The presented BPMN models do not follow the actual complex process model. The business processes are represented in brief way by using the abstraction. With the aim of a unification attempt, these BPMN models compromise between finding similarities with other domains and describing an aggregated truth. Meanwhile, after a deeper analysis, we have been able to construct the Business Model Canvas per domain, and constructed a number of e³ value models for further analysis of the value proposition of the OPENCOSS platform in the designated domain.
5.3 Avionics domain

The highly aggregated safety assessment process for avionics is depicted in Figure 4. Note that it also includes the system development process because that is closely interlinked with the safety assessments; for example, the safety requirements are coming from safety standards and have a direct influence on the product, while the evidence for demonstrating safety are based on the test results of the product. This makes it impossible to look at the safety assessment without considering the development process.

Another important aspect is included in the overall safety assessment process: the process of the component supplier. One of the goals stated in Section 3.3 (Mission and objectives) is to reduce the recurring safety assessment efforts for component safety assurance (which forms a part of the system safety assessment or certification). As such it is important to know how the process of the component supplier is interwoven in the total system safety assessment process.

In avionics there are three levels of development and construction activities: the platform or aircraft level, the system level, and the item or component level. Platforms are created by aircraft or rotorcraft manufacturers, components by equipment or component providers. Certification only happens at these two levels: the platform or aircraft level and the physical component level. Avionic systems are not yet certified as standalone systems, even though progress is made in this direction with IMA (Integrated Modular Avionics) certifications.

Figure 4 does not explicitly include the avionics system manufacturers. Implicitly this supplier is integrated it the process of the aircraft manufacturer, represented by the original equipment manufacturer (OEM), or the system supplier could be seen as a component supplier, but the system safety certification process step does not exist, yet.

For reasons of aggregation and formulating an initial cross domain understanding of the safety assessment process, Figure 4 uses terms that are equivalent to the terms used in avionics, but are not necessarily the exact ones used in this domain. The items indicated with the grey/blue colour are, however, avionics domain specific.
Figure 4: Safety assessment business process for the avionics domain

For avionics EASA is the European Authority to hand out Type Certificates (TC), certifications that assure the safety of the aircrafts. Other airworthiness authorities (AAs) allow TC validation for certifying airplanes on other parts of the world like the CAAC for China, IAC-AR for Russia, or issues their own based on the TC like the FAA for the USA. For certification there are 4 Airworthiness Authority Stage of Involvements (SOI1-4) during the development process. These audits are performed at aircraft level, system level, and item level (including software and hardware). Certificates are handed out only for aircrafts and for equipment (item level), not for the intermediate avionics system level between aircraft and components. The main standards are the CS 25 (European requirements for larger aircrafts), ARP4754A/ED-79A (development of civil aircraft and systems), ARP4761 (safety assessment process on civil airborne systems and equipment), DO-178B/ED-12B (software considerations in airborne systems and equipment), DO-160D/ED-14D (environmental conditions and test procedures for airborne equipment), DO-254/ED-80 (design assurance guidance for airborne electronic hardware) and DO-297/ED 124 (Integrated Modular Avionics (IMA) development)

Based on the semi-structured interviews mentioned in Section 5.2, a number of generalized avionic business cases are formulated; these are issues in the avionics domain that are targeted by the OPENCOSS project and, if resolved, probably have a high added value in the avionics. The term generalized refers to the fact that these business cases are formulated in such a way that they can be applied to other domains as well:

- **Unification and update** of the process and requirements. In the fine-tuning between manufacturers and certification bodies, much time is investigated to find a common understanding of the terms, the approach that will be followed, how the requirements are tailored in the specific application domain and even specific aircraft, and detailed in the system specifications. This can be improved.
  
  *Impact: faster process and better safety;*
• Better view on verification and validation data and traceability. Data supporting the safety assessments is often detailed, complex, and hard to get an overview of. Impact: more effective assessment process;

• For Avionics Component Suppliers and System Manufacturers: Avoid complete recertification or reassessment of suppliers’ multi-function subsystems. It should not be mandatory to reassess subsystems if multiple functions are integrated into one item or when the system is reassessed for another domain. Through the IMA it may be possible to achieve this even faster. Impact: 50% to 90% cost reduction.

The generalized avionic business cases are further detailed in the following section.

5.3.1 Business cases: Avionics domain

In the avionics domain, three business cases were identified and are elaborated below. First of all we have filled in the building blocks from the Business Model Canvas with the relevant OPENCOSS information for this domain in Figure 5. In Table 2 similar results are listed for OPENCOSS in the context of the BOAT framework. In the next sections we describe the e³ value models for the identified business cases.

![Business Model Canvas for avionics](image)

**Figure 5: The Business Model Canvas for avionics**

**Table 2: OPENCOSS’ BOAT Business model for avionics**

<table>
<thead>
<tr>
<th>Business model: OPENCOSS platform in avionics</th>
<th>Concepts Categories</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties</td>
<td>B2B, B2G</td>
<td>G2B is also possible</td>
</tr>
<tr>
<td>Time scope</td>
<td>Static/semi-dynamic</td>
<td></td>
</tr>
</tbody>
</table>
### Business model: OPENCOSS platform in avionics

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Categories</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drivers</td>
<td>Increasing reach</td>
<td>More companies, especially avionics system manufacturers, will be able to certify their safety critical systems. Stored and reusable safety cases will be better understood by stakeholders, and enrich the relationships and results in repeat sales.</td>
</tr>
<tr>
<td></td>
<td>Increasing richness</td>
<td></td>
</tr>
<tr>
<td>Chains</td>
<td>By reintermediation</td>
<td>An added unification step in safety cases and enabling reuse allows for skipping (part of) the certification of already assessed (complete/sub) systems.</td>
</tr>
<tr>
<td></td>
<td>enabling disintermediation</td>
<td></td>
</tr>
<tr>
<td>Directions</td>
<td>Time compressed business</td>
<td>Time advantage through reuse of safety cases. Increased safety is a second important direction.</td>
</tr>
<tr>
<td>Structure</td>
<td>Uniform and reusable safety</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cases.</td>
<td></td>
</tr>
</tbody>
</table>

The stakeholders in this process are described in Section 6.2.1, for more information about their goals and needs, we refer to this section.

### 5.3.1.1 Unification and update of the process and requirements

For every aircraft type, each airworthiness authority has its own set of requirements, standards, and processes to be followed. Because of differences between the evidence and analysis required in each jurisdiction, reuse of components and streamlining of the certification process becomes difficult. If the OPENCOSS platform can help in the unification of terms, standards, requirements, and processes, reusing components can be increased and the time to certify can be decreased.

There are two ways in which the unification can help. First, by applying a unified certification dossier, where there is a time gain because there is no discussion about the form in which the analysis and evidence is presented, thus assessors and manufacturers can focus on the contents (See Figure 6). The OPENCOSS Community will provide the OPENCOSS users (industrial companies) with a platform assisting them to build homogeneous certification dossiers. Exchanges with airworthiness authorities regarding the development of certified products together with lessons learnt received from the OPENCOSS users will enable the OPENCOSS Community to improve the OPENCOSS platform.
Figure 6: Unification of the certification dossier by introducing the OPENCOSS platform/community
The second advantage in the avionics domain is the fact that lobby groups or working groups will have a better framework to enable them to reach to a common understanding of matters relating to safety assessment. These working groups aim to improve the standards from the industrial point of view, in close co-operation with the standards organizations and the industrial partners. Figure 7 depicts the e³ value model for smoothing cooperation between stakeholders by the introduction of the OPENCOSS platform. The OPENCOSS Community will provide the OPENCOSS users (industrial companies) with a common platform, leading them to share concepts, terms and practices. This will facilitate a growing consensus in working groups mandated by standards organisations, involving in particular the OPENCOSS partners and airworthiness authorities. The OPENCOSS Community will in turn upgrade the OPENCOSS platform to keep it up to date with the improved standards.

Figure 7: Unification for working group improvement by introducing the OPENCOSS platform/community
5.3.1.2 Better view on verification and validation data, and traceability

A commonly-cited myth in avionics is that the certification authorities seem to have an implicit requirement that the weight of the supporting certification documentation should exceed the weight of the aircraft in order to be certified. Joking apart, it is worth noting that handling the large amounts of data required for the assurance process is hard. Managing the traceability between documents is even harder. Maintaining and checking the traceability through the whole chain from aircraft requirement level to equipment-implementation level is, however, a tedious and ill-supported job that has a highly manual character. The OPENCOSS platform can support the handling of verification and validation data in such a way that the airworthiness certification assessment becomes faster and easier. Note that traceability is already a hard safety requirement in the avionics domain. Also note that the support may only include a standard prescribing the traceability format.

Figure 8 depicts the e3 value model for this situation. The OPENCOSS platform is assumed to be used by all industrial stakeholders and is not depicted explicitly in the model. The OPENCOSS users (industrial companies) will be supported by the OPENCOSS platform to trace requirements and evidences at various levels, in order to provide the airworthiness authorities with comprehensive certification dossiers. The contents handled by the OPENCOSS platform are still to be determined (e.g. full actual industrial data versus traceability labels and links only).

Figure 8: Improved insight in data through traceability overview
5.3.1.3 Avoid complete recertification of suppliers’ multi-function subsystems

When changes are made to a certified aircraft, the recertification is done on the entire aircraft again. Before the introduction of Integrated Modular Avionics (IMA), it was very difficult to consider just a subsystem. A current trend is to go from “one function per box” to multi-function subsystems. Because of this trend, the need for modular certification becomes even greater. The IMA approach was elaborated to meet this need. If the OPENCOSS platform can support modular certification and the need for complete recertification is not necessary for every change, the time and effort that is saved, can be significant. Figure 9 depicts the $e^3$ value model. Also here, the OPENCOSS platform is included implicitly; stakeholders make use of it in their value exchange. The OPENCOSS platform will help OPENCOSS users (industrial companies) obtain incremental acceptance for new or modified applications or modules, without the need for re-acceptance of existing unmodified applications and modules. This accumulation of credit toward approval of the avionics system contributes to the recertification of the aircraft.

Figure 9: Reuse of certification dossier
5.4 Railway domain

The highly aggregated safety assessment process for railway is depicted in Figure 10. The same structure as in the avionics domain in Figure 4 is used, describing both the safety assessment as well as the system development process, and the component supplier process is detailed as well. Additions to the safety assessment business process for the railway domain are indicated in this figure.

For reasons of aggregation and formulating an initial cross domain understanding of the safety assessment process, Figure 10 uses terms that are equivalent to the terms used in railway, but are not necessarily the exact ones used in this domain. The items indicated with the grey/blue colour are, however, railway domain specific.

**Figure 10: Safety assessment business process for the railway domain**

ERA is the European Railway Agency specifying standards and regulating relations between National Railway Authorities. Each National Safety Authority has its own set of additional rules. National Safety Authorities (Proposer) appoint Independent Safety Assessors. The main and most highly-evolved standards in this domain are: CENELEC EN 50126, EN 50128, and EN 50129 (resp. life cycle, software, and systems railway standard).

Based on the semi-structured interviews a number of generalized railway business cases are formulated; these are issues in the railway domain that are targeted by the OPENCOSS project and, if resolved, probably have a high added value in this domain. The term generalized refers to the fact that these business cases are formulated in such a way that they can be applied to other domains as well:

1. **Delta-assessment** offers a competitive knowledge advantage for assessors. Being able to reuse the safety case of a previous version or similar product, offers a major time and effort reduction on safety assessments, especially when the re-assessment is done by a different assessors. These so-called delta assessments require a lot of effort at this moment. Being able to avoid this kind or
work will increase the competitive advantage significantly.  
*Impact: lower costs, competitive advantage.*

2. Use of the OPENCOSS Platform will mean that recertification is not necessary or is only partially necessary when manufacturers produce identical products for another country.  
*Impact: when entering a new market, there is 50% chance that the product is not compliant with additional rules and a 20-30% chance that the product needs to be reconstructed and, therefore, needs a reassessment. Possible cost reduction: costs of 1 or 2 complete certification assessments per target country;*

3. Use of the OPENCOSS Platform will mean that the developer has a better view of the relationship between requirements and system specification and implementation (e.g. with formal methods like Event-B, a formal language based on set theory which is used in the Rodin project. Event-B is used to formalize the requirement of a system in order to prove mathematically some properties of the system specification.)  
*Impact: better safety, faster process;*

The generalized railway business cases are further detailed in the following section.

### 5.4.1 Business cases: Railway domain

In the railway domain, three business cases were identified and are elaborated below. First of all, we sketch the building blocks from the Business Model Canvas for this domain in Figure 11. In Table 3 are the results for the BOAT framework. In the next sections we describe the e³ value models for the identified business cases.
Table 3: OPENCOSS’ BOAT Business model for railway

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Categories</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties</td>
<td>B2B, B2G</td>
<td>G2B is also possible</td>
</tr>
<tr>
<td>Objects</td>
<td>Digital goods</td>
<td>Certificates, safety cases, arguments, evidence</td>
</tr>
<tr>
<td>Time scope</td>
<td>Static/semi-dynamic/dynamic</td>
<td>More companies will be able to afford a certification of their safety critical system, despite the fact that they need an ISA for the assessment. Stored and reusable safety cases will be better understood by stakeholders, and enrich the relationships and results in repeat sales.</td>
</tr>
<tr>
<td>Drivers</td>
<td>Increasing reach</td>
<td>An added unification step in safety cases and enabling reuse allows for skipping (part of) the certification of already assessed (complete/sub)systems.</td>
</tr>
<tr>
<td></td>
<td>Increasing richness</td>
<td></td>
</tr>
<tr>
<td>Chains</td>
<td>By reintermediation enabling disintermediation</td>
<td>Time advantage through reuse of safety cases. Increased safety.</td>
</tr>
<tr>
<td>Directions</td>
<td>Time compressed business</td>
<td>Time advantage through reuse of safety cases. Increased safety.</td>
</tr>
<tr>
<td>Structure</td>
<td>Uniform and reusable safety information (dossiers, evidence, patterns).</td>
<td>The stakeholders in this process are described in Section 6.2.2, for more information about their goals and needs, we refer to this section.</td>
</tr>
</tbody>
</table>

5.4.1.1 Delta-assessment offers a competitive knowledge advantage for assessors

5.4.1.1.1 Summary of key idea

From the assessor’s point of view, an assessment is an activity to be performed from scratch, unless it is a modification of a product already considered by the same assessment body. Assessors need to repeat many assessment activities for products of the same type from different manufacturers because of differences in the ways in which similar safety principles and measures are described. This results in increase in cost overheads. Also, in the event of the introduction of new functions/changes in a certified product, there is a need for re-assessment of the product as a whole, especially if the first certification was released by another (Independent) Safety Assessor (ISA), because of the difficulty of identifying the activities, procedures and methodologies used by the other Safety Assessor. Use of a standard assessment language should simplify communication and technical discussions between manufacturers and assessors (because they talk the same language).

The business scenario provided here aims at highlighting the critical situations that Safety Assessors have to deal with in their job. First of all, we can consider the case of a system (assessment performed by Independent Safety Assessor 1) containing two sub-systems (sub-system 1 and sub-system 2), respectively certified by the original assessor ISA1 and Independent Safety Assessor 2 (ISA2). This first small scenario
allows us to draw attention to the exchange of information between the assessor of the entire system (ISA1) and the Safety Assessors of the sub-systems (ISA1 and ISA2). This is a potentially critical legal situation: without the presence of a mutual recognition agreement among Assessors, ISA1 is responsible for the certification of the entire system, although some malfunctions may be traced back to the assessment performed by ISA2.

Another goal of the described scenario is to emphasize what happens whenever an upgrade of a sub-system is required. In order to describe this, we can consider what happens when a sub-system (e.g. sub-system 2) is upgraded and the delta-assessment is committed to a third Independent Safety Assessor (ISA3) different from the one who was in charge of assessing the original sub-system 2.

The two critical situations described above obviously have an impact on the costs of assessment activities, on their correct estimation and on the share of knowledge among assessors.

5.4.1.1.2 Stakeholders and their goals
It is important to identify the stakeholders in the scenario and their responsibilities, roles and goals. Actors in the scenario are:

- Ministry of Infrastructure and Transport
- National Safety Authority
- Independent Safety Assessor
- Infrastructure Manager
- Railway undertaking
- Railway Transport Consumer
- System and subsystem manufacturer
- Safety assurance tool vendor
- Safety consultant

For details on these we refer to Section 6.2.2.

5.4.1.1.3 Context and scope
The business context of the described scenario relates to the certification of railway systems, sub-systems and components by different ISAs. The organization described in the scenario is quite new, especially with regards to the establishment of the National Safety Authority (implementation of the EU Directive n.2004/49/EC). However, the roles, responsibilities and required competencies of several “actors” in the scenario are typically well-established and based on standardized procedures and methodologies coming from experts of the sector. In the light of these considerations, we can describe it as a quite mature market. Despite the presence of several regulations and requirements to be met in this domain, until now mutual recognition agreement among Assessors has been missing. This means that there is a potential for misunderstandings in the delta-assessment of any component undergoing an upgrade and also a need for time-consuming activities to be performed before its certification.

With respect to the technical context, the railway domain in general relies on well-established safety standards and procedures that are undergoing a steady refinement process and are used as a reference by all stakeholders in this sector. The assessment process is based on test reports and other text documents, written on the basis of test results and other evidence.

The scenario describes the main actors in the railway domain at a national level, for freight and passenger transport. In particular, the proposed business case is aimed at underlining the bottlenecks in the assessment of a system made up of sub-systems assessed by different Safety Assessors and at focusing the
attention on the critical aspects resulting from an upgrade of one sub-system whose safety assessment is assigned to a Safety Assessor different from the one assessing the original system.

The scenario is presented from the point of view of a Safety Assessor. Therefore, safety requirements, safety application conditions and so on represent an important part of the added value exchanged among the actors in the scenario. The scenario does not describe possible outsourcing of activities, which might be a feature of the real world (i.e. maintenance for infrastructure manager or railway undertaking).

Important pre-conditions for scenario are:
- appropriate safety standards must be followed;
- appropriate quality standards must be followed;
- appropriate documentation must be available for every aspect of the scenario;
- shared knowledge about failure modes of system/sub-system of railway application must exist within the domain;
- there must exist an appropriate management system for the maintenance, use of railway infrastructure, rolling stock and every sub-system involved;
- there must be appropriate procedures to govern the Independent Safety Assessor’s activities.

Even though this is not modelled in the e³ value model, it should be noted that it is not the role of the (Independent) Safety Assessor to give National safety approval of the system and sub-systems. This is the responsibility of the National Safety Authority, on the basis of the safety assessment report (and possible certificates) issued by the Safety Assessor and other technical considerations.

5.4.1.1.4 Technology infrastructure
The scenario requires the following technological infrastructure; a shared repository containing information about:
- certification activities regarding the product assessed by another assessor;
- Safety regulations/standards applicable to the product;

Important aspects of this repository should be:
- The repository should contain adequately detailed/documented information about assessment activities, so that they can be used by another assessor when required;
- The repository should be accessible to assessors and operators who need this information;
- The repository should maintain the integrity of information (no one shall modify information from another source);
- Every source of information shall be authenticated and verified (comparable with a financial transaction);
- Information shall be signed (i.e. qualified electronic signature);
- It shall be possible to define different user types, with different scope of visibility, for confidentiality reasons.

5.4.1.1.5 Interaction and communication
Further script information is provided in the form of UML sequences. This shows some info about dynamics, interaction and control flows.
Figure 12: assessment of a system made up of two sub-systems, each assigned to a specific ISA

In this sequence diagram, it is demonstrated that the responsibility of the NSA to certify any system/sub-system on the basis of the test report and other technical considerations coming from ISAs.
The aim of this sequence diagram is to describe the sequence of “events” in case of delta-assessment due to the request of an upgrade to sub-system 2 coming from the system manufacturer. In particular, this sequence diagram highlights that it is the responsibility of the National Safety Authority to certify the sub-systems and the entire system as safe.

5.4.1.1.6 Value model and scenario

The value model describes the value exchanges between the actors. An e³ value model for the delta assessment context is depicted in Figure 14.
The aim of this section is to briefly describe the business context related to delta-assessment in the railway scenario. The e³ value model of the context is depicted in Figure 14.

Going through the e³ value model clockwise, starting at the top right, the first actors we encounter are the “Ministry of Infrastructure and Transport” and the “National Safety Authority”. In particular, the “Ministry of Infrastructure and Transport” sets-up an independent body, the “National Safety Authority”, for the purpose of assuring safety. In case of an accident and/or a dangerous inconvenience, the Ministry of Infrastructure and Transport investigates and consequently provides recommendations for the increase of the railway safety and for the future prevention of similar accidents.

The “National Safety Authority” accredits the “Safety Assessors” as long as they demonstrate the ability to perform an evaluation of components and/or applications of railway system(s) compliant with specific procedures/methodologies/specification with the due competence and independence, free of economic constraints, cultural/intellectual prejudice and any other kind of implication that may reduce their objectivity.

Figure 14: Delta-assessment e³ value model
A Safety Assessor is paid for assessing a system/sub-system and providing a safety report (and, where needed, a certificate), that will be used as a basis by the National Safety Authority in order to declare the system as safe in its intended context-of-use. The assessment typically requires the manufacturer to provide the Safety Assessor with the evidence of Safety and V&V activities (test reports, safety and risk analyses, etc.) as required to demonstrate the safety of the system/subsystem.

The “System/Sub-system Manufacturer” can co-operate with “Safety Consultant(s)” and/or “Safety Assurance Tool Vendor(s)”.

In particular, the “Safety Consultant” is paid by the System/Sub-system Manufacturer to provide technical solutions, design suggestions and expertise. The Safety Assurance Tool Vendor, on the other hand, is paid to provide tools for design, testing, configuration management, etc.. Some of these tools can be safety-related.

A safety-related sub-system has to be assessed (and, where requested, certified) by a Safety Assessor (depending on its complexity and functional completeness, the sub-system can undergo the safety acceptance of the National Safety Authority that, on the basis of the Safety Assessment Report, declares it safe to be used in the National railway network (under given safety-related safety conditions)). The sub-system manufacturer can sell it to a System Manufacturer for inclusion within a wider system. The System Manufacturer shall appoint a Safety Assessor for assessing the system and issuing a safety report (and, where requested, a certificate). The System shall undergo the safety acceptance of the National Safety Authority that, on the basis of the Safety Assessment Report, declares it safe to be used in the National railway network (under given safety-related safety conditions)).

The scenario described can be useful to understand what happens in the case of a system (with assessment performed by the Safety Assessor ISA1) containing two sub-systems (sub-system 1 and sub-system 2), respectively certified by two Safety Assessors, ISA1 and ISA2, and in particular to focus the attention on the exchange of information between the Assessor of the entire system (ISA1) and the Safety Assessors of the sub-systems. Without the presence of a mutual recognition agreement among Assessors, ISA1 is responsible for the certification of the entire system, although some malfunctions may be traced back to the assessment performed by ISA2: this represents a critical situation from a legal point of view. Another interesting case to consider is the upgrade of any sub-system. For example, we can consider what happens when a sub-system (e.g. sub-system 2) is upgraded and the delta-assessment is committed to a Safety Assessor different from the one that was in charge of assessing the original sub-system 2.

In any of the two situations described above, the system manufacturer is then paid by the infrastructure manager or by the railway undertaking to sell its system certified as safe (with safety-related safety conditions).

In addition to this, the railway undertaking pays the infrastructure manager to maintain the infrastructure as safe. Moreover, the railway undertaking has to demonstrate compliance to the operational safety requirements provided by the National Safety Authority.

Finally, the railway transport consumer pays the railway undertaking for a safe transportation.

5.4.1.1.7 Cost considerations

In the proposed scenario, the cost related to technical consultants is not negligible. Since we are dealing with safety-related applications and, at the same time, innovative technical solutions to reduce time-to-market, it is natural to take advantage of experts. This cost is mainly applicable to system/sub-system manufactures and to Independent Safety Assessors. Another cost is related to the management of
standards and official procedures. This cost is mainly applicable to Independent Safety Assessors, because of the necessity of tracking all changes to the reference standards to be used to perform assessments. From the perspective of the manufacturers, the use of software tools for the management of requirements and for the establishment of repositories is becoming increasingly widespread (applicable also to ISAs).

Finally, every sub-system/system manufacturer – and indeed several of the other actors in the scenario - invests a percentage of its revenue in Research and Development.

5.4.1.8 Success measure
A business case is successful if it meets its objective(s) and if it is economically viable. Technology acceptance, for instance, or fault-free technical functioning of the necessary hardware are important prerequisite for a business case success. The ‘degree’ of success is reflected by meeting the qualitative or quantitative targets set beforehand.

This business case will demonstrate the success of the OPENCOSS Platform, if:

- Assessment from Independent Safety Assessors is reusable;
- Assessment procedure is clear and available to other assessors (assessor interoperability);
- The test report is available and written/compiled in a way shared among assessors (minimal set of information agreed among assessors)
- The time required for delta-assessment not comparable to the one necessary for the assessment of the entire system from scratch.
5.4.1.2 Avoid complete recertification for products entering another country market

For the following business cases we only describe the e³ value model, since it demonstrates the added value of the OPENCOSS platform and community sufficiently. In these models we explicitly depict the OPENCOSS platform and community as an actor, pinpointing its role and value exchanges in the context of the business case.

Because of different standards, different interpretation of standards and political concerns, it is hard to reuse the result of certification in a different country. On many occasions, adjustments need to be made or even complete recertification is in order to be able for a product to enter another country. The OPENCOSS platform can help in unifying the different standards and interpretations to streamline the certification for entering other countries, hence saving money and time. The e³ value model is depicted in Figure 15.

Figure 15: Avoid complete recertification for products entering another country market.
5.4.1.3 Better view on relation between requirements and system

Handling many requirements and other sorts of data such as test reports, design and architecture is a daunting job. The traceability between these elements is even harder. By offering a structured way of working with artefacts and traceability relations, the OPENCOSS platform can reduce the errors made in working with these large volumes and hence improve the quality of the products. The \( e^3 \) value model is depicted in Figure 16.

![Diagram of the \( e^3 \) value model]

---

**Figure 16: \( e^3 \) Value Model on Better view on relation between requirements and system**
5.5 Automotive domain

The highly aggregated safety assessment process for automotive is depicted in Figure 17. The same structure as in the avionics domain in Figure 4 is used, describing both the safety assessment as well as the system development process, and the component supplier process is detailed as well. Additions to the safety assessment business process for the automotive domain are indicated in this figure.

For reasons of aggregation and formulating an initial cross domain understanding of the safety assessment process, Figure 17 uses terms that are equivalent to the terms used in automotive, but are not necessarily the exact ones used in this domain. The items indicated with the grey/blue colour are, however, automotive domain specific.

The key difference between this automotive model and the processes in the other domains are that the automotive domain is characterised by the absence of national and international regulators or certification authorities for system safety. Whilst the services of reviewers (such as Independent Safety Assessors (ISAs)) are often used by the vehicle manufacturers (OEMs) and component suppliers, they are always engaged on a commercial rather than quasi-regulatory basis; reviewing practices and exact roles of reviewers vary between different countries and even different vehicle manufacturers’ supply chains.

![Figure 17: Safety assessment business process for the automotive domain](image)

In terms of system safety engineering and assurance standards the current standard for the automotive domain is ISO 26262. Published in late 2011, this standard is a domain-specific adaptation of the generic IEC 61508 standard (that was previously regarded as prevailing standard within the automotive sector). However, ISO26262 introduces significant new information, processes and refinements of the requirements as compared to its ‘parent’ document. Consequently, migration to the new standard regime is a non-trivial challenge faced by the automotive industry. Further common approaches and frameworks of working with respect to system safety engineering and assurance have emerged as a result of various
co-operation initiatives between automotive manufacturers (for example VSC, HIS, CE4A, ELVS, EUCAR, AUTOSAR, etc.).

Overall, it should be noted that industrial system safety assurance practices are less well established in the automotive sector as compared to avionics and railway domains discussed previously. This can be largely attributed to the extremely short period of time that has passed from publication of the automotive standard (ISO 26262 mentioned above). The automotive industry is currently investing significant resources into establishing frameworks for implementing requirements of- and demonstrating conformance with ISO 26262. As a consequence, two of the generalised business cases for OPENCOSS platform relate to the provision of support for these endeavours. The need to provide support for what could be seen in other domains as “baseline” or “core” safety assurance activities may be a challenge for the OPENCOSS project. However, it also represents a significant market opportunity for the OPENCOSS platform in the automotive sector where there is currently lack of tools that facilitate comprehensive management and demonstration of conformance to the standard.

Based on the semi-structured interviews a number of generalized automotive business cases are formulated; these are issues in the automotive domain that are targeted by the OPENCOSS project and, if resolved, probably have a high added value in this domain. The term generalized refers to the fact that these business cases are formulated in such a way that they can be applied to other domains as well:

1. **Maximize safety and minimise safety-related business risks and costs** while the complexity of car systems and components increase and costs for safety assessments should not increase. *Impact: improved system safety (leading to minimised recall costs and reduced number of post-accident claims), maintaining the cost of safety assessments close to the current levels.*

2. **Marketing improvement** by using a system that improves the current euro NCAP stars for cars system, introducing a more stable, reliable, trustworthy valuation system that has a well-defined relation with safety. *Impact: improved product marketing*

3. **Decrease number of claims** by using the standard which is the industrial de facto best practice. In case of a lawsuit the automotive industry should be able to defend the car’s (safety) design by stating that it was designed and constructed by using the commonly accepted standard c.q. the best practice at that moment. *Impact: improving insight in safety design*

The generalized automotive business cases are further detailed in the following section.

### 5.5.1 Business cases: Automotive domain

Before describing the three business cases elicited in the automotive domain we present the Business Model Canvas and the results of the BOAT framework.

Firstly, the Business Model Canvas for the automotive sector (Figure 11) bears similarities with those for Aviation/Avionics and Railway sectors described in the preceding sections: usage and license fees are the key revenue streams with maintenance and personal assistance (that should be feasible for the value proposition) resulting in higher costs. Overall, the platform will provide a framework for (controlled) exchange of safety assurance data between the three groups of stakeholders (that correspond to three distinct customer segments): vehicle manufacturers, their suppliers and, potentially, reviewers. The inclusion of reviewers at this stage is a “growth provision” that is based on business case related to utilisation of marketing opportunities arising from third-party verification of vehicles conformance with best industrial practice embedded in ISO26262 standard (or any other future standards). At this stage we intentionally leave definition of
platform will also provide specific support for ISO26262 processes in general and, in particular, for the reuse of safety assurance data (in-line with the SEooC – Safety Element out of Context concept). This forms the basis for ‘primary’ value propositions with an additional expected “emerging” benefit of improvement in safety of automotive systems. The platform can add value by facilitating safety assurance (reducing the efforts necessary for assembling assurance artefacts and facilitating uniformity through the supply chain), effective exchange of assurance artefacts (reducing the need to reassure reused systems and components) and allowing effective review of conformance (that can be utilised for purposes of marketing and construction of defence for post-accident claims).

The value added by the platform to customer segments, of course, depends on the content provided by customers themselves: component manufacturers would have to upload assurance artefacts (e.g. safety case modules and evidence) into the platform whereas vehicle manufacturers would have to upload integrated assurance artefacts for the entire vehicle. Additionally vehicle manufacturers and reviewers may use the platform for disseminating guidance on their preferred means of compliance with the standards and [in case of manufacturers] any assurance requirements imposed in addition to those contained in the international standards. Finally, all users will provide feedback on platform usage leading to continuous improvement and maintenance of the platform itself. For these reasons we include three groups of customers in Key Partners of the business model.

In addition to customers’ involvement, the OPENCROSS platform value proposition relies on:

- **Design & analysis tool vendors** – e.g. reliability, availability, maintainability, and safety (RAMS) tool vendors – who will integrate and adapt their tools to export assurance evidence in formats that can be ‘consumed’ and traced by OPENCROSS platform.

- **Standardisation organisations and authors of best practice and standard compliance guidance** – who will make their standards and guidance (respectively) available through the platform in a format compatible with the internal platform structure and will maintain those artefacts up-to date\(^2\).

\(^2\) Initially the OPENCROSS platform will be populated and guidance will be developed by the project partners. However, in the long term it is foreseen that the guidance will be expanded and updated by a wider community of practice that will emerge from the project.
It can be noted that those partners can also be seen as our potential customers, since the OPENCOSS platform can add value to their business processes by providing a new channel for distribution and licensing of their products. This value may be especially significant in the automotive sector given the low saturation of the tools and consultancy/guidance markets established by publication of ISO26262. However, for simplicity, we exclude those potential customers from the Business Model Canvas at this stage.

Figure 18: The Business Model Canvas for automotive

Secondly, the BOAT model for the automotive sector (Table 4) is largely the same as the generic OPENCOSS model presented earlier in this document with most changes confined to details of the commentary (in the rightmost column). However, one difference is that – due to the absence of governmental regulators / certification bodies with jurisdiction over system safety in the automotive domain – all parties in the model are businesses (with no involvement of government and, thus, no B2G or G2B provisions currently foreseen).

In the next sections we describe the e³ value models for the identified business cases.

Table 4: OPENCOSS’ BOAT Business model for automotive

<table>
<thead>
<tr>
<th>Business model: OPENCOSS platform in automotive</th>
<th>Concepts</th>
<th>Categories</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties</td>
<td>B2B, B2G</td>
<td></td>
<td>B2G and G2B cooperation may be added in the future if required (e.g. by changes to the legislative and regulatory frameworks of particular jurisdictions)</td>
</tr>
<tr>
<td>Objects</td>
<td>Digital goods</td>
<td></td>
<td>Safety case, arguments, evidence (including, in case of SEooC,</td>
</tr>
</tbody>
</table>
characterisation of the past usage context of components)

<table>
<thead>
<tr>
<th>Time scope</th>
<th>Static/semi-dynamic</th>
<th>characterisation of the past usage context of components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drivers</td>
<td>Increasing reach</td>
<td>More companies will be able to demonstrate safety of their safety critical systems. Stored and reusable safety cases will enrich the relationships and results in repeat sales.</td>
</tr>
<tr>
<td></td>
<td>Increasing richness</td>
<td></td>
</tr>
<tr>
<td>Chains</td>
<td>By reintermediation enabling disintermediation</td>
<td>Unification of safety cases and enabling reuse provides support for SEooC concept of ISO26262 and, thus, allows for skipping (part of) the assessment of already assessed (complete/sub)systems.</td>
</tr>
<tr>
<td>Directions</td>
<td>Time compressed business</td>
<td>Time advantage through reuse of safety cases. Increased safety is a second important direction.</td>
</tr>
<tr>
<td>Structure</td>
<td>Uniform and reusable safety cases.</td>
<td></td>
</tr>
</tbody>
</table>

The stakeholders in this process are described in Section 6.2.3, for more information about their goals and needs, we refer to this section.

5.5.1.1 Maximise safety and minimise safety-related business risks and costs

Accidents that can be attributed to vehicle design are, obviously, highly undesirable because of the financial impact of recalls and litigation, reputational damage, and, most of all, loss of human lives. The use of the OPENCOSS platform can help in maximizing safety and, thus, minimizing associated business risks and costs.

5.5.1.1.1 Summary of Key Idea

This business case addresses the perceived need to improve the levels of system safety whilst maintaining, as far as practicable, the cost of safety assurance processes across an automotive product line over the medium to long term. It is hoped that adopting an evidence-based approach to safety assessment and exploiting the assurance artefacts reuse capabilities afforded by the OPENCOSS Platform and the methodologies associated with it will facilitate this. In particular, the platform will provide clear frameworks, templates and guidance for safety assurance that will enable proactive and effective safety management and will minimise start-up costs for new product programmes. By facilitating common practices and effective exchange of safety assurance artefacts within the supply chain the platform will contribute to reductions of costs associated with re-assurance activities performed by vehicle integrators. Further reduction will be achieved by facilitating the reuse of safety assurance assets in the context of component reuse. These savings – shared between vehicle and component manufacturers – will help to offset costs associated with the new ways of working and with the (perceived) increase of rigour necessitated by the newly published international automotive system safety standards ISO26262.

5.5.1.1.2 Stakeholders and Their Goals

Automotive manufacturers – desire to avoid increase in the cost of safety assessment as a proportion of system development costs. They wish to maintain a rigorous, but cost-effective approach to safety assessment through the supply chain (and therefore to be clear about what assessment artefacts are
required from suppliers). They wish to achieve an equitable distribution of safety assurance responsibilities, efforts and costs over the supply chain and to utilise, as far as practicable, assurance artefacts generated by component suppliers. This approach should be scalable to future systems across the product line, which will include vehicles to be deployed in a variety of markets and terrains.

Component suppliers (supply chain) – desire to work to clear requirements and have their safety assurance responsibilities clearly defined from the onset of the projects. They wish to minimise the incidence of safety assurance rework being caused by poor definition of processes and objectives and miscommunications with clients positioned further up the supply chain (e.g. vehicle manufacturers). Furthermore they desire common contractual interfaces to integrators of diverse safety-critical systems to maximise the reach of their products.

Transport Consumers (not directly shown in this business case) – wish to avoid knock-on costs in the purchase of new vehicles which might be occasioned by a more expensive approach to safety, while at the same time being assured that the systems are safe.

5.5.1.1.3 Context and Scope
As Toyota’s mass recall of vehicles in the wake of an accelerator pedal failure in 2010 indicates, safety concerns in the automotive sector can have serious financial consequences, in terms of immediate costs of rework and in terms of reputational damage and loss of future sales income. One way to reduce these costs is to maximize the confidence consumers have in the safety of the vehicles they buy. This can be achieved by the provision of, and adherence to, well-controlled, credible and transparent safety assessment processes.

Automotive systems are becoming increasingly complex, and increasingly dependent on novel technologies, often in combination with one another – for example, next-generation cars will combine new fuel technologies (such as electric power, hybrid power etc.) with innovative fully-automated control functions (‘drive by wire’). These conceptual complexities are mirrored in the increased complexity of the engineered system: the number of components, and the interdependencies between them, is proliferating. The contractual/commercial context of the systems is thus complicated by the manufacturers’ need to manage an increasingly diverse, numerous and globalized supply chain, with which common communication protocols are required. This scenario describes the role of OPENCOSS platform in establishing and maintaining common safety assurance frameworks and assurance information exchange channels throughout the extended supply chain and across numerous development projects.

There are considerable costs associated with the generation of evidence artefacts to support safety assessment activity. Many of these costs are associated with the repetition of identical, or near-identical activities across near-identical systems – for example, the repetition of MC-DC testing on an identical component reused from one system variant to another in a well-managed product line.

This scenario considers the use of the OPENCOSS Platform and approach (i.e. the methods and processes it enshrines) to support and de-risk the managed reuse of safety assessment artefacts and processes within an automotive product line, and thereby to reduce costs.

5.5.1.1.4 Technology Infrastructure
The OPENCOSS platform will provide guidance, templates and patterns for the compositional development of safety assurance portfolios or dossiers (from now on – “safety cases”) compliant with the requirements of ISO 26262. These will include material targeted at vehicle manufacturers (who will be responsible for setting up the overall safety case framework for a project/vehicle, for formulation of requirements and constraints for suppliers and for integration of the overall safety case for the vehicle) as well as component
suppliers (who will be responsible for demonstrating conformance to vehicle manufacturers and standards requirements/constrains and production of safe assurance data / safety case modules for the supplied components).

The platform will provide the environment for communicating safety assurance information (guidance, requirements, constraints, safety evidence, safety cases and their fragments/modules) between all supply chain stakeholders.

Related to component reuse between different vehicles, the OPENCOSS Platform will provide a structured means for the storage of safety evidence and records of contextual assumptions relating to individual reusable components; this is motivated in part by the concept of Safety Element out of Context (SEooC) in ISO 26262. In so far as is practicable, these assessment artefacts can be treated as encapsulated, ‘plug-in’ components for reuse in safety assessment arguments and activities relating to future automotive systems in which the components themselves are reused.

In addition, OPENCOSS will also provide scalable techniques to guide the development of safety assurance arguments and evidence artefacts to support this reuse, by encapsulating argument concerns in a modular breakdown of the argument. These techniques will highlight areas of ‘mismatch’ between reused systems, and enable any required additional work to generate further safety assessment evidence to be focused and bounded, meaning that appropriate cost calculations can be made.

5.5.1.1.5 Scenario
Precondition: The OPENCOSS Platform infrastructure exists. It provides storage and retrieval facilities for evidence artefacts and contextual assumptions related to safety-critical components.

1. Vehicle manufacturer initiates the project within OPENCOSS platform using guidance and templates provided by the platform. They specify constraints and requirements that must be met by individual suppliers and, where necessary, additional guidance (incl. templates) for suppliers.
2. Having designed the components, suppliers provide safety assurance evidence and artefacts associated with individual components to the manufacturer via OPENCOSS platform. They use generic guidance provided by the platform (including guidance on compliance with the standards) along with the project-specific guidance relayed through the OPENCOSS platform by the vehicle manufacturer.
3. The Automotive manufacturer uses these techniques to develop a system argument (System A).
4. System B is a variant on System A, within a well-managed automotive product line. The nature of the similarities and differences between the two systems is well-known and is bounded. System B reuses a safety-related component which is also used in System A.
5. The OPENCOSS Platform provides templates and techniques for the integration of evidence, justification and associated contextual information from the modular safety argument created for System A in system-level argument for System B.
6. The OPENCOSS platform provides a means to generate an outline argument, and to query interfaces between argument modules with which the component module interacts, to permit investigation of whether the rely-guarantee relationships between those modules are still valid, given the context into which the component has been inserted and the role played in the argument by the evidence argument (i.e. the assertions and dependencies it supports).

3 The term ‘component’ is used loosely here. The scope of reusable elements will need to be established by the OPENCOSS work on modular safety arguments. For the purposes of this document, the term has the same scope as does ‘System Element’ in ISO 26262.
7. Where ‘plug-in’ reuse is not possible because the degree of confidence required of the argument module cannot be supported by the reused evidence artefact in the new argument context, the OPENCOSS Platform provides an indication of where there are ‘mismatches’ in the argument and/or the evidential chain which violate the rely-guarantee relationships.

8. The Automotive Manufacturer uses these indications to motivate and bound the generation of additional evidence, or the recasting of the argument, or reconsideration of the component reuse decision.

The e³ value model is depicted in Figure 19.

Figure 19: e³ value model in automotive maximise safety (and reuse)

5.5.1.1.6 Cost considerations

In addition to the costs inherent in the initial establishment of the OPENCOSS Platform and methods, which are borne by the OPENCOSS project, there may be additional costs relating to the specialization of the approach for the specific automotive product line. These would relate to the establishment of data storage protocols and (potentially) specialized argument templates⁴, and would be borne by the automotive manufacturers. There will also be costs to the automotive manufacturers inherent in uploading data to the Platform, examining output arguments and reworking to ‘fill’ the gaps identified.

5.5.1.1.7 Success measures

Quantitative targets for the reduction of certification costs – or maintenance of same at current levels, pro rata – over a defined timescale (medium/long-term), and relative to system development costs (taking into account the increasing complexity of the systems) will need to be supplied by automotive manufacturers.

⁴ While it is anticipated that OPENCOSS will develop some generic, reusable safety argument templates, as part of the compositional assurance methodology, it is likely that these will require specialisation for individual project instances.
5.5.1.2 Marketing Improvement

If the OPENCROSS platform can help in developing safer cars, and this is measurable, the fact that it is used in the daily way of working can be used as an argument to increase the Euro NCAP stars.

5.5.1.2.1 Summary of Key Idea

This business case addresses the perceived need to increase the effectiveness of safety as a driver for the marketing of new automotive products. This will be achieved by focusing safety assessment activity on key aspects of the assurance case, as these are perceived from the perspectives of the safety assessors and consumers, and also by improving public communication of the relevant safety aspects of the system.

5.5.1.2.2 Stakeholders and Their Goals

Vehicle manufacturers – desire to maximize the ‘returns’ of their investment in safety assessment activities through marketing of the fact that systems are engineered for safety (rather than ‘merely’ to withstand damage caused in accidents). They wish to ensure that vehicle’s safety assurance conforms to the best industrial practice in the sector (e.g. as described in ISO26262 standard) and to use such conformance as product feature in marketing. Manufacturers also wish to improve their assurance practices through independent third-party review.

Reviewers - wish to remain confident that the safety of systems can be assured and that best practice has been followed in the engineering activities. To reduce assessment/appraisal costs they desire for safety assurance to be performed in a traceable and transparent way and for responsibilities of- and assurance artefacts produced by- all supply chain stakeholders to be defined in a clear and reviewable fashion. Above all, reviewers wish to maintain their image of impartiality and credibility.

Transport Consumers – wish to have a means to come to an informed decision about the safety of various car models to inform future purchase. Wish for assurance of the safety of the car they currently own.

5.5.1.2.3 Context and Scope

Within the three industrial sectors directly represented in OPENCROSS, automotive is unique in terms of operating within the context of consumer market. Whilst air and rail passengers are rarely aware of safety characteristics of particular equipment their transportation relies upon, car buyers routinely actively seek this information as part of selecting a vehicle model to purchase. Vehicle safety is therefore one of commercial and marketing drivers for automotive manufacturers which also means that costs of investment into demonstrable achievement of higher levels of safety can be in principle offset by higher levels of sales.

To facilitate informed consumer choice various publications and associations independently appraise safety of different vehicle models. One of the most prominent appraisal programs in Europe today is Euro NCAP (European New Car Assessment Programme) – a voluntary car safety performance assessment programme, which is supported by a number of European government agencies. NCAP publishes reports on the safety of new cars and awards star ratings based on the performance of the vehicles in a series of pre-defined crash tests. Test results are widely publicized in the motoring press, and are a major influence on consumer choices and demand. Automotive manufacturers and safety assessors do, however, identify some shortcomings in the Euro NCAP approach – notably the restricted nature of the tests that contribute to the star ratings and focus on crashworthiness of vehicles rather than inherently safety of designs. The manufacturers are keen to improve product marketing by providing consumers with a more informed, system-specific and context-focused assessment of the safety of their products.
This scenario considers the use of the OPENCOSS Platform and approach to support independent third-party appraisal of vehicles’ safety assurance. Such appraisal can be used by manufacturers in both marketing and process improvement and, in the future, can be disseminated to the consumers through extended NCAP (or similar) schemes to facilitate informed choice.

5.5.1.2.4 Technology Infrastructure

The OPENCOSS project will provide approaches and guidance on the development of assurance arguments to provide confidence in the safety of new automotive systems. In particular, the arguments will demonstrate the evidential support offered to provide confidence of the coverage of key safety concerns for particular systems in particular contexts. The OPENCOSS Platform will support these approaches by providing technology to facilitate the development of the arguments, and also the identification of key safety drivers.

The platform will provide means for third-party reviewers to access (abstracted/partial views of) safety cases for independent appraisal.

5.5.1.2.5 Scenario

Precondition: The OPENCOSS Platform infrastructure exists and provides (among other things) access to various guidance on best practice in safety assurance. A vehicle manufacturer has initiated a new development program and, as development progressed, has populated the infrastructure with assurance artefacts for the new vehicle (or a system). Vehicle manufacturer is planning to utilise those artefacts for vehicle marketing through obtaining third party appraisal.

1. Vehicle manufacturer contracts a reviewer for Independent appraisal of safety assurance of the new vehicle (or system)
2. Vehicle manufacturer provides reviewer with OPENCOSS platform access credentials and sets up appropriate level of access to assurance artefacts within the platform.
3. Reviewer uses the OPENCOSS platform to access (abstracted/partial view) of assurance artefacts and evidence
4. As and when necessary the reviewer uses OPENCOSS platform to access generic- and standard-specific guidance stored by the platform and vehicle-specific guidance issues by the vehicle manufacturer to its suppliers.
5. Reviewer assesses conformance of the assurance artefacts to the best industrial practice (including conformance to ISO26262) and issues appraisal report
6. Vehicle manufacturer receives the appraisal report and uses it to motivate improvement of safety assurance practices on future (and, in rare cases, on the current) development programs
7. Reviewer and/or vehicle manufacturer disseminates appraisal results to consumers through various international and national assessment schemes (e.g. Euro NCAP), specialised automotive periodicals and marketing campaigns.

It should be noted that, for simplicity, the above scenario focuses on the final appraisal of a finished (or nearly finished) product only. In practice, it is likely that review and appraisal will be done in an iterative manner where early review of incomplete assurance artefacts will lead to (confidential) feedback to vehicle manufacturer. The later will, in turn, use this feedback to revise the safety assurance programme as

---

5 See scenario in Section 5.5.1.1.5 and e³ value model in Figure 19 for details.
6 At this stage we make no assumption on whether the report takes a form of a simple conformance certificate or is more substantial / descriptive in nature. We also make no assumptions about whether the OPENCOSS platform is to be used for storing the report/certificate.
appropriate at the stages of development and safety lifecycles where such changes can be made in a cost-effective fashion.

It should also be reiterated that we intentionally leave the detailed description of the “reviewer” stakeholder undefined. This can be an Independent Safety Assessor (ISA), the representative of some national or international programme (e.g. NCAP) or other types of stakeholders.

The scenario is summarised by the e³ value model in Figure 20. For simplicity the model shows the direct link between reviewers and consumers. This is unlikely to hold in practice as information is likely to be disseminated through indirect channels (and possibly via vehicle manufacturer). However, the dissemination channel is unlikely to directly involve OPENCOSS platform and this simplified representation is therefore considered to be fit-for-purpose in the context of the present document.

![Figure 20: e³ value model for automotive marketing](image)

### 5.5.1.2.6 Cost considerations

In addition to the costs inherent in the initial establishment of the OPENCOSS Platform and methods, which are borne by the OPENCOSS project, there may be additional costs relating to the development of generic argument templates and the establishment of ‘equivalence claims’ across safety-critical domains. These costs may, however, be within the scope of the OPENCOSS project itself.

### 5.5.1.2.7 Success measures

Quantitative measures for the improvement in sales resulting from improved communication with a ‘positive spin’. Qualitative measures of ‘marketing effectiveness’. These will need to be supplied by automotive manufacturers.

---

7 These costs may, however, be within the scope of the OPENCOSS project itself.
5.5.1.3 Decrease Number of Claims

Every time an accident happens due to a design fault or construction error, the automotive company stands the chance of being sued. Using the OPENCOSS platform and the best practices that it prescribes and enforces, makes for safer cars which will result in less accidents and hence, less claims.

5.5.1.3.1 Summary of Key Idea

This business case addresses need to decrease the number and cost of negligence claims arising from accidents or product recalls relating to (alleged) shortcomings in vehicle safety. This will be achieved by improving safety engineering processes and hence product safety, and by providing a legal defence of adherence to best industrial practice.²

5.5.1.3.2 Stakeholders and Their Goals

Automotive Manufacturers - wish to decrease the number of negligence claims arising from accidents or product recalls relating to safety concerns. Provision of a legal defence by appeal to adherence to best practice is a desideratum. There is also a desire to improve the safety of products – and to be able to demonstrate this safety by convincing justification.

5.5.1.3.3 Context and Scope

In an increasingly litigious society, transport consumers – and their insurers and lawyers – are ever more inclined to bring negligence claims relating to manufacturing defects in the wake of automobile accidents. Given the increasing complexity of vehicle designs and the increased globalization of the market (see business case 1 above), the liabilities involved can be massive. For example, in February 2010, in the wake of the product recall occasioned by a faulty accelerator component in the Prius and other models, Toyota was subject to more than 30 class action lawsuits in the United States alone, one of these involving over 5 million separate claims. The liabilities were estimated at billions of US Dollars.[2]

Automotive manufacturers – and their lawyers – are keen to reduce their level of exposure to this type of claim.

This scenario considers the use of the OPENCOSS Platform to provide a legal defence against this type of lawsuit, by providing evidence of adherence to best practice in the evaluation of the safety of systems.

5.5.1.3.4 Technology Infrastructure

The OPENCOSS project will provide a common framework for the evaluation of safety of safety-critical systems in the automotive, avionic and railway domains, and will establish a community of practice across Europe to instil the approach enshrined in the framework as industrial best practice.

5.5.1.3.5 Scenario

1. OPENCOSS project provides methods and guidance for the safety assessment of safety-critical systems in several domains.
2. Automotive manufacturer develops products to meet the requirements enshrined in this guidance, and uses the OPENCOSS Platform and methodology to produce a reasoned argument for the safety of a system, supported by focused, well-motivated evidence.

² It might be possible to argue that the re-use of ‘safe’ components – as facilitated by the OPENCOSS modular certification approach – actually makes systems safer. There is, however, little evidence to support this claim.
3. OPENCOSS project develops a pan-European (indeed, potentially global) community of practice derived from target and related domains. This community validates the OPENCOSS approach as a de facto best practice standard for safety assessment.

4. Automotive manufacturer participates actively in this community of practice.

5. In the event of a lawsuit, a best practice defence can be mounted, based on adherence to the OPENCOSS framework and participation in the community of practice (CoP).

The $e^3$ value model is depicted in Figure 21.

![Figure 21: $e^3$ value model on decrease claims](image)

5.5.1.3.6 Cost considerations

There will be development costs associated with adherence to the OPENCOSS framework, and also some costs associated with participation in the CoP.

5.5.1.3.7 Success measures

Quantitative measures of reduced amount and cost of litigation over time. These will need to be supplied by automotive manufacturers.

5.6 Conclusion

Even though the business cases for all domains are slightly different, they share common themes. Both from the development and the certification perspective, respondents expect the OPENCOSS platform to
minimize development time and costs. They think this could be possible by facilitating the following functionality.

**Unification of terms and concepts**
Safety concepts are shared across domains, though the terminology is not the same in different domains and the same terms sometimes have a slightly different interpretation. The OPENCOSS platform can aid in unifying terms or show their differences between domains, giving experts a better starting point to reason about cross domain certification and reuse of safety argumentation.

Moreover, if in one domain, an innovation is introduced that has not been available in another domain; it is highly desirable to reuse the best practices and lessons learned. The OPENCOSS platform can also help with the reuse of the safety argument. By linking concepts and terms, and by making innovations from other domains accessible in the same format, experts can discover and reuse parts of other domains, innovating their own products.

Furthermore, if a component is certified in one domain, it is virtually impossible to reuse that certification in another domain, as matters currently stand. The OPENCOSS platform can help make this possible by showing, in a structured and clear way, how the safety argument is structured and what assumptions it makes about the system context. This allows a certifying body to examine the argument and for instance only ask for additional evidence, instead of discarding the previous certification and doing the certification all over again.

By unifying standards, OPENCOSS platform will enable system manufacturers to reuse components from other domains (cross domain) or different countries much easier.

**Reuse - modularity of safety assessments or certificates as an enabler**
Currently when some part of a certified product is changed, the recertification of the entire product is required. It is not possible to assess the safety of a changed subsystem only. Splitting the complex system into modules and performing re-certification of the changed ones only would save a lot of work.

Assessing not the complete product again and again, but focusing on changes (deltas) of distinct components, can decrease the assessment effort, increasing time to market and decreasing development costs.

**Innovation – support for traceability, for example**
Safety critical systems are mostly complex, with big volumes of requirements definitions, design, architecture. Maintaining the traceability information between those artefacts and most importantly further traceability to verification and validation tests, source code and safety cases is a very challenging and time consuming task.

All the above topics are planned to be worked on in OPENCOSS project. The unification of standards will be addressed in WP4 with the CCL and ontologies. The modularization and compositional certification to maximize reuse is addressed in WP5. Finally, transparency and traceability will be addressed in WP6.
6 Stakeholder goals and user needs

In this chapter, we summarise the work undertaken to identify the Stakeholders relevant to the OPENCOSS Project, and to elicit their high-level needs with respect to the principal technical deliverable, the OPENCOSS Platform. This analysis serves as the basis for the high-level requirements which will be detailed in deliverable D2.2.

In Section 6.1, we outline the methodologies used to identify stakeholders and analyse their interests with respect to the OPENCOSS Platform. The results of this analysis are summarised in Section 6.2, which details the findings according to the three target domains for the project – avionics, automotive and railway transport. Section 6.3 details the high-level user needs relating to the Platform.

6.1 Stakeholders

In requirements engineering, the term ‘Stakeholder’ is used to refer to a person, organisation or system which has an interest in the system under development [6]. Stakeholders are directly affected by the product, in terms of being users or investors, or are people or organisations whose input is required in order to finalise the requirements for the product. It is common to think of a layered model of stakeholders, such as that shown in Figure 24, where typical stakeholder types for an IT project are grouped according to the nature of their interest in the system under development. Alexander and Maiden [6] refer to this as an ‘onion model’, since the stakeholders are visualised as belonging to a series of different ‘skins’, each of which represents a different type of interest, and each of which is encompassed in a wider context.
In Figure 24, the innermost circle, labelled ‘The Product’ denotes the system under development: the hardware and software, equipment and installations that we are making. The next circle out, labelled ‘The System’ encompasses all of the material contained in the ‘Product’ circle and also the people and systems which are interacting directly (functionally) with that material – as operators, maintainers or as systems which interface with the product. These are referred to as the product’s ‘Direct Stakeholders’. Figure 24 is a generic model, and as such contains generic placeholders for these generic stakeholders. They are instantiated for OPENCOSS in Section 6.2.4.

All of the other Stakeholder roles indicated in Figure 24 – i.e. the ones outside the ‘System’ circle – are generic roles for ‘Indirect Stakeholders’ of the product. In other words, they are not directly involved in the operation or functionality of the product, but play many different roles in the wider ‘Containing System’ (the other infrastructure and organisations with which the product has a direct non-functional interface) and the Wider Environment which it serves.

A number of Direct and Indirect Stakeholder groups have been identified for the OPENCOSS Project and its principal product, the OPENCOSS Platform. These stakeholders are analysed in detail in Section 6.2 below.

The Stakeholder analysis reported in Section 6.2 was carried out using a standard template derived from that available as part of the Volere requirements resource set developed by James and Suzanne Robertson and available for download at [9]. This template provides a structured method for characterising the kinds
of interests in and information about the system that Stakeholders are likely to provide. The template is reproduced in the Appendix in Chapter 16 below.

The Volere template provides a generic set of Stakeholder roles, which accords with that presented in the “onion model” in Figure 24. Stakeholder classes representing direct users of the system – operators, maintainers and systems interacting directly with the system – are captured, as are indirect stakeholders in the ‘containing system’, which is here given a business focus – the client investing in the product, functional beneficiaries from the product, the product sponsor (interface between the product and the wider containing system). In the wider environment, a series of positive and negative stakeholders are identified. Positive stakeholders include the customer (the ultimate purchaser of the product) and the regulatory bodies. Negative ones might include competitors, political interest groups or hackers. The template requires an accurate record of the exact stakeholder role and organisation, and the name of the individual holding this role within the project. Rationale for including the stakeholder, including benefits and drawbacks to his/her inclusion is recorded (from the perspective of the project), and an indication is given as to how much involvement (in terms of time) is required of that particular stakeholder.

The template then goes on to give a series of ‘classes of knowledge’ about the product, against which the Stakeholder’s contribution can be recorded. These classes of knowledge are as follows:

- Goals
- Business Constraints
- Technical Constraints
- Functionality
- Look and Feel
- Usability
- Performance
- Safety
- Operational Environment
- Portability
- Security
- Cultural Acceptance
- Legal
- Maintenance
- Risk
- Design Ideas

6.2 Stakeholder Analysis

In this section, we report on the stakeholder analysis carried out for OPENCOSS. It is worth noting that, conceptually, there is a distinction to be drawn between the OPENCOSS Project and its principal technological deliverable, the OPENCOSS Platform. In particular, we must distinguish between the direct client or sponsor of the OPENCOSS Project and the clients of the OPENCOSS Platform, who are not likely to be identical. Since OPENCOSS is an FP7 project, the European Commission – in the person of the Project Officer – is identified as the direct client of the project. He has the final say on the acceptance of the project deliverables, and must therefore be satisfied with the product as delivered. In project terms, ‘the product’ is the complete set of project deliverables, including all reports, guidance material and technological deliverables. In addition, the European Commission acts as a proxy stakeholder representing the interests of the European taxpayers and transport consumers.
The direct client for the OPENCOSS Platform, however, is a group of people, representing the manufacturer and safety assessor interests who will benefit from the system in terms of the savings made to recertification by adopting it for use. The European Commission is clearly involved in this group, and is also a beneficiary in these terms, but cannot be regarded as a direct client in this definition. Since OPENCOSS is intended to be an open-source project, the direct clients cannot be explicitly identified at this stage. However, there are a number of target groups within the three principal domains who definitely have a customer role in relation to the OPENCOSS Platform. In abstract terms, these can be considered as belonging to three general groups:

- Stakeholders involved in the development of a safety-critical product – i.e. manufacturers, component suppliers;
- Stakeholders concerned with the demonstration of a product’s compliance to a standard or series of standards – i.e. regulators, certification, bodies, standards organisations;
- Stakeholders concerned with supporting the development and compliance demonstration – i.e. consultancy companies, ISAs.

Sections 6.2.1, 6.2.2, and 6.2.3 below present the results of Stakeholder analysis for the different target domains of OPENCOSS, identifying Stakeholders in the OPENCOSS Platform (as opposed to the Project in general) from the avionics, railway and automotive sectors respectively. The stakeholders are identified as Primary or Secondary stakeholders, in terms of their proximity to the OPENCOSS Platform in use, and some indication is given as to the goals of the Stakeholders with respect to their business and the knowledge needed from these stakeholders by the project. Section 6.2.4 conflates these results into a general Stakeholder map for the OPENCOSS Platform, which is represented as an ‘onion model’.

### 6.2.1 Avionics Stakeholders for the OPENCOSS Platform

#### 6.2.1.1 Direct Stakeholders (Users)

**Aircraft or rotocraft manufacturer** – the manufacturer or system integrator who seeks approval from the certification authority in the form of a “type certificate” confirming that the aeronautical product complies with the applicable regulations. Note that “aeronautical product” refers here to a fixed-wing aircraft or a rotorcraft.

**Avionics system manufacturer** – the manufacturer who seeks acceptance of avionics systems from the certification authority. The goal of acceptance is to achieve credit for future use in a certification project.

**Equipment or component provider** – a supplier who seeks to establish the compliance of the hardware and/or software elements which it provides with requirements from the avionics system manufacturer who integrates them into the wider system.

#### 6.2.1.2 Indirect Stakeholders

**Airworthiness authority** – the certification organisation which formally recognises, on behalf of the state (or states) responsible for the certification, that an aeronautical product complies with the applicable regulations. ‘Aeronautical product’ means here a fixed-wing aircraft or rotorcraft.

**Standards organisation** – a domain-independent organisation whose primary activities are concerned with the development, co-ordination, promulgation, revision, emendation, reissuing, interpretation or production of technical standards that are intended to address the needs of some relatively wide base of adopters of the standards.
**Working group** – a team of domain experts who collaborate to draft new standards, or update existing ones, on behalf of a standards organisation. The lifespan of a working group can last between a few months and several years. Participants represent the interests and views of stakeholders from disparate sections of the community, all of whom happen to have some interest vested in the results of the working group’s activity.

**Tool provider** – a legal entity which delivers hardware and/or software facilitating the performance of some work.

**OPENCOSS community** – the set of partnering entities developing and maintaining the OPENCOSS Platform in order to offer products and services to the aircraft manufacturers, avionics system manufacturers and equipment or component providers.

### 6.2.2 Railway Stakeholders for the OPENCOSS Platform

#### 6.2.2.1 Direct Stakeholders (Users)

**System and subsystem manufacturer** - a company which produces components of a railway system or subsystem. The manufacturer is responsible for designing and producing systems or subsystems which comply with relevant safety standards and customer requirements and which are interoperable with the products of other manufacturers. The manufacturer is also responsible for demonstrating the safety of his products to the Independent Safety Assessor. The manufacturer’s goals are:

- To earn revenue from the manufacturer of railway systems/subsystems;
- To increase its share of the market by researching and developing new systems/subsystems;
- To reduce the cost and timescales inherent in obtaining approval for new systems/subsystems from the National Safety Authority;
- To reduce the costs of production and increase the volume of production.

**Safety assurance tool vendor** - a company which develops and sells software for use during the design and/or production of railway systems/subsystems. In addition to software design and development, the tool vendor analyses the needs of its user base (system manufacturers) in order to enhance the functionality of its software and keeps itself informed of the evolution of safety standards in order to ensure that its tools are state-of-the-art. The tool vendor’s goals are:

- To earn revenue from the sale of software tools and support packages for them;
- To research and develop new functions to meet market needs;
- To reduce the cost and development overheads for new features.

**Safety consultant** - a company which offers some kind of service (SW/HW development, Verification and Test, job-renting, experience for new systems etc.) to manufacturers of railway systems/subsystems. The consultant’s responsibilities are to conform to the company standards imposed by the client and to general safety standards, and to offer expertise in the field of interest to the client, including the provision of new knowledge. The safety consultant’s goals are to earn revenue from the sale of his services, and to reduce the cost of his operational activity, as well as to acquire new knowledge and competencies in order to enlarge his potential market.

**Independent Safety Assessor** - an independent body having expertise in the field of systems engineering and rail components, accredited by the National Safety Authority for railway systems. The ISA is responsible for the assessment of the compliance of a generic product, application or application-specific component to the applicable safety requirements, and for assessing its suitability for use in the railway domain. The ISA also assesses the compliance of a system and processes related to the safety of rail
traffic, with respect to the applicable safety standards. More explicitly, on behalf of the National Safety Authority, the ISA assesses the compliance of a system and processes related to the safety of rail traffic to the applicable National safety standards and rules. The Independent Safety Assessor’s goals are to provide an independent evaluation of components, applications, products of a railway system (i.e. to ensure that the assessment is not subject to business interests or economic constraints related to the company that developed the product).

6.2.2.2 Indirect Stakeholders

Ministry of Infrastructure and Transport – a national government body, which is ultimately responsible for the control and monitoring of the overall railway system. The Ministry’s goals are to ensure the safety of passengers and workers on the national railway system, and to prevent environmental damage arising from the use of the railway system (i.e. environmental pollution, damage from EMC).

National Safety Authority – an independent body established by the Ministry of Infrastructure and Transport for the purpose of ensuring rail safety. The National Safety Authority implements EU Directive 2004/49/EC, and is technically independent from the railway operators. It defines the legislative framework for the operational safety of railway systems, verifies that regulations have been adopted, carries out the approval process for systems, subsystems and components and issues safety certificates to railway undertakings and safety authorisations to infrastructure managers as appropriate. The goals of the National Safety Authority are as follows:

- to guarantee non-discriminatory treatment of all of the entities involved in railway transportation;
- to clarify safety principles and safety rules for railway operators;
- to check that current safety levels are maintained;
- to promote a steady improvement in safety, taking technological and scientific progress into account;
- to play an important role in the harmonization of national and international safety regulations, encouraging interoperability across the European railway sector.

Independent Safety Assessor - an independent body having expertise in the field of systems engineering and rail components, accredited by the National Safety Authority for railway systems. The ISA is responsible for the assessment of the compliance of a generic product, application or application-specific component to the applicable safety requirements, and for assessing its suitability for use in the railway domain. The ISA also assesses the compliance of a system and processes related to the safety of rail traffic, with respect to the applicable safety standards. More explicitly, on behalf of the National Safety Authority, the ISA assesses the compliance of a system and processes related to the safety of rail traffic to the applicable National safety standards and rules. The Independent Safety Assessor’s goals are to provide an independent evaluation of components, applications, products of a railway system (i.e. to ensure that the assessment is not subject to business interests or economic constraints related to the company that developed the product).

Rail Infrastructure Manager - a company which manages and usually owns railway infrastructure. It is responsible for the overall management and maintenance of the rail network. Specifically, the Infrastructure Manager will design and commission new installations, such as stations, track infrastructure, signalling subsystems; will manage and maintain trackside control systems; will supply railway undertakings with information pertinent to the operation of the railways – track status information, for example; and will manage the practical and contractual aspects of track management – line rental, maintenance schedules etc.. The goals of the infrastructure manager are as follows:

- to earn revenue from the rental of the network to the railway companies which use it;
- to reduce the cost of the ownership and maintenance of the infrastructure;
- to expand its network and market;
- to guarantee the safety of the record.

**Railway undertaking** - a company which rents tracks from railway infrastructure. The railway undertaking usually owns the train rolling stock used to offer service for passengers or goods. Its responsibilities are to manage and maintain trail rolling stock and to provide facilities for passenger travel and the transportation of goods. The railway undertaking’s goals are to make revenue from selling travel to passengers or from the transportation of freight, to reduce the cost overheads of owning and maintaining train rolling stock and to expand its share of the rail transportation market.

**Railway Transport Consumer** – an individual who purchases a ticket for rail travel, or a company which purchases freight transport from the railway undertaking. The individual consumer has not responsibilities beyond the reasonable use of the rail system, while the freight customer has a responsibility to inform the railway undertaking of the types of goods for which transportation is required and any hazards relating to them. The consumer’s goals are safe, comfortable, timely transport at a low price.

### 6.2.3 Automotive Stakeholders for the OPENCOSS Platform

#### 6.2.3.1 Direct Stakeholders (Users)

**Automotive manufacturer** – an organisation which is responsible for the development and marketing of new automotive vehicles, usually acting as a integrator of component subsystems developed in the supply chain. Automotive manufacturers will have the safety of their vehicles as a general goal, though it should be noted that there is, as yet, no clearly-defined safety authority or certification body for the automotive sector in Europe. Instead, safety activities are carried out in a manufacturer- (and to a certain degree market-) led environment.

**Safety Assessor** – an individual or organisation responsible for assessing the safety of an automotive system, subsystem or component with respect to defined safety requirements or the applicable standard. For software in the automotive domain, the ISO Standard 26262 has recently been adopted as the industry norm. The degree of independence required of the safety assessor and the safety assessment process with respect to ISO 26262 depends on the ASIL (Automotive Safety Integrity Level) of the system, subsystem or component under consideration.

**Automotive component manufacturer** – an organisation which is part of the supply chain for the automotive manufacturer, responsible for the development and marketing of a component to be integrated into the overall automotive system. The components developed by this organisation may be bespoke – i.e. for use only in automotive systems, whether or not those produced only by an individual; automotive manufacturer – or generic – i.e. for sale and deployment in more than one domain of application.

#### 6.2.3.2 Indirect Stakeholders

**Transport Consumer** – an individual or organisation who purchases a new vehicle or drives an automotive vehicle.

### 6.2.4 General Stakeholder Model for the OPENCOSS Platform

In this section, we present a general stakeholder model for the OPENCOSS Platform, based on the stakeholder analysis presented above. The model is presented in Figure 23: ‘Onion Model’ of OPENCOSS Platform Stakeholders in the form of an ‘onion model’, as introduced in Section 6.1:
The nature of the Stakeholders’ interest in the OPENCOSS Platform is described below. Some initial observations about the stakeholder model presented are required, however. Firstly, it should be noted that, even though this model represents an instantiation for the OPENCOSS Platform, the Stakeholder roles presented here are represented relatively generically. For example, broad stakeholder groups for manufacturers of safety-critical systems and components are included, which conflate the groups described in detail in Sections 6.2.1 through 6.2.3 for the target domains. Secondly, it should be noted that the manufacturing organisations actually appear as Stakeholders in two separate layers of the model – their role as direct stakeholders – users of the Platform – is captured in the generic roles of Project Manager, Safety Engineer and Argument Developer in the ‘Direct Users’ layer, since these generic roles are the representatives of the companies’ direct interaction with the Platform. The manufacturing organisations are represented as organisations in the ‘Indirect Stakeholders’ layer, since that layer represents their functional and financial benefit from the system. Similarly, the European Commission appears twice in the diagram: firstly in the ‘Indirect Stakeholders’ layer as the ultimate customer for the system, and secondly in the ‘Wider Environment’ layer as a political beneficiary. Thirdly, it should be noted that there are other types of Stakeholder with an interest in the OPENCOSS Project and Platform who have not been represented in this analysis. Most notable among these are various research institutes and consultancy groups who have a research interest in the work of the OPENCOSS Consortium. Finally, no negative Stakeholders are identified in this model.

The interests represented by the Stakeholders in each layer of the model are described below.
6.2.4.1 ‘Direct Users’ Layer

**Interfacing Systems** within the user organisations. These include existing systems used by manufacturers and safety assessors to carry out their safety assessment activities, produce evidence and so on.

The **OPENCOSS Consortium** will develop and provide ongoing operational support and maintenance for the OPENCOSS Platform.

The **Project Manager** will be working on a project within a system or component manufacturing organisation. He will use the OPENCOSS Platform to view and produce metrics on the progress of safety assessment projects, to plan resource and to view workflows indicating progress on compliance and assurance-based projects.

The **Safety Engineer** will be responsible for the demonstration of safety on a project within a system or component manufacturing organisation. He will use the OPENCOSS Platform to plan, review, view, develop, store and save workflows, evidence artefacts, safety arguments and compliance checklists. He may also use the Platform to reuse argument and evidence artefacts relating to the safety of a reused component.

The **Argument Developer** will be responsible for the presentation of an argument of assurance of the safety of the system or subsystem being developed by a manufacturing organisation. He will use the OPENCOSS Platform to plan, build, review, view, develop, store and save safety arguments or modules, sometimes by composing pre-existing argument modules, and reusing arguments and evidence relating to reusable components.

The **Safety Assessor** is responsible for assessing the adequacy of the evidence and assurance ‘package’ provided by the manufacturers, in terms of demonstrating the safety of the system or component under consideration. Depending on the domain, and on the nature of the system under consideration, the safety assessor may be more or less independent of the manufacturing organisation. The safety assessor will use the OPENCOSS Platform to view workflows, arguments, compliance checklists and evidence artefacts relating to the system or component.

6.2.4.2 ‘Indirect Stakeholders’ Layer

**System and Component Manufacturing Organisations** are the functional and financial beneficiaries of the OPENCOSS Platform. The functionality provided by the Platform will reduce costs and time overheads associated with the assurance of safety-critical components and will improve marketability of the companies’ products. The Manufacturers might also be regarded as the final **Purchasers** of the Platform, but this is currently unclear, since the project uses an open-source model. Purchaser is therefore left as a generic stakeholder at this point.

The **European Commission** is included in this layer as the project’s sponsor and funder.

6.2.4.3 ‘Wider Environment’ Layer

The **National Government** is included here as a generic Stakeholder type, representing the national political bodies which hold ultimate authority for safety in the transport domains and which delegate to the national safety authorities.

The **National Safety Authority** is a generic placeholder for the various national bodies responsible for safety in a particular domain (note that this is not directly relevant in automotive). These bodies are answerable to the national governments. They are included here as political beneficiaries from the OPENCOSS Platform, since improved visibility of safety assurance is a benefit.
The European Safety Authority is a generic placeholder for the European overseers of overall transport safety in the aerospace and railway domains. As with the National Safety Authorities, they will benefit politically from the enhanced visibility of safety assurance.

The Regulator is a generic placeholder for the safety regulatory and safety certification bodies in the aerospace and railway domains (automotive manufacturers do not answer directly to a certification body).

The Transport Consumer will benefit from the reduced costs of safety assurance, and from the confidence that enhanced transparency of the assurance process brings to the travelling experience.

6.3 User Needs

6.3.1 User Needs for the Avionic Domain

In this section, the term ‘aircraft’ is used instead of ‘aircraft or rotorcraft’, in order to improve readability. We consider three classes of user here: aircraft manufacturers, who subcontract various parts of the aircraft development to avionics system manufacturers, who in turn rely on equipment or component providers.

Aircraft manufacturers seek approval from the certification authority in the form of a ‘type certificate’, which confirms that the aircraft complies with the applicable regulations. The set of applicable standards (the “certification basis”) is established by the certification authority in consultation with the applicant for a given aircraft certification. These particular certification requirements are constituted by national regulations completed by special conditions as necessary. Some of these requirements apply to the avionics system manufacturers and/or to the equipment/component providers as well. The three users would benefit from a platform helping them to handle these certification bases, identifying commonalities and peculiarities regarding different aircraft certifications.

All three users establish several plans: certification, development, validation/verification, configuration management and process assurance plans. They would benefit from a platform helping them to handle these plans.

Aircraft manufacturers perform Function Hazard Assessments (FHA) to identify the failure conditions of the aircraft functions and establish their severity, and Preliminary System Safety Assessments (PSSA) to determine safety requirements for every part of a proposed system architecture and implementation, using the results of the FHA. The PSSA is an iterative analysis associated with the design definition and imbedded within the overall development. Aircraft manufacturers also perform System Safety Assessments (SSA), which are systematic and comprehensive evaluations of the implemented system, to show that the qualitative and quantitative safety requirements as defined in the FHA and PSSA have been met. The avionics system manufacturers and equipment/component providers contribute to these assessments. All three users would benefit from a platform helping them to handle the allocated requirements and the associated compliance evidences.

During the development lifecycle, aircraft manufacturers build the certification data package required by the certification basis. Several documents are formally submitted, among which the accomplishment summaries, while other documents are made available to the certification authority; this depends for each document on the Level Of Involvement (LOI) defined in the certification basis. The avionics system manufacturers and equipment/component providers contribute to these certification data packages. The aircraft manufacturers would benefit from a platform helping them to handle the data packages in conformance with the applicable certification requirements.
Acceptance is the acknowledgement by the certification authority that a module, application or system complies with its defined requirements. The goal of acceptance is to achieve credit for future use in a certification project. Incremental acceptance is the process for obtaining credit towards approval and certification by accepting or finding that an Integrated Modular Avionics (IMA) module, application and/or off-aircraft IMA system complies with specific requirements. Incremental acceptance provides the ability to integrate and accept new applications and/or modules in an IMA system and to maintain existing applications and/or modules without the need for re-acceptance. All three users would benefit from a platform helping them to handle the allocated requirements and the associated compliance evidences in the context of incremental acceptance.

As a summary, the aircraft manufacturers, system manufacturers and equipment/component providers exchange and share numerous pieces of information which tie them together. Incremental development and iterative activities tend to have rippling impacts on already existing pieces of information. All three users would benefit from a platform helping them to cope consistently with the induced complexity, in particular to manage information traceability and to enable delta recertification.

### 6.3.2 User Needs for the Railway Domain

Assessors frequently need to repeat assessment activities for products of the same type from different manufacturers, because of the differences in the ways in which similar safety principles and measures are described. The activity is time-consuming and difficult to estimate, because every assessment is different. With the OPENCOSS Platform, every manufacturer should be able to describe the system he is developing, and the safety principles applicable to it, in a more transparent way, thus simplifying the safety assessment itself and facilitating more accurate estimates in terms of the time and resources it requires.

Use of the OPENCOSS Platform should also help manufacturers to predict the time, resources and other costs required for assessment of products more precisely. Moreover, the process and conceptual transparency provided by the common certification language should allow for easier, more complete and more accurate transfer of technical information between assessment bodies, simplifying product endorsement, cross-acceptance and delta-assessment. This will yield considerable cost benefits for these activities.

It is essential that assessors should understand how the manufacturer plans to provide assurance of the safety of the product. The manufacturer produces evidence in the form of documentation, tests, reports etc. Every manufacturer uses a different means to organise this information, which is not always complete. In consequence, it can be very difficult for the assessor to have a clear understanding of the system functions, relevant safety aspects and so on. In this situation, the assessor spends a lot of time and resource in obtaining information from the manufacturer (especially from the system designers) in order to fully understand the assumptions related to the test results and other evidence artefacts with which he is confronted. As a consequence, the time actually required for the assessment varies markedly from the original estimation, resulting in an increase in resource- and cost-demands on both the assessor and the manufacturer.

The OPENCOSS Platform should help the manufacturer to allocate functional and safety requirements to designed subsystems, components and external facilities, in order to organise the information he needs for safety assessment and to evaluate the documentation which has been made available, across all the lifecycle stages. Tooling should help in locating deficiencies and inconsistencies in the information before the information is given to the assessor, resulting in a clearer understanding of system safety and how it can be assured.
In addition, the OPENCOSS Platform should encourage the exchange of technical and safety-related information between the manufacturer and the assessor in an easily comprehensible and easily auditable way. The assessor’s needs in terms of the compositional approach to assurance to be provided by OPENCOSS are to understand how safety of a component can be assured and how this can be extended across the system as a whole.

Finally, it will be important for manufacturers to have tool support to enable them to take safety implications into account during financial analysis of plans for system development and in assessing the safety implications of any planned modifications to the system.

6.3.3 User Needs for the Automotive Domain

Automotive manufacturers have the safety of their vehicles as a general goal, though it should be noted that there is, as yet, no clearly-defined safety authority or certification body for the automotive sector in Europe. Instead, safety assurance activities are carried out in a manufacturer- (and to a certain degree market-) led environment. In terms of the OPENCOSS Platform, which focuses on the assurance of safety-critical systems and components, the needs of the automotive stakeholders may be summarised as follows:

Automotive manufacturers desire to avoid increase in the cost of safety assessment as a proportion of system development costs. Wish to maintain a rigorous, but cost-effective approach to safety assessment through the supply chain (and therefore to be clear about what assessment artefacts are required from suppliers). This approach should be scalable to future systems across the product line, which will include vehicles to be deployed in a variety of markets and terrains. Automotive Manufacturers wish to decrease the number of negligence claims arising from accidents or product recalls relating to safety concerns. Provision of a legal defence by appeal to adherence to best practice is a desideratum. The manufacturers also have a desire to maximize the effectiveness of their investment in safety assessment activity by focusing their effort on those aspects of the assurance effort which are important drivers for consumers and government agencies. They wish also to exploit possibilities of using safety as a marketing tool, in particular by putting a ‘positive spin’ on the fact that their systems are engineered for safety, rather than to withstand damage caused in accidents. There is also a genuine desire to improve the safety of products – and to be able to demonstrate this safety by convincing justification.

Transport consumers wish to avoid knock-on costs in the purchase of new vehicles which might be occasioned by a more expensive approach to safety, while at the same time being assured that the systems are safe. They also wish to have a means to come to an informed decision about the safety of various car models to inform future purchase, as well as for assurance of the safety of the car they currently own.

Safety Assessors wish to remain confident that the safety of systems can be assured, and to reduce the time and cost overheads inherent in repeated or overly cumbersome work occasioned by the presentation of safety justification and evidence data in a format which is difficult to read and navigate.

Automotive component manufacturers desire common contractual interfaces to integrators of diverse safety-critical systems across the automotive and other domains.
7 Conclusion

Safety assurance and certification are among the most expensive and time-consuming tasks in the development of safety-critical embedded systems. European innovation and productivity in this market is curtailed by the lack of affordable (re)certification approaches. Therefore, the OPENCOSS project aims to devise a common certification framework that facilitates the reuse of assurance assets across and between domains. The ultimate goal of the project is to bring about substantial reductions in recurring safety certification costs, and at the same time to increase product safety through the introduction of more systematic certification practices. Both will boost innovation and system upgrades considerably.

At this moment the framework, the OPENCOSS platform, is currently under definition and its exact form is still debated. Nevertheless, the aim of the OPENCOSS platform is clear, and in this context we have looked at the future OPENCOSS framework and community and analysed its business opportunities in any domain that involves safety critical systems. The goal of this deliverable is to demonstrate the added value of the possible OPENCOSS business cases.

First we have looked at the possible business opportunities in the domains included in OPENCOSS and have identified the following generalised business cases. The term generalized refers to the fact that these business cases are formulated in such a way that they can be applied to any domain. We have divided the business cases in three drivers: unification, innovation, and reuse.

- Unification: helps the common understanding between assessors and manufacturers, but also between stakeholders in different domains. Provides a faster assessment process and a safer product by increased understandability. These are the business cases related to unification:
  - **Avionics**: Unification and update of the process and requirements
  - **Automotive**: Marketing Improvement

- Innovation: will be based on cross-over effects between application domains and applying theoretical knowledge in practice. Dependent on the innovation, it will result in a faster assessment process, a safer product, etc. These are the business cases related to innovation:
  - **Avionics**: Better view on verification and validation data, and traceability
  - **Railway**: Better view on relation between requirements and system
  - **Automotive**: Maximise safety and minimise safety-related business risks and costs
  - **Automotive**: Decrease Number of Claims

- Reuse of the assessment data of already approved systems or system component. From a development perspective, we expect the OPENCOSS platform to minimize development activities where possibilities, time and cost by facilitating the reuse of components. This also holds for the certification perspective in the reuse of assessment information, possibly even across domains. These are the business cases related to reuse:
  - **Avionics**: Avoid complete recertification of suppliers’ multi-function subsystems
  - **Railway**: Delta-assessment offers a competitive knowledge advantage for assessors
  - **Railway**: Avoid complete recertification for products entering another country market

These drivers are confirmed in the business case context description of the Business Canvas Model view on OPENCOSS. The value propositions all have these drivers in common.

For all of these business cases we have demonstrated what the aggregated safety business process looks like in a BPMN, and how the stakeholders involved benefit from the future OPENCOSS platform and community by identifying the value exchange and the added value for each stakeholder. Moreover, we see an increased reach and richness for the safety assessment business. Reach is defined in the BOAT framework as the parties with whom the (e-)business can exchange objects. Reach for assessors increases
in that OPENCOSS lowers the (cost) threshold for new manufacturers to enter the safety critical system market, especially the component suppliers.

Richness of an e-business, according to BOAT, is determined by the intensity of the communication between parties. Richness increases since existing safety cases will be a new source for cost reduction in the next safety assessment both for manufacturers as for assessors. The ability of reuse will also improve the transparency and understanding of the safety cases and the safety critical systems themselves, therefore contributing to an increased richness as well.

The stakeholder goals and needs can be roughly divided into direct and indirect stakeholders. The direct ones are the users directly interacting with the system. Most of them represent the organisations like the (component) manufacturers and the assessors. The indirect stakeholders are merely residing in the regulating organisations. Both stakeholder goals and needs are in the line of the identified business cases.

The OPENCOSS business cases provide enough support to claim that the future OPENCOSS platform has, from a business perspective, a clear and feasible goal.
8 Appendix: Commonalities

All domains are different, but also share commonalities. This chapter will address the most significant commonalities relevant for OPENCOSS.

The general safety business processes that can be defined on basis of the domain specific processes in Chapter 5 is depicted in Figure 24. This figure describes a general process model of a safety assessment on a high level of abstraction. In it, we can identify 2 stakeholders, namely the OEM and the component supplier. Furthermore, we can identify 2 processes running in parallel. The first describing the (software) development process was is commonly described in literature. The second process describes the verification and validation or certification activities. The level of abstraction used leaves out back-edges. This is done for readability only. This generalized process model describes the activities that are common to all three (and potentially even more) domains.

Furthermore, Section 4 also holds various customized models of the same process but in railway, avionics and automotive.

Avionics deviates from the generalized model only in that there are additional safety certification activities present. Each component supplier is supposed to undergo a safety certification on equipment level. The OEM needs to undergo a safety certification on airplane level.

In the railway domain, we see a model that is very much like the model of avionics. The difference lies in the fact that on the component supplier’s side, there is a safety assessment instead of a certification.

Differences between the avionics, railway, and automotive domain are most prominent in the automotive case. There the assessment of safety is not regulated by an authority of some sort, but is handled in tailor made contracts between manufacturers wherein they assess each other’s work. The overall process still stands in which assessments are focused inwards.

8.1 Cross domain business processes

In Figure 24, we see the general business process of the safety assessment for all domains described in the BPMN (business process modelling notation). The model aims at identifying the consecutive process steps in safety assessment. The most basic functions are depicted here that are at least present in all domains. In two swim lanes a vehicle manufacturer (OEM – upper swim lane) and the component supplier (lower swim lane) are depicted. The component supplier is included to show the implications for component or subsystem implementation within the complete product development.
Figure 24: General safety assessment business process

Figure 24 also includes the double V-lifecycle model in which both the manufacturing processes (requirements, design, development, tests) and verification and validation processes are contained. The latter is depicted in the top process line for both the OEM as for the component supplier. Note that only the good weather process is described, exceptional situations are omitted for the sake of simplicity and understandability of the figure. The figure shows only the process flow and does not include information streams. For example information from Safety Plan to Requirements and from Requirements to Hazard/Risk Analysis, are not included to avoid clogging up the figure.

Additionally an example feedback loop is included in Figure 24 after the last safety assessment; this demonstrates that the safety assessment has a filter function, where either the product is assessed as acceptably safe or as having the opportunity to improve the product on safety. In Figure 24 an assessment that has detected faults results for example in re-analysis of the subsystems. In most cases, however, a safety assessment with negative outcome will have repercussions in both V-model cycles: the product development and the verification and validation of the product.

The main standard is the cross domain (and therefore less specific) standard IEC 61508. For all domains there is a specific-domain-translation which is based on this standard.

Generalized cross domain business cases:

1. **Reuse** of safety assessments or certificates from other systems or domains. In line with the OPENCOSS’ mission, the reuse of assessment data is one of the most interesting business opportunities to make the safety assessment process faster and, therefore, less costly.  
   *Impact: faster process*

2. **Unification** of terms and concepts for a better understanding of safety and improved safety in systems. Unification will also make the process faster as the understanding of how safety is
translated into system design will become faster.

*Impact: improved safety*

3. **Innovation** in product safety and process by selecting the best of breeds of all domains.

*Impact: improved safety and faster process*

Concerning cross domain certification, three business cases were identified. These business cases have not been elaborated to a complete business model canvas nor did we provide the e³ value models. Reason for that is the lack of real data and experience in the cross domain field at this moment. Appendix D provides an example scenario for a cross domain application.

Even though differences are present, in general, there is much communality between the domains. In all domains, the goal is to create safe products. The assessment of safety and quality in general is known to all domains as is shown in Section 4.

Lastly, as mentioned in Section 5.9, the business cases of the domains also share common interests: minimizing development time and costs while maximizing reuse of components and delta-assessment making for much communality between the domains.
9  Appendix: Abbreviations and Definitions

9.1  Abbreviations

AA  Airworthiness authority
AMC  Acceptable Means of Compliance
ASIL  Automotive Safety Integrity Level
BPMN  Business Process Model Notation
CAA  Civil Aviation Authority (UK)
CAAC  Civil Aviation Administration of China
CoP  Community of Practice
EASA  European Aviation Safety Agency
EMC  Electromagnetic Compatibility
EMI  Electromagnetic Interference
ERA  European Railway Agency
EuroNCAP  European New Car Assessment Programme
FAA  Federal Aviation Administration
IAC-AC  Interstate Aviation Committee – Aviation Register
IMA  Integrated Modular Avionics
ISA  Independent Safety Assessor
OEM  Original Equipment Manufacturer
RAMS  reliability, availability, maintainability, and safety
SOI  Stage Of Involvement
TC  Type Certificate
TRL  Transport Research Laboratory
V&V  Verification and Validation

9.2  Definitions

Acceptable Means of Compliance (AMC)
Acceptable methods and procedures that an applicant may use to show compliance with the applicable requirements.

Application domain
The domain in which certain types of safety critical systems are constructed and that need to have a safety assessment. For example, the application domains included in OPENCOSS are: avionics, railway, and automotive, but also other application domains like health, nuclear power plants, chemistry, etc.

Certification credit
Acceptance by the airworthiness authority that a process, product, or demonstration satisfies a certification requirement.

Certification dossier
Set of evidences provided by the applicant for showing compliance with the applicable requirements.

Domain
See application domain.

Integrated Modular Avionics (IMA)
Shared set of flexible, reusable, and interoperable hardware and software resources that, when integrated, form a platform that provides services, designed and verified to a defined set of safety and performance requirements, to host applications performing aircraft functions.
**Stage of Involvement (SOI)**

Required review point between the airworthiness authority and the applicant.

**Safety case**

The work products, argumentation, evidences necessary for a successful safety assessment

**Type Certificate (TC)**

Written approval issued by the airworthiness authority recognising that the design of an aeronautical product complies with the applicable regulations. “Aeronautical product” means an aircraft, rotorcraft, engine, propeller or, for some airworthiness authorities, auxiliary power unit.
10 Appendix: References

[1]  http://e3value.few.vu.nl/, consulted on May 9, 2012,


[9]  Robertson, James, Robertson, Suzanne, Volere template, download at http://www.volere.co.uk.
11 Appendix: Relations between WPs and Deliverables

Initial Proposal

0. OPENCOSS Vision/Business idea
1. Scope
2. (Current) Challenges/Problems
3. Safety Assessment Business Process
4. Stakeholders/Users
5. Glossary
6. General Use Cases

Glue

WP3
Industrial cases, glossary

WP4, WP5, WP6, WP7

WP1, Task 1.1-3

D1.1 Use Case Specific Constraints/Requirements
D1.2a Use Case Specific Business Case(s)
D1.2b (Harmonized) Use Case

WP2, Task 2.1

D2.1a Business Case(s)
D2.1b e3 Value Models
D2.1c User Goals and Needs

WP2, Task 2.2

D2.2a Business Requirements
D2.2b High Level User Requirements
D2.2c Extra-Functional Requirements

T2.3/4
Validation
WP9
Exploitation

WP1, Task 1.1-3

Specific

WP2, Task 2.1

General

WP2, Task 2.2

Refined

WP4, WP5, WP6, WP7

Detailed User Requirements
System/Software Requirements
12 Appendix: a BOAT framework\textsuperscript{9} view on OPENCOSS

12.1 Introduction

Looking at OPENCOSS as a safety oriented e-business will intensify the view on new business opportunities through ICT-technology. We therefore introduce a framework aimed at supporting e-businesses: the BOAT framework. There are, however, still some aspects in the certification business, like manufacturing safety critical hardware, which do not necessarily share the e-business characteristics. Therefore, we also describe the business cases with a popular general business model: the Business Model Canvas, described in Section 4.3. We will include the central safety aspect of OPENCOSS as much as possible into these approaches, as they do not have this focus specifically incorporated. It must be noted that the safety aspect and related trust issues make it harder to quantify any of the exchanged values.

12.2 Phases of the BOAT framework

Developed by prof. Paul Grefen, the BOAT framework \textsuperscript{3}integrates several development stages into one spiral model. BOAT is aimed to develop new e-business, businesses that are characterized by a strong technological drive and that need a number of cycles to fully understand and profit from the interaction between business and technology.

BOAT is an acronym consisting of the four consecutive development stages or aspects: Business aspect, Organisation aspect, Architecture aspect, and Technology aspect (BOAT). The last step is followed by a review of the earlier steps in order to see the impact of the previous choices and to increase the added value of the business proposition; it requires a continuous business development. If used rigorously, BOAT can support opening up completely new business opportunities and a big change in existing market value chains.

In OPENCOSS we have made a first iteration through business, organisation, architecture, and technology aspects already. The OPENCOSS DoW describes most of the aspects quite clearly from business goals, to architecture and technology solution directions. In this document we analyse the business to a more refined level, taking the existing aspects into account.

The BOAT framework defines a number of concepts in which the business is described: parties, objects, and time scope.

There are three types of e-business parties:

- Business party (B) is a commercial organization of any size and any type, ranging from a multinational to a one-person company;
- Consumer party (C) is an individual acting as a private person, not on behalf of a business or government;
- Government party (G) is part of a government organization or a related non-commercial organization.

Any initiator-responder combination can be made to characterize the different aspect, from business to business (B2B initiator-responder combination), to government to consumer (G2C).

\textsuperscript{9} We thank prof. Paul Grefen for his lecture and explanation on the BOAT framework in context of OPENCOSS
In OPENCOSS the interaction between business and government (B2G and G2B) plays a crucial role. Although consumers will not play a direct role in the OPENCOSS platform, the safety issue reaches the elementary concerns of consumers in a profound way.

There are five types of business goods or objects that can be exchanged between the e-business partners:

- Physical goods: tangibles physically exchanged between parties, divided in discrete goods and bulk goods;
- Digital goods: intangibles electronically exchanged between parties, divided into content (copies), information (on demand produced informational data), and software;
- Services: activities that one party specifically performs for another party, either physical or digital;
- Financial goods: sums of money or guarantees to provide money in the future;
- Hybrid objects: a combination of the object classes above.

Four types of time scopes in the e-business collaboration scenarios:

- static: e-business collaboration is long-lasting, or even permanent;
- semi-dynamic: e-business collaborations are changed periodically, but not on the basis of individual orders;
- dynamic: e-business collaborations are determined for each individual e-business order;
- ultra-dynamic: collaborations are changed during the execution of an individual e-business order.

Note that these types can be applied to any of the aspects in the business framework: business, organisation, architecture, and technology.

### 12.3 Business aspect

The business aspect describes the business goals of e-business. It explains existence of a scenario, access to new markets, reorientation of interaction with customers, and leverage of efficiency levels.

Electronic business is conducting inter-organizational core business activities in dynamic collaborations, such that these activities are enabled by the integrated use of information technology for both communication and processing of information. The key issues the BOAT framework describes in the business aspect are in terms of business drivers (reach and richness), reorganisation in business chains, business directions, and business structures (See Figure 25).

![Figure 25: Business aspects for e-business models (the BOAT framework)](image-url)
12.3.1 Reach and Richness

Reach and richness describe the main business drivers for e-businesses. Reach is defined as the parties with whom the e-business can exchange objects. There are three types of reach: geographical reach where I can exchange objects), temporal reach (when), and modal reach (through which channels).

The richness of an e-business scenario is determined by the intensity of the communication between parties. Richness is determined by the bandwidth, like frequency, level of interactivity, and level of detail. Also the choice of media, plain text as opposed to virtual reality, or the level of customization.

In OPENCOSS both reach and richness are business drivers. The reach is increased by the fact that the accessibility for manufacturers, small and medium enterprises in particular, will be increased. By reducing costs and efforts for safety assessments, more companies will be able to introduce (certified) safety critical systems in the market.

By supporting unification of safety cases, and by storing reusable decision history of safety cases, both claims and evidence, for assessors and manufacturers, relationships between manufacturers and assessors will be enriched, becoming richer. Assessments will be more transparent, portable to other assessors, and faster because unnecessary re-work can be avoided.

Assessors and regulators will be able to set a clear standard of what is required in demonstrating an acceptable safety standard, they will also be able to react faster in detecting unsafe designs and implementations.

12.3.2 Reorganisation in business chains

There are two main changes in business chains: disintermediation and reintermediation. Disintermediation is removing a link from a business chain using e-business technology. Typical examples in e-business are markets where the brokers or retailers are replaced by web shops of the wholesales industry. The removed link often has an intermediary function between producer and consumer. Figure 27 shows disintermediation; deleting one activity in the business chain.
The OPENCOSS platform typically applies disintermediation for the safety assessments where reusable parts allow for skipping activities of the assessment work.

Reintermediation involves inserting a new link into a business chain using e-business technology. The new link often has an intermediary function like a broker in an electronic market. An example of intermedialtion is the letsbuyit.com (beginning of 2000) where consumers united their product wishes to get a discount from product vendors. Figure 28 shows reintermediation in an abstract way.

The OPENCOSS business case shows a typical case of reintermediation. By introducing the OPENCOSS platform, it introduces an extra service for developing safety cases in a uniform way. A new service that enables a better structured way of working, a unification, and a way to be able to reuse parts of the safety case in future safety assessments.

12.3.3 Business direction

Business directions are (new) ways to conduct business from the viewpoint of one party. Examples of important directions could be: true on-time and online capability, enriched customer relationship management, integrated bricks and clicks, multi-channel business design, completely automated business, time-compressed business. The latter is, by introducing safety case reuse, the business direction of OPENCOSS.

12.3.4 Business structures

Business structures are (new) ways to organize the collaboration of parties in a scenario. Important structures could be demand chains, dynamic partnering, highly dynamic supply chains, or dynamic service outsourcing. OPENCOSS offers a service to provide a uniform and reusable safety case.

12.3.5 Business model

The business model summarizes the observations made on the different items of the business aspect in the BOAT framework. The business model for OPENCOSS is depicted in Table 5.
Table 5: OPENCOSS’ BOAT Business model

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Categories</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties</td>
<td>B2B, B2G</td>
<td>G2B is also possible</td>
</tr>
<tr>
<td>Objects</td>
<td>Digital goods</td>
<td>Safety case, arguments, evidence</td>
</tr>
<tr>
<td>Time scope</td>
<td>Static/semi-dynamic</td>
<td>More companies will be able to certify their safety critical systems Stored and reusable safety cases will enrich the relationships and results in repeat sales.</td>
</tr>
<tr>
<td>Drivers</td>
<td>Increasing reach</td>
<td>Increasing richness</td>
</tr>
<tr>
<td></td>
<td>By reintermediation enabling disintermediation</td>
<td>Unification of safety cases and enabling reuse allows for skipping (part of) the certification of already assessed (complete/sub)systems.</td>
</tr>
<tr>
<td>Directions</td>
<td>Time compressed business</td>
<td>Time advantage through reuse of safety cases. Increased safety is a second important direction.</td>
</tr>
<tr>
<td>Structure</td>
<td>Uniform and reusable safety cases.</td>
<td></td>
</tr>
</tbody>
</table>

The business model canvas (from the business model generation) describes the overall context of the business case in Section 4.3.

12.4 Organization aspect

The organization aspect describes how organizations are structured and connected to achieve business goals. It includes business processes and business functions. The organisational aspect is further elaborated in the e³ Value Models in 4.4.

12.5 Architecture aspect

The architecture aspect covers the conceptual structure of automated information systems used to enable organisational structures. It includes information system structures between organizations, within organizations. The architecture aspect will be fully covered in deliverable 2.3: Design of the OPENCOSS platform architecture.

12.6 Technology aspect

The technology aspect describes the technological realization of the systems of with architectural structures. The technology aspect describes software, languages, communication protocols, and hardware. This subject is covered in the implementation of work packages 4 to 7, dealing with the common safety assessment meta model (in WP4, also known as the common certification language), Compositional Certification (WP5), evolutionary evidential chain (WP6), resp. Transparent Certification and Compliance-Aware Process (WP7).
13 Appendix: A Business Model Canvas view on OPENCOSS

13.1 History

In 2004, Alexander Osterwalder developed an approach to business model ontology and described this in his dissertation. Together with his supervisor he wanted to sell the idea, the business model generation, to the world. He was, however, unhappy with the traditional idea to write ‘just’ a book about his new innovation technique. Together, they decided to apply their own technique to their venture and aim to distinguish themselves from the countless strategic and management books being published each year. Their strategy: develop a visual and practical book together with a large number of co-creators who provide over 200 cases of business models. At the same time, these co-creators form, a large marketing force to promote the book based on their intrinsic motivation.

13.2 The Canvas

The business model canvas (Business Model Generation - Alexander Osterwalder et al. [4]) can summarize all the business-related concept descriptions in the right business context. In addition to the BOAT framework, the Canvas includes the value proposition, cost structure, and revenue streams. Together with the BOAT framework and e³ value models, the canvas covers all business aspects and the details to analyse the business case. The Canvas summarizes these results in one overview.

The Business Model Canvas is a strategic management template for developing new or documenting existing business models. It is a visual chart with elements describing a firm's value proposition, infrastructure, customers, and finances. It assists firms in aligning their activities by illustrating potential trade-offs. An overview of all these aspects is depicted in Figure 29.

The building blocks of the Business Model Canvas consist of:

1. Customer segments
2. Value proposition
3. Channels
4. Customer relationships
5. Revenue streams
6. Key resources
7. Key activities
8. Key partners
9. Cost structure
13.3 Customer segments

Customers are the heart of the organisation. This building block defines the different groups of people or organisations that the business wants to reach with the product they offer. It is relevant to define different groups if the offered value needs to be a separate one, either in content, (consumption) channel, relationships, profitability, or different groups are willing to pay for certain aspects of the objects.

For the OPENCOSS platform the different customer segments (not exhaustive) will be:

- Manufacturers, where there could be a distinction between safety or quality managers, requirements engineers, developers, testers, internal safety assessors.
- Independent safety assessors
- Regulators
- System designers and integrators
- End users/customers
- Standards organisations
- European Union

The target markets are European companies involved in development, advice, and assessment of safety critical systems. The OPENCOSS project does not necessarily limit itself to the three domains specified above, but these domains will have a higher priority, since the knowledge about these domains is abundantly present with the OPENCOSS partners.

These customer segments or stakeholders are defined in more detail in Section 0
13.4 Value proposition

The building block value proposition describes the bundle of products/objects and services that creates value for the customer segments. It is the reason that customers prefer one business over another. The value proposition provides value through various elements such as newness, performance, customization, getting the job done, design, brand/status, price, cost reduction, risk reduction, accessibility, and convenience/usability.

In the OPENCOSS platform, the value proposition is unique. If the project succeeds in creating a platform capable of reusing (parts) of safety cases, there probably is no other competitor that provides a service similar to this. The downside of the OPENCOSS value proposition is that the market segments must be prepared to invest in creating safety cases in a new environment. The first customers to evaluate the value proposition will be amongst the OPENCOSS partners, which makes the threshold for newcomers lower.

13.5 Channels

The building block ‘channels’ describes how the business is communicating with its customers. These channels have different functions, like creating awareness about the products/objects offered, determining the value proposition in negotiations, buying products, delivering products, provide value proposition to the customer, as well as customer support.

The OPENCOSS platform will communicate mainly over the internet (or intranet) and per customer segment through a separate channel.

13.6 Customer relationships

In order to optimize operations and reduce risks of a business model, organizations usually cultivate buyer-supplier relationships so they can focus on their core activity. Complementary business alliances also can be considered through joint ventures, strategic alliances between competitors or non-competitors.

To ensure the survival and success of any business, companies must identify the type of relationship they want to create with their customer segments. Various forms of customer relationships include:

- Personal Assistance: Assistance in a form of employee-customer interaction. Such assistance is performed either during sales, after sales, and/or both.
- Dedicated Personal Assistance: The most intimate and hands on personal assistance where a sales representative is assigned to handle all the needs and questions of a special set of clients.
- Self Service: The type of relationship that translates from the indirect interaction between the company and the clients. Here, an organization provides the tools needed for the customers to serve themselves easily and effectively.
- Automated Services: A system similar to self-service but more personalized as it has the ability to identify individual customers and his/her preferences. An example of this would be Amazon.com making book suggestion based on the characteristics of the previous book purchased.
- Communities: Creating a community allows for a direct interaction among different clients and the company. The community platform produces a scenario where knowledge can be shared and problems are solved between different clients.
- Co-creation: A personal relationship is created through the customer’s direct input in the final outcome of the company’s products/services.
For the OPENCOSS platform the relationships could vary from self-service to personal assistance. Dependent on the value proposition and the customers’ willingness-to-pay, the future OPENCOSS community could be similar to the RedHat company providing personal assistance services on Linux; a new company could provide the services for the OPENCOSS platform. But it could be that the OPENCOSS platform does not provide enough added value to transcend the concept of an open source community.

13.7 Revenue streams

If the customers are the heart of the business, revenue streams are the arteries of the business. An important question for the revenue stream is: what is the willingness-to-pay of each customer segment for the products offered. There are two kinds of revenue streams: transaction based and revolving funds. A finer division is:

- Asset Sale - (the most common type) Selling ownership rights to a physical good. i.e. Wal-Mart
- Usage Fee - Money generated from the use of a particular service i.e. UPS
- Subscription Fees - Revenue generated by selling a continuous service. i.e. Netflix
- Lending/Leasing/Renting - Giving exclusive right to an asset for a particular period of time. i.e. Leasing a Car
- Licensing - Revenue generated from charging for the use of a protected intellectual property.
- Brokerage Fees - Revenue generated from an intermediate service between 2 parties, i.e. broker selling a house for commission
- Advertising - Revenue generated from charging fees for product advertising.

For the OPENCOSS platform the revenue streams can be related to direct services, subscription fees, licensing, and brokerage fee. Analysis of the situation will point out the necessity for the choice of revenue stream(s).

13.8 Key resources

The building block ‘key resources’ describes resources that will be required to create value for the customer. They are considered an asset to a company, which are needed in order to sustain and support the business. These resources could be human, financial, physical and intellectual.

The key resources for the OPENCOSS platform will be:
- The software of the platform and its interfaces to the tools of the users,
- The experts working with the platform and providing content for it,
- Developers and maintenance staff for the platform to solve problems or to extend functionality,
- The content of the platform: standards and interpretation of the standards.

13.9 Key activities

The most important activities in executing a company's value proposition. For the OPENCOSS platform this would mean that it offers a service to support safety assessments. This also means that this service and the software necessary for the service, needs to be maintained.

13.10 Key partners

The key partners are the partners that will provide the knowledge, basic functionality, social networks, for the platform to run smoothly. Partnerships can be formed using strategic alliances, co-optation (a co-
operation between competitors), joint ventures, and direct buyer-supplier relationships to secure product deliveries.

For the OPENCOSS platform the key partners are most certainly the manufacturers. They are customer and supplier at the same time. Their developers might contribute to the open source community directly, they definitely will share their requirements for the platform. Manufacturers will also benefit directly from the time (and cost) reduction because of a faster safety assessment.

For the same reason assessors can be regarded as key partner. As independent players in a competitive market, it is important for them to follow the latest developments and to stay ahead in the competition. Faster safety assessments would increase their service value considerably. Also assessors will be able to provide valuable requirements for the platform.

Furthermore, the OPENCOSS project consortium is a very good starting point to create new key partners.

### 13.11 Cost structure

This describes the most important monetary consequences while operating under different business models.

For the OPENCOSS platform, maintenance of the platform, both in hardware and software, will probably be the biggest part of the cost structure. Dependent on the customer relationship, personal assistance or consultancy could get an expensive second part.

### 13.12 The resulting Canvas

Figure 30 shows general Business Model Canvas for OPENCOSS.

![Figure 30: The Business Model Canvas for OPENCOSS](image-url)

- **Key Partners**
  - Partners in 3 domains
  - Standards organization
  - Tool provider

- **Key Activities**
  - Safety assessment support
  - Maintenance on platform

- **Key Resources**
  - The software platform
  - The experts providing content
  - Developers for maintenance
  - Content platform

- **Value Propositions**
  - For reuse: Much faster safety assessment process (30-40% faster)
  - Safety improvement expected.
  - Investment in new way of working.
  - For the offered value proposition a personal assistance relationship should be feasible.

- **Customer Relationships**
  - Equipment/Component provider
  - System manufacturer

- **Channels**
  - Platform will be an intra- or internet site

- **Cost Structure**
  - Maintenance and personal assistance results in biggest costs
  - Usage fee, licensing for standards.
Appendix: $e^3$ value model elicitation steps

The elicitation steps are based on the $e^3$ value business ontology approach. From http://e3value.few.vu.nl/docs/bibtex/pdf/EarlyReqDet2006.pdf we learn that:

To clarify early business requirements, a process of elicitation is needed that starts from initial business ideas and subsequently details them and evaluates their consequences. The methodology used for this process consists of a series of steps to be performed by business developers. It is a specialization of the general design process. Parts of this process were done in the form of short workshops and interviews with executives, while the more detailed modeling and evaluation activities were carried out as desk studies by industry researchers, business developers or strategy analysts. The latter are usefully supported by the developed $e^3$ value tool for business modeling, whereas communication with managers is clearly facilitated by the visual diagram format of the networked business models. The major steps in this process are as follows:

Step 1: Business Idea Description. Stakeholders are asked to concisely state their business idea. In workshops we employed a description template to state the idea in structured natural language. This template covers (1) a one-liner presenting the essentials of the idea, (2) a statement of scope (e.g. for the region is of importance), (3) the core business processes that are required for the idea, (4) the main enterprises (actors) involved, (5) potential and IT equipment/components that may be required for the idea, (6) the ownership of equipment (ideas often require investments), and (7) regulatory incentives (as some ideas lean on subsidy schemes).

Step 2: Goal Selection. In this step, stakeholders representing various enterprises are asked to specify the goals a particular business idea may serve. To aid the goal specification process, we have constructed two taxonomies of long-term strategic goals and short-term operational goals, respectively. In each case study, our research partners have selected strategic goals from the predefined taxonomy, and the lists of goals per stakeholder were then used to negotiate goals in case of conflicts. There are in this industry sector strategic goals such as environmental ones that relate to society in general (e.g. reduction of greenhouse gas emissions such as CO2); often governments promote such goals. Operational short-term goals contribute to reaching strategic goals, such as Market development (M), Environment (E) or Quality and efficiency of supply (QE).

Step 3: Technology Selection. Understanding goals is important to select suitable technology and to construct a value model. To help stakeholders with technology selection, we developed two redefined tables to select from. The first table is an industry-specific taxonomic hierarchy of technologies and their characteristics, the second is a score matrix whether and to what extent specific technologies assist in reaching listed goals. This step is clearly industry-specific and must be driven by domain experts, although we believe that technology characterization tables and goal-technology matrices are practical instruments of wider applicability.

Step 4: Value Model Design. To construct a value model, stakeholders decided what value activities should be carried out for a specific business idea. Additionally, value interfaces of activities are stated. These interfaces may be compared to wall outlets for electric power: they state what a particular activity or actor offers of economic value to other actors. Our methodology supported this step of constructing a value model by providing modelling guidelines as well as libraries of predefined value activities and value interfaces specific to the domain. To assist in the allocation of value activities to actors, we developed a matrix of frequently occurring assignments. For example, some assignments of activities can be fixed by regulatory frameworks (often stated by country law) to a specific actor. For instance, a long distance electricity Transport activity is in some countries legally assigned to one specific actor, usually called the Transmission System Operator (TSO). This step is of crucial importance in clarifying business requirements related to a value proposition, as it clarifies in detail which actors are involved for what activity and what
their mutual relationships are. The e³ value modelling tool is helpful here in checking whether the value model is well formed, i.e., complies with the set of business rules that underlie the ontology, and by giving corresponding modelling suggestions in the style of a CASE tool.

Step 5: Financial sustainability evaluation. To assess the financial sustainability of a business idea, net value flow estimates based upon the value model from the previous step are calculated by means of a spreadsheet approach. First, the important operational scenarios are identified; they may be identified from the business process narratives produced in Step 1. Stakeholders then decide on valuation functions for value objects representing money (often fees). For example, a pricing formula has to be given, e.g. the price per kWh for electricity. If we estimate these valuation functions, as well as other variables in the model, the e³ value tool automatically calculates all net cash flows for each actor involved (the tool generates Excel spreadsheet results on a per actor basis). In a network of actors, such calculations are way too complex to be handled manually. This part of the evaluation shows whether the actors benefit from a business model, under assumed normal operating conditions.

Step 6: Sensitivity Evaluation. Many financial parameters in a business model are difficult to estimate or are expected to change. So, a final step is to identify possible future events that may influence the business case positively or negatively, and evaluate this influence by means of financial parameter sensitivity analysis. The basis for this part of the evaluation are what-if or evolutionary scenarios, in a way similar to scenario-based strategic decision making (Van Heijden 1996).

Such events may influence valuations or even the structure of the value model itself. Evolutionary scenarios considered in the business model studies often relate to changing regulations, changing fuel prices, and exhausting fossil fuels in different rates than expected. We have experienced that ‘playing’ with the financial parameters to test the robustness of a business model against a range of possible future conditions is of much more value to stakeholders than relying on the numbers themselves. It can be seen as the stress testing of a business model idea; if it passes these tests, it helps to convince managers of the potential of the idea and increases their confidence that it will actually work.
15 Appendix: European projects related to OPENCOSS

Assessment and Certification Rules for Digital Architecture
The project dealt with safety assessment of system architecture for interlocking computers in distributed railway networks. As a result, ACRuDA defined a common method and common criteria for assessment of such architectures. They are applicable to all currently implemented digital architectures.
In relation to OPENCOSS, ACRuDA results correspond to techniques that could be used for provision of evidence for safety certification in the railway domain. The project can be a possible beneficiary of OPENCOSS, and its tools could also be used as external tools whose artefacts could be stored in the WP6 infrastructure.

The project aimed to coordinate the study of resilience measuring and benchmarking in computer systems and components, addressing the strategic objective “Secure, dependable and Trusted Infrastructures”.

ARM aims to facilitate communication, in a structured way, of how systems and services meet assurance requirements. It also allows interchange of structured arguments between diverse tools by different vendors. For these purposes, ARM provides a metamodel for specifying structured arguments. The metamodel represents the core concepts for structured argumentation that underlie a number of existing argumentation notations. Each ARM instance represents the argument that is being asserted by the stakeholder that is offering the argument for consideration.

ARTIST - http://www.artist-embedded.org
The project aimed at integrating topics, teams, and competencies, through an ambitious and coherent research programme of research activities that were first grouped into four topics in ARTIST 1 (modelling and validation; software synthesis, code generation, and timing analysis; operating systems and networks, and; platforms and multiprocessor system-on-chips) and later into seven in ARTIST2 (modelling and components; hard real-time; adaptive real-time; compilers and timing analysis; execution platforms; control for embedded systems, and; testing and verification)

ASSERT - http://www.assert-project.net/
The Automated proof-based System and Software Engineering for Real-Time systems.
ASSERT focusses on aerospace application domain and ESA leads the project. The main objective of the project is to introduce a new methodology to aerospace system development, based on modeling and on preservation of system properties from design down to the code.

Certification Together - http://www.certification-together.com
The project deals with certification challenges in the avionics domain and offers training and expert consulting services. For example, such services aim to help companies to gain knowledge about avionics safety standards (ARP 4754, DO-178B...), perform gap analyses, and prepare documentation for certification audits. In addition, Certification Together provides user groups, seminars and conferences.

CEMSIS - http://www.cemsis.org/
The aim of the project is to maximize safety and to minimize cost of refurbishments of control and instrumentation Systems Important to Safety (SIS). The project has developed guidance to help achieve this aim while making use of contemporary commercial technology (e.g. COTS) and developing a set of approaches that build towards common practices within the EU.
**CESAR - http://www.cesarproject.eu/**
Cost-efficient methods and processes for safety relevant embedded systems
The three transportation domains automotive, aerospace, and rail, as well as the automation domain share the need to develop ultra-reliable embedded systems to meet societal demands for increased mobility and ensuring safety in a highly competitive global market.
To maintain the European leading edge position in the transportation as well as automation market, CESAR aims to boost cost efficiency of embedded systems development and safety and certification processes by an order of magnitude.
CESAR pursues a multi-domain approach integrating large enterprises, suppliers, SME's and vendors of cross sectoral domains and cooperating with leading research organizations and innovative SME's.

**CHESS - http://chess-project.ning.com/**
The project sought to improve Model Driven Engineering practices and technologies to better address safety, reliability, performance, robustness and other extra-functional concerns while guaranteeing correctness of component development and composition for embedded systems.
The CHESS methodology for the development of critical real-time systems is based upon a model driven engineering approach, whereby the central artefacts of development are models rather than documents or code. It is a demanding approach that requires comprehensive tool support for all aspects of the development process.

**CRITICAL STEP - http://www.critical-step.eu**
The CRITICAL Software Technology for an Evolutionary Partnership (CRITICAL STEP)
The project aims at establishing the basis for a long term strategic research collaboration between partners involved in this project in the growing and challenging domain of software for large-scale Safety-Critical Systems (SCSs) based on the use of Off-The-Shelf (OTS) software components for the control of complex distributed infrastructures such as Air Traffic Management (ATM) systems, complex industrial plants, etc.

**DECOS - http://www.decos.at/**
The project dealt with reuse of pre-validated hardware and software components and functional blocks for both design and certification purposes, including safety certification. The domains that DECOS addressed were automotive, aerospace and control applications.

**DITSEF - www.ditsef.eu/**
Digital & Innovative Technologies for Security & Efficiency of First responder operations
The project aims at increasing the effectiveness and safety of First Responders (fire fighters, police) by optimal information gathering and sharing with their command levels.

**eDIANA - http://www.artemis-ediana.eu/**
Embedded Systems for Energy Efficient Buildings
The project addresses the need of achieving energy efficiency in buildings through innovative solutions based on embedded systems. The eDIANA Platform is a reference model-based architecture, implemented through an open middleware including specifications, design methods, tools, standards, and procedures for platform validation and verification.

**EDONA**
This project started in 2007 and finished in 2010, and was developed in France. It goal was to develop an open platform for development of embedded systems in the car industry that integrated different tools.
The EDONA platform integrated components, tools and gateways to develop automotive software systems. It has a layered architecture, some of them based on Eclipse or AUTOSAR.

**EVOLVE - http://www.evolve-itea.org**
Evolutionary Validation, Verification and Certification.
The aim of the EVOLVE project is "The creation of a methodological framework for early verification and validation of evolutionary products through the accredited/certified integration of each iteration and/or component in a MDE (Model Driven Engineering) context."

FACIT-SME - http://www.facit-sme.eu
The FACIT SME project targets to facilitate the use of Software Engineering (SE) methods and to systematize their application in IT SMEs. It will provide methods for efficient and affordable certification of these processes according to internationally accepted standards. Furthermore, it will help the SMEs to share best practices, tools and experiences with development partners and customers. ICT SME communities (organized by associations) will experience significant benefit through the exchange of recent knowledge and best practices.

Flanders’ DRIVE - http://www.flandersdrive.be/
Company dealing with the development of competences for the automotive industry with a focus on innovation in products and processes.

GENESYS - http://www.genesys-platform.eu/
GENeric Embedded SYStem Platform
The project aimed at developing a cross-domain reference architecture for embedded systems that meets the requirements and constraints of the ARTEMIS strategic research agenda (composability, networking and security, robustness, diagnosis and maintenance, integrated resource management, evolvability and self-organization). The reference architecture provided is domain-independent and serves as a template that can be instantiated to concrete platforms for individual application domains (i.e., automotive, avionic, industrial control, mobile, consumer electronics).

HYBRIDGE - http://www.csl.mech.ntua.gr/Projects/Hybridge/
Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design
The objective of HYBRIDGE is to develop the methodologies to control system designs for safety critical operations which are embedded within sound safety management systems such that the level of safety stays under control of humans, and to demonstrate their use in support of advanced air traffic management design.

iFEST - http://www.artemis-ifest.eu/
Industrial Framework for Embedded Systems Tools
The project aims at specifying and developing an tool integration framework for HW/SW co-design of heterogeneous and multi-core embedded systems.

INTERESTED - www.interested-ip.eu
Interoperable Embedded Systems Toolchain for Enhanced Rapid Design
The project aims at development of suites of interoperable design tools for rapid design and prototyping. Namely creating a reference and open interoperable embedded systems tool-chain, fulfilling the needs of the industry for designing and prototyping embedded systems.

MAENAD - http://www.maenad.eu/
Model-based Analysis & Engineering of Novel Architectures for Dependable Electric Vehicles
This project wants to deal with the new complex power management and optimization algorithms that are needed to ensure high performance, range of travel and low energy consumption to Fully Electric Vehicles (FEV). The challenges faced in the engineering of FEV are already partly met by EAST-ADL2, an emerging
automotive architecture description language (ADL) compliant with AUTOSAR, and that EAST-ADL2 is the appropriate vehicle for fully meeting these challenges.

**MBAT - [http://www.mbat-artemis.eu](http://www.mbat-artemis.eu)**

Combined Model-based Analysis and Testing of Embedded Systems

The project deals with the development, integration and delivery of high-quality products in the transportation domain, such as aircraft, cars and trains. More concretely, MBAT focuses on V&V of embedded systems.

MBAT will provide Europe with a new leading-edge Reference Technology Platform for effective and cost-reducing validation and verification, focusing primarily on the transportation domain, but also to be used in additional domains.

**MICIE - [http://www.micie.eu/](http://www.micie.eu/)**

**Aim:** to establish a Critical Infrastructure Warning Information Network (CIWIN), aimed to design and implement a so-called “MICIE alerting system” able to identify, in real time, the level of possible threats induced on a given CI by "undesired" events happened in such CI and/or other interdependent CIs. In particular, whenever such events occur, the MICIE alerting system supports the CI operators providing them with a real time risk level.


More Integrated Systems Safety Assessment

The project aims to develop methods and tools to help safety engineers to collect, navigate, and manage information, structure their arguments, express their ideas, and most importantly find solutions to problems in an efficient, auditable and exhaustive way.

**ModelME! - [http://modelme.simula.no/](http://modelme.simula.no/)**

Its purpose was to identify, tailor, and improve software engineering best practices for integrated software-dependent systems in the maritime and energy sector. The ultimate goal was to enable safe continued growth of advanced functionality based on software.

ModelME! defined a metamodel to ensure compliance with IEC 61508. The plan in OPENCOSS is to reuse as far as possible the taxonomy of evidences and refine it, as well as the process and tools released in this project.

**Modelplex - [http://www.modelplex.org/](http://www.modelplex.org/)**

MODELPLEX has three major objectives:

- Develop an open solution for complex systems engineering improving quality and productivity;
- Lead its industrialization;
- Ensure its successful adoption by the industry.

**MODSafe - [http://www.modsafe.eu/](http://www.modsafe.eu/)**

Modular Urban Transport Safety and Security Analysis

The purpose of the MODSafe project is to undertake research of major steps of the Safety Life Cycle of urban guided transport systems in Europe.

**MOGENTES - [http://www.mogentes.eu/](http://www.mogentes.eu/)**

Model-based Generation of Tests for Dependable Embedded Systems

It aimed to significantly enhance testing and verification of dependable embedded systems by means of automated generation of test cases. It addressed both testing of non-functional issues such as reliability (e.g., by fault injection) and functional safety tests, meeting the requirements of standards such as IEC61508, ISO26262, or AUTOSAR.
MOMOCs - http://www.momocs.org/
MOMOCs aims at studying a methodology and related tools for fast reengineering of complex systems. A complex system is characterized by an interconnection of hardware, software, user interfaces, firmware, business and production processes.

MULTIFORM - http://www.multiform.bci.tu-dortmund.de/
Integrated Multi-formalism Tool Support for the Design of networked Embedded Control Systems. It focuses on development, integration and interoperation of techniques and provision of coherent software tools for the integrated design of the control of large and complex networked systems. The key contribution of the project towards the goal of integrated model-based control systems design is the connection of tools that support the design of different layers of the control hierarchy and on different levels of abstraction.

NEXT TTA - http://www.vmars.tuwien.ac.at/projects/nexttta/
High-Confidence Architecture for Distributed Control Applications
The NEXT TTA project enhances the structure, functionality and dependability of the time-triggered architecture (TTA) to meet the austere cost structure of the automotive industry, while satisfying the rigorous safety requirements of the aerospace industry.

OPEES - www.opees.org
Open Platform for the Engineering of Embedded Systems
Aim: to settle a community and build the necessary means and enablers to ensure long-term availability of innovative engineering technologies in the domain of dependable / critical software-intensive embedded systems.

Open-DO - http://www.open-do.org/
The project aims at building a community around certification-oriented free software tools and libraries. In particular, it provides a forge and a visible portal to host such tools and libraries. Open-DO is being developed in the context of safety certification according to DO-178C. It deals with:
- Continuous certification
- Qualifiable open source tools and certifiable components
- Making development of safety-critical system accessible

PARSEC - http://www.parsec-project.fr/
The PARSEC project aims at defining a development environment for critical distributed embedded systems requiring certification according to strict standards such as DO-178B (avionics) or IEC61508 (transportation) or Common Criteria for Information Technology Security (information systems security). The projects approach is to provide developers of these systems with an integrated tool suite that tackles the specific challenges related to these systems.

RECOMP - http://atc.ugr.es/recomp/
"RECOMP" stands for Reduced Certification Costs Using Trusted Multi-core Platforms
The aim is establish methods, tools and platforms for enabling cost-efficient (re-)certification of safety-critical and mixed-criticality systems. Applications addressed are automotive, aerospace, industrial control systems, and lifts and transportation systems.
ReSIST - [http://www.resist-noe.org](http://www.resist-noe.org)
The project was undertaken in a form of a network of excellence that addressed the strategic objective “Towards a global dependability and security framework” of the European Union Work Programme, and responded to the stated “need for resilience, self-healing, dynamic content and volatile environments” in the context of ubiquitous computing and ambient intelligence.

This initiative corresponds to OMG ARM specification. SAEM and ARM comprise SACM. SAEM establishes the necessary fine-grained models of evidence elements required for detailed compliance and risk analysis. The structure of the SAEM provides the basis for logical design of easily-constructed tools for storing, cross-referencing, evaluating, and reporting the elements of evidence for systems during the software assurance process. This specification provides a schema for collecting, developing, evaluating, communicating, and managing software assurance evidence.

SAFE - [http://safe-project.eu](http://safe-project.eu)
Safe Automotive soFtware architEcture
The project will speed up the efficient development of safety features in cars. The objective is to extend the AUTOSAR architectural model, enhance methods for defining safety goals and define development processes complying with the new ISO 26262 standard for functional safety in automotive electrical and electronic systems.

SafeCer - [http://www.safecer.eu/](http://www.safecer.eu/)
Safety Certification of Software-Intensive Systems with Reusable Components.
SafeCer is targeting increased efficiency and reduced time-to-market by composable safety certification of safety-relevant embedded systems.

The project dealt with nuclear power plant safety, including certification facilities for software. In this area, SAFIR 2010 aimed to define the necessary software certification services for nuclear industry needs, mainly focusing on process assessment and product evaluation. The services actually corresponded to the collaboration (and information) needs of several stakeholders. Conditions defined for the services were the application of diverse expertise and the application of effective evaluation tools.

Self Management for Large-Scale Distributed Systems based on Structured Overlay Networks and Components.
A major innovation of SELFMAN is to combine the strengths of structured overlay networks and advanced component models. Structured overlay networks originate in peer-to-peer applications, but have matured to provide strong guarantees and efficient communication and storage operations. They reorganize themselves to maintain these properties in a changing environment, which is already a low-level self-management property. Advanced component models provide introspection, reflection, and dynamic reconfiguration abilities, which give the hooks needed for an application to manage itself. SELFMAN will reformulate the overlay network as part of a self-managing component architecture and use it to support high-level self-managing services.

Its overall objective was to develop a means of using BBNs to reason about the safety of programmable electronic systems. This objective achieved by developing a method, the SERENE Method, for representing programmable electronic systems safety arguments using a BBN and by enhancing an existing BBN tool
with features needed to support the method. The project also provided a manual that contains procedures for identifying and structuring evidence that a system meets the safety requirements of IEC61508.

It aimed at enhancing security and dependability for AmI ecosystems by capturing security expertise and making it available for automated processing. SERENITY provided a framework supporting the automated integration, configuration, monitoring and adaptation of security and dependability mechanisms for such ecosystems.

**SESAMO**
This project will start in 2012 and finish in 2015. SESAMO will study the root causes of problems arising with convergence of safety and security in embedded systems at architectural level. These problems result in subtle and poorly understood interactions between functional safety and security mechanisms. This hinder system definition, development, certification, and accreditation procedures and standards. The proposed solution is to develop a component-oriented design methodology based on model-driven technology, which will jointly address safety and security aspects and their interrelation for networked embedded systems in multiple domains (automotive, aerospace, energy, mobile medical, and metropolitan rail transport).

**SHARE - http://www.share-project.eu**
The SHARE project aims to facilitate open source software code sharing and utilization within the embedded system domain, creating a nurturing environment for applications and solutions to be developed on OSS middleware, and paving the way for new business models and services.

**SHIP**
The overall objective of SHIP was to devise a means of assessing, ideally numerically, the achieved reliability or safety of a system in the presence of design faults, and thus to improve industrial practice for safety assessment. SHIP investigated a range of software engineering techniques for minimizing and estimating (design) failures to see if they could be applied to industrial plants, and developed a safety case approach.

**SPEEDS - www.speeds.eu.com**
The Speculative and Exploratory Design in System Engineering European project
The main objective of SPEEDS is to define end-to-end methodologies, processes and supporting tools for embedded-system design
SPEEDS defines a heterogeneous rich-component (HRC) (meta)model and a mathematical structure that allow engineers to soundly compose heterogeneous subsystems. A contract-based design supports such a heterogeneous composition.

**T-CREST - http://www.t-crest.org/**
The T-CREST will research and develop tools and build a system that prevents pauses by identifying and addressing the causes for possible pauses. The T-CREST time-predictable system will simplify the safety argument with respect to maximum execution time striving to double performance for 4 cores and to be 4 times faster for 16 cores than a standard processor in the same technology (e.g. FPGA). Thus the T-CREST system will result in lower costs for safety relevant applications reducing system complexity and at the same time faster time-predictable execution.

**VERDE - http://www.itea-verde.org/**
Validation-driven design for component-based architectures
It aims to improve the V&V activities of real-time embedded systems. Currently, these activities often start only when implementation and integration is completed; the consequence is that many major issues, often
related to the architecture and introduced early in the process, are not found until integration and validation stages of the product lifecycle. As a result, the issues are more difficult and more expensive to fix. While preserving the V&V cycle, VERDE aims at promoting a more iterative and incremental approach to software development that will be driven by the early V&V activities.

**VIKING - [http://www.vikingproject.eu](http://www.vikingproject.eu)**
Vital Infrastructure, Networks, Information and Control Systems Management
The main objectives of VIKING are:
- To investigate the vulnerability of SCADA systems and the cost of cyber attacks on society
- To propose and test strategies and technologies to mitigate these weaknesses
- To increase the awareness for the importance of critical infrastructures and the need to protect them

The objective of this project is to achieve a framework for the introduction of safety related fault tolerant electronic systems without mechanical backup in vehicles (so-called "x-by-wire systems").
16 Appendix: The Volere Stakeholder Template

The following is the generic template used by OPENCOSS in the stakeholder identification and analysis work reported in Section 6.2

<table>
<thead>
<tr>
<th>Stakeholder Class</th>
<th>Stakeholder Name</th>
<th>Classes of Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The template includes columns for Stakeholder Class, Stakeholder Name, and Classes of Knowledge. The template is designed to identify the roles of stakeholders and their knowledge classes.
17 Appendix: a cross domain high level scenario

OPENCOSS USE CASES FROM POV OF OPENCOMRTOS

17.1 Purpose of scenario

The intention of this scenario is to provide high-level cross domain description for the OPENCOSS Platform. This scenario has been derived from consideration of a potentially reusable component – the OpenComRTOS – which has been developed by Altreonic [5] [6]. The OpenComRTOS was developed using formal methods, so, from the OPENCOSS point of view, some potentially reusable assurance evidence artefacts do exist, in the form of the formal verification of the RTOS. The scenario presented here focuses on how the OPENCOSS Platform can support reuse of this component and its associated assurance evidence both within and across safety-critical domains. Although it is intended to highlight some of the issues inherent in the assurance of real-time systems, it should be stressed that the scenario is conceptual. It expresses at a very general level, and do not derive a priori from any known use of the OpenComRTOS itself.

17.2 Background: The OpenComRTOS

The OpenComRTOS [5] was developed to support real-time operations in embedded systems in safety-critical domains. Such systems are typically ‘hard’ real-time systems, in that missing a task deadline can result in a total system failure. Conventional RTOS are either designed for deployment on a single processor or in systems characterised by shared memory resources. The OpenComRTOS, however, is explicitly designed to exploit modern distributed processor architectures: it is developed on a network-centric model, which assumes that each processor has a local memory and that the supporting hardware permits and secures communication between the distributed memory resources [5], while preventing this where necessary (i.e. maintaining partitioning between applications as required). The OpenComRTOS supports concurrent programming in this distributed environment, in such a way as to be transparent to the application developer: the system handles the mapping between of tasks and entities and deals with routing and system-level communication so that application source code can remain independent of the topology of the target system [5]. The RTOS is developed in ANSI-C and is thus highly portable: it is scalable to a range of target systems, from very small systems with a single microprocessor to widely-distributed networks comprising large numbers of distributed processing nodes [6]. OpenComRTOS supports the reuse of applications across varied platforms, by recompiling and remapping the source code without the need to modify the code itself, independently of the underlying processor architecture, from 8-bit to 64-bit CPUs [5]. The RTOS can be extended with the addition of application-specific services and entities without the need for redevelopment of the RTOS kernel or the development of an additional middleware layer [5].