ECSEL Research and Innovation actions (RIA)

AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

Business cases and high-level requirements D2.1

Work Package:	WP2 Reference Architecture and Integration
Dissemination level:	PU = Public
Status:	Final
Date:	09 February 2018
Responsible partner:	Benito Caracuel (Schneider Electric)
Contact information:	Benito.caracuel@schneider-electric.com
Document reference:	AMASS_D2.1_WP2_TLV_V1.0

PROPRIETARY RIGHTS STATEMENT
This document contains information, which is proprietary to the AMASS 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 AMASS consortium.

This deliverable is part of a project that has received funding from the ECSEL JU under grant agreement No 692474. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and from Spain, Czech Republic, Germany, Sweden, Italy, United Kingdom and France.

Contributors

Names	Organisation
Benito Caracuel	Schneider Electric
Huáscar Espinoza, Alejandra Ruiz, Garazi Juez	Tecnalia Research & Innovation
Petr Böhm	AIT Austrian Institute of Technology
Stefano Puri	INTECS SPA
Barbara Gallina, Inmaculada Ayala, Mustafa Hashmi	Mälardalen University
Jose Luis de la Vara, Jose Maria Alvarez, Eugenio Parra	Universidad Carlos III de Madrid
Luis Maria Alonso, Borja Lopez	The REUSE Company
Anna Carlsson	OHB Sweden
Carlo Vertua	Thales Italia SPA
Thierry Lecomte	ClearSy SAS
Frank Badstübner	Infineon Technologies AG
Javier Herrero Martín, Elena Alaña Salazar	GMV Aerospace and Defence, S.A.U.
Tomáš Kratochvíla	Honeywell Internacional SRC
Bernhard Winkler, Robert Bramberger	Virtual Vehicle
Marc Born	Ansys medini Technologies AG

Reviewers

Names	Organisation
Fabien Belmonte (Peer Reviewer)	ALSTOM Transport SA
Detlef Scholle (Peer Reviewer)	ALTEN Sverige Aktiebolag
Mohamed Bakkali (Peer Reviewer)	Alliance pour les Technologies de L' Informatique
Jose Luis de la Vara	Universidad Carlos III de Madrid
Cristina Martínez	Tecnalia Research & Innovation

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

The AMASS project is developing an integrated and holistic approach and supporting tools for assurance and certification of Cyber-Physical Systems (CPS). AMASS plans to achieve the mentioned approach by creating and consolidating the first European-wide open certification/qualification platform, ecosystem and community spanning the largest CPS vertical markets. In order to keep a consistent and cohesive vision, WP2 Reference Architecture and Integration shall focus on a common set of requirements derived from WP1 Case Studies and Benchmarking and the state of the practice from the technical work packages (WP3-WP6).

The work described here is the result of a systematic analysis and the capture and formulation of meaningful business models of the AMASS solutions. The work has paid special attention to capture the needs of different types of stakeholders including tool vendors, embedded systems developers, integrators, component suppliers, certification entities, governmental agencies, regulation bodies, and standardization bodies. The business models have been described based on the application domain: industrial automation, automotive, railway, avionics, space, and air traffic.

This document also includes the formalization of functional and non-functional requirements to be met by the technical AMASS work packages, including legal constraints, security and reliability requirements. Requirements have been developed by using input from the industrial case studies (WP1) and the DX.1 technical deliverables, where X is 3 to 6 [1][2][3][4].

This deliverable was planned to include the requirements to be covered throughout the project lifetime, i.e. across different implementation iterations. Anyway, in case a new requirement appears, it will be included in the technical work packages' deliverables and a reference to this document will be created.

Finally, this document will be the input for the implementation tasks in the technical work packages (T3.3, T4.3, T5.3 and T6.3).

1. Introduction

The AMASS Reference Tool Architecture (ARTA) is intended to be a reference in the area of CPS assurance and certification. It is an open architecture with no constraints on the implementation. It plans to be a solution to provide a customizable assurance assets management infrastructure to support assurance activities along the CPS development lifecycle.

The AMASS Platform Basic Building Blocks are the result of merging existing technologies from OPENCOSS [5] and SafeCer [7], and other related project such as CHESS [6]. These building blocks include tools for specification of system component and specification of assurance cases such as structured argumentation trees, evidence management, and compliance management. In addition to these, the basic building blocks include user access management and data management tools, as well as the Common Assurance and Certification Metamodel (CACM).

CACM is an evolution of OPENCOSS CCL (Common Certification Language) and SafeCer metamodels, as they will be merged during the AMASS project. CACM is implemented as a structured semi-formal language, which will act as a meta-model for assurance and certification specification. This meta-model will be used to capture assurance knowledge and we able to store this information in a structured database. Using a common conceptual language for different application domains and assurance activities will also enable management of certification assets in a common format, sharing patterns of technology and architecture, and cost-effective re-use between different domains and standard frameworks.

Supported on the basic building blocks, AMASS will work on four (4) pillars, which correspond to specific project Scientific and Technical Objectives (STOs). Their purpose can be summarized as follows:

- ***Architecture-Driven Assurance (STO1):*** Explicit integration of assurance and certification activities with the CPS development activities, including specification and design, which provides support for the system components composition in accordance with the domain best practices and guarantee that emerging behaviour does not interfere with the whole system assurance.
- ***Multi-concern Assurance (STO2)***: Tool-supported methodology for the development of assurance cases, co-assessment and contract-based assurance, which addresses multiple system characteristics (mainly safety and security, but also other dependability aspects such as availability, robustness and reliability).
- ***Seamless Interoperability (STO3)***: Open and generically applicable approach to ensure the interoperability between the tools used in the modelling, analysis, and development of CPS, among other possible engineering activities (in particular, interoperability from an assurance and certification-specific perspective, and collaborative work among the stakeholders of the assurance and certification of CPS).
- ***Cross/Intra-Domain Reuse (STO4)***: Provide consistent assistance for intra-and-cross-domain and/or cross-concern reuse, based on a conceptual framework to specify and manage assurance and certification assets.

Figure 1 provides a high-level picture of the AMASS Reference Tool Architecture (ARTA):

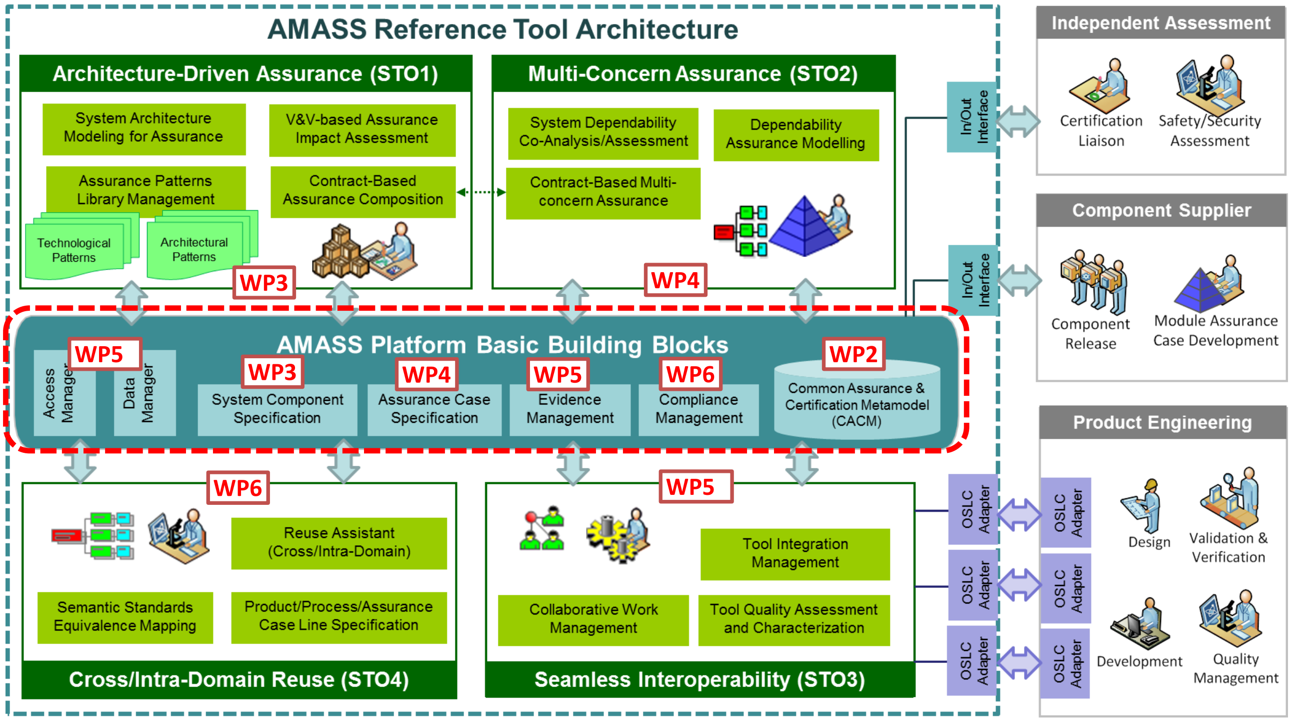

AMASS Reference Tool Architecture
Architecture-Driven Assurance (STO1)
System Architecture Modeling for Assurance
V&V-based Assurance Impact Assessment
Assurance Patterns Library Management
Contract-Based Assurance Composition
Technological Patterns
Architectural Patterns
WP3
Multi-Concern Assurance (STO2)
System Dependability Co-Analysis/Assessment
Dependability Assurance Modelling
Contract-Based Multi-concern Assurance
WP4
AMASS Platform Basic Building Blocks
WP5
Access Manager
Data Manager
WP3
System Component Specification
WP4
Assurance Case Specification
WP5
Evidence Management
WP6
Compliance Management
WP2
Common Assurance & Certification Metamodel (CACM)
WP6
Reuse Assistant (Cross/Intra-Domain)
Semantic Standards Equivalence Mapping
Product/Process/Assurance Case Line Specification
Cross/Intra-Domain Reuse (STO4)
WP5
Tool Integration Management
Collaborative Work Management
Tool Quality Assessment and Characterization
Seamless Interoperability (STO3)
In/Out Interface
In/Out Interface
OSLC Adapter
OSLC Adapter
OSLC Adapter
Independent Assessment
Certification Liaison
Safety/Security Assessment
Component Supplier
Component Release
Module Assurance Case Development
Product Engineering
OSLC Adapter
OSLC Adapter
OSLC Adapter
Design
Validation & Verification
Development
Quality Management

Figure 1. AMASS Reference (High-Level) Architecture

This deliverable introduces the basic definition of the AMASS Reference Tool Architecture. Firstly, section 2 analyses and formulates the business models of the AMASS solutions for several domains (industrial automation, automotive, railway, avionics, space, and air traffic), identifying the value proposition of AMASS and capturing needs of the different stakeholders (tool vendors, embedded systems developers, integrators, component suppliers, certification entities, governmental agencies, regulation and standardization bodies).

Secondly, section Requirements3 defines the high-level functional and non-functional requirements for the technical AMASS work packages. These requirements summarize what results the stakeholders want. Business models and requirements will be the roadmap for the remainder of the project.

Finally, section 4 provides some conclusions about the document.

2. Business Cases

2.1 Introduction

This section is organized as follows. First, we describe the business model canvas, which is a well-known and broadly accepted mechanism to describe the business model of different organizations. Then we describe the business models per domain: industrial automation, automotive, railway, avionics, space, and air traffic.

2.2 AMASS Business Model Canvas

A business model describes the rationale of how an organization creates, delivers, and captures value. The Business Model Canvas is a visual representation to describe and design a business model. It provides a holistic view of the business as a whole and is especially useful in running a comparative analysis on the impact that an increase in investment may have on any of the contributing factors.

In this first stage of the project, the following Canvas represents an initial business analysis about AMASS. A more detailed analysis will be included in task T8.1 “Exploitation”.

The Business Model Canvas is composed by nine building blocks that cover the four main areas of a business (customers, offer, infrastructure and financial viability):

1. **Customer segments**

This block defines the different groups of people or organisations that we want to reach with AMASS. It is relevant to define different groups if the offered value needs to be separated, either in content, (consumption) channel, relationships, profitability, or if different groups are willing to pay for certain aspects of the objects.

In the case of AMASS, we could identify the following customer segments [10]:

- Original Equipment Manufacturers (OEMs): OEM refers to the manufacturer of the original equipment. They are interested in complying with the assurance and certification process for safety-critical items, and in an efficient tool for safety analysis, documentation and certification.
- Component suppliers (manufacturers): Component suppliers are responsible for assuring the critical properties of their delivered products. They are interested in the specification of assurance case modules, transferring certification artefacts across certification for multi-domains, and preserving the integrity of the evidence that they provide to platform integrators.
- Integrators of Safety-critical Platforms: Platform integrators are ultimately responsible for the dependability of the products delivered to the end users of the consumer market. They are interested in the composition of the assurance safety case based on individual modules, ensuring the integrity of the evidence passed through the supply chain and interested in tools that support these processes.
- Consulting and Service Providers: Consulting and service providers support OEMs, component suppliers, and integrators of safety-critical platforms during the assurance process. They are interested in the integrity of the evidence passed through the supply chain.
- Certification Organizations: Certification organizations support OEMs, component suppliers, and integrators of safety-critical platforms regarding assessment during the assurance lifecycle. They are interested in intra/cross-domain and multi-concern assurance.
- Tool Vendors: Tool vendors support both platform integrators and component suppliers, and they facilitate the exchange of relevant information between all supply chain and certification stakeholders. They are interested in interoperability with existing tools and ensuring that all the information relevant for the tool development is available.

- Policy Makers and Standardization Groups: the policy makers represent stakeholders for standardization and regulatory bodies. They are interested in the assurance and certification process.

2. Value proposition

This block describes the value proposition that AMASS would provide for the customer segments. It is the reason why 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.

The value proposition identified for AMASS would be the following:

- Efficiency and effectiveness: efficiency is a relationship between results achieved and resources used. Effectiveness is the ability to achieve excellent results regardless of the used resources. In the context of AMASS, efficiency and effectiveness are provided by:
  - Introducing safety/security concerns in the early phases of product development in order to reduce costs
  - Introducing safety/security co-assessment
  - Reducing efforts and costs for managing compliance with targeted standards
  - Reducing efforts and costs for safety/security assurance and certification
  - Reducing efforts to run safety/security analyses
  - Improving the safety/security demonstration (completion, quality, communication, acceptation)
- Scalability: is the ability to be effective, efficient and predictable while the size of the certified product or process increases. In the context of AMASS, scalability is provided by:
  - Reusing of assurance results for product upgrades and re-certifications
  - Reducing the risk for new developments/certifications
- Interoperability: is the ability to work with other systems or products. In the context of AMASS, interoperability is provided by:
  - Reducing efforts and costs related to the co-existence of heterogeneous tools and tool-chains

3. Channels

The Channels block refers how AMASS is accessible to its customers. The medium through which AMASS provides its value proposition is the channel. These channels could have different functions, such as creating awareness about the product offered, determining the value proposition in negotiations, buying products, delivering products, provide value proposition to the customer, as well as customer support.

In the case of AMASS, the channel should be accessible, efficient and with the least investment required. In this sense, the appropriate channel for AMASS could be an intranet or internet site.

4. Customer relationships

This block describes the type of relationship that AMASS would create with its customers to ensure the success.

In order to create a successful and sustainable relation with customers, the AMASS experts should assist them during the different processes, such as installation, configuration, etc. In this sense, personal assistance would be suitable to facilitate the integration of AMASS solutions in the customer processes. Another option is to use the AMASS Open Source Community for an interaction with the clients.

5. Revenue streams

This block refers the way to obtain revenues respect to the solution offered to customers.

In this case, the AMASS platform will be available as open source, meaning that the platform will be delivered together with its source code and clients will be able to modify or redistribute it.

The fact that the base platform of AMASS will be available as open source is not only a way to reduce costs by gathering a larger industrial community for development and maintenance of the platform, but also, by disseminating a de facto standard, an enabler of different kinds of business models mainly separated in two categories:

- Proprietary products built on top of the platform with classical revenue streams of selling licenses and support contracts.
- Service offers for users of the AMASS platform, such as support subscriptions, specific development to specialize the platform to a domain or corporate context, and training and consulting to apply AMASS methods and tools to a project.

The main revenue is expected to be from services associated to the platform for specialization and training. On the other hand, libraries of standards and architectural patterns could be a way of revenue if third-party companies sell those models.

6. Key resources

This block describes the resources that would be required to create value for the customer. The resources could be human, financial, physical and intellectual.

The resources needed to provide value to the customers in AMASS would be the AMASS software platform, the engineers for development and maintenance of the platform and the AMASS Open Source Community.

7. Key activities

This building block defines the most important activities that will be needed to offer the value proposition to the customers.

The relevant activities that AMASS needs to offer the value proposition would be the development and maintenance of the platform, the platform technical support to the customers and the maintenance of the AMASS Open Source Community.

8. Key partners

This block describes the external partners that are needed to provide the knowledge, basic functionality, and social networks for the AMASS platform to run without problems.

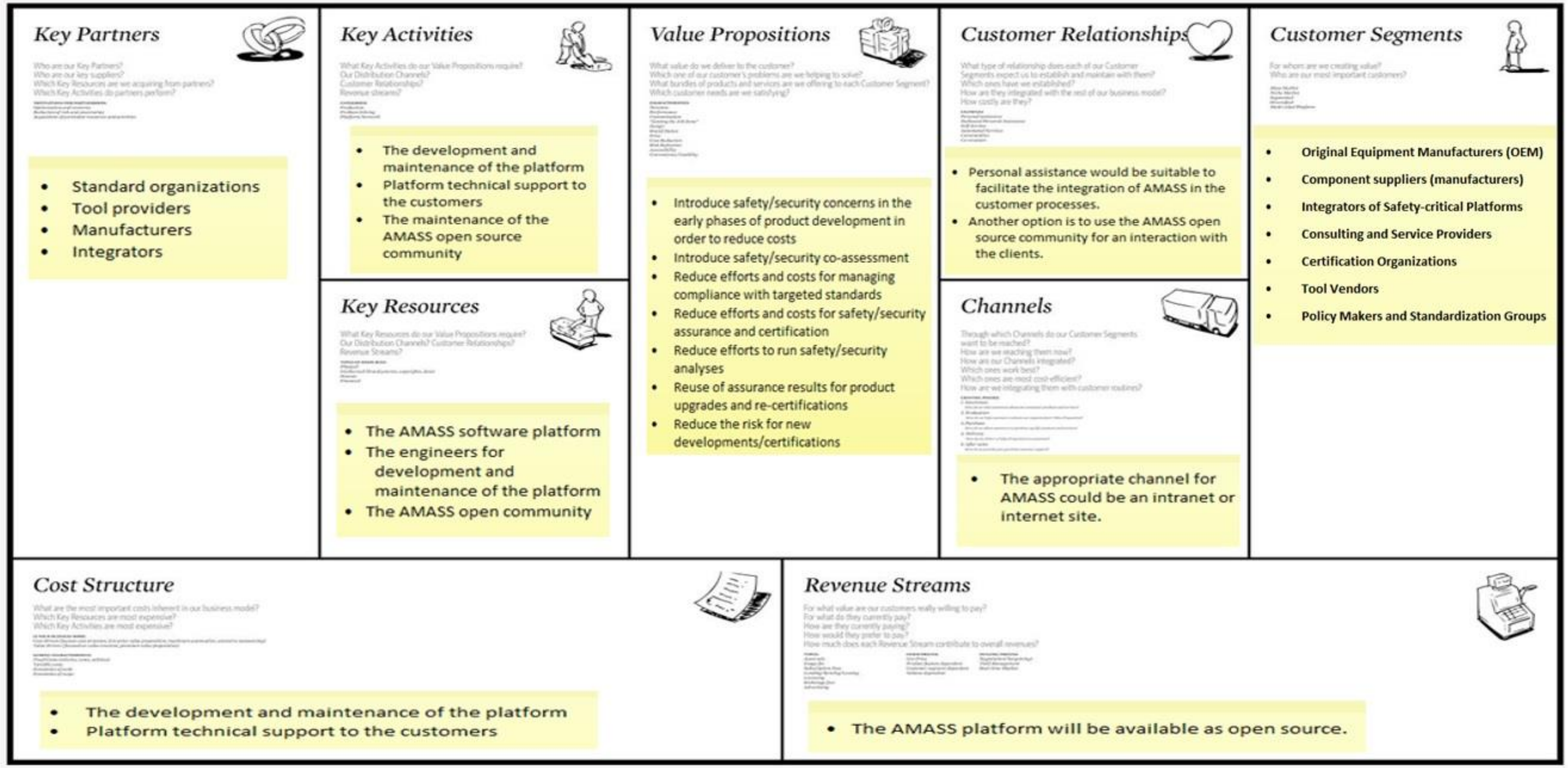
For the success of AMASS, it is needed to collaborate with external partners who complement each other in helping AMASS create its value proposition and reducing risks. In this sense, we could identify the following partners: standard organizations, tool providers, manufacturers and integrators.

9. Cost structure

This block defines the main costs that AMASS platform would incur. It depends on the key partners, key activities and key resources that we have.

The main costs identified for the AMASS platform would be the development and maintenance of the platform and the platform technical support to the customers.

Figure 2 shows the Business Model Canvas for the AMASS platform:



Key Partners

Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acquiring from partners?
Which Key Activities do partners perform?

- Standard organizations
- Tool providers
- Manufacturers
- Integrators

Key Activities

What Key Activities do our Value Propositions require?
Our Distribution Channels?
Customer Relationships?
Revenue streams?

- The development and maintenance of the platform
- Platform technical support to the customers
- The maintenance of the AMASS open source community

Key Resources

What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?

- The AMASS software platform
- The engineers for development and maintenance of the platform
- The AMASS open community

Value Propositions

What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?

- Introduce safety/security concerns in the early phases of product development in order to reduce costs
- Introduce safety/security co-assessment
- Reduce efforts and costs for managing compliance with targeted standards
- Reduce efforts and costs for safety/security assurance and certification
- Reduce efforts to run safety/security analyses
- Reuse of assurance results for product upgrades and re-certifications
- Reduce the risk for new developments/certifications

Customer Relationships

What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
Which ones have we established?
How are they integrated with the rest of our business model?
How costly are they?

- Personal assistance would be suitable to facilitate the integration of AMASS in the customer processes.
- Another option is to use the AMASS open source community for an interaction with the clients.

Channels

Through which Channels do our Customer Segments want to be reached?
How are we reaching them now?
How are our Channels integrated?
Which ones work best?
Which ones are most cost-efficient?
How are we integrating them with customer routines?

- The appropriate channel for AMASS could be an intranet or internet site.

Customer Segments

For whom are we creating value?
Who are our most important customers?

- **Original Equipment Manufacturers (OEM)**
- **Component suppliers (manufacturers)**
- **Integrators of Safety-critical Platforms**
- **Consulting and Service Providers**
- **Certification Organizations**
- **Tool Vendors**
- **Policy Makers and Standardization Groups**

Cost Structure

What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?

- The development and maintenance of the platform
- Platform technical support to the customers

Revenue Streams

For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?

- The AMASS platform will be available as open source.

Figure 2. Business Model Canvas

2.3 Industrial Automation Domain

2.3.1 Introduction

Industrial Automation is the use of information technologies and control systems for managing industrial processes, without significant human intervention. The automation devices include RTU, IED, PLC, SCADA, etc. The industrial automation market tries to improve the performance of the industry, mostly those that rely on high-volume output and process repeatability. These include energy, oil and gas, automotive, food and beverage, metals and materials, packaging, etc.

Few players dominate the global market for industrial automation, namely Schneider Electric, ABB Ltd., Siemens AG, and GE Corporation. Safety aspects are one of the main concerns in this domain due to the increase of the automation system complexity. IEC 61508 “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”, IEC 62061 “Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems” and EN ISO 13849-1 (safety standard which deals with safety-related design principles of employed control systems to establish different safety Performance Levels (PL)) are some of the main standards regarding functional safety in the industrial automation domain.

It has to be mentioned that AMASS focuses in the energy sector within industrial automation domain. To the best of our knowledge, no specific functional safety standard exists in this area, thus IEC 61508 will be considered.

The fact that the distribution network is evolving towards a multidirectional network that requires new automation is a reality. To do so, in recent years, the power system is being equipped with a new generation of intelligent electronic devices (IEDs) increasing availability and power quality in power distribution networks. These devices include sensing capabilities to monitor the status of the grid, predict issue-related network behaviours, and allow a bidirectional communication.

However, these advantages in availability and quality do not come without challenges to overcome. At the core of this technology are microprocessors, DSPs, MCUs and FPGAs. As a result, the correct functioning of the safety-related systems must be ensured as the breakdown and malfunction of IEDs can lead to environmental and material risks or even risk to people. In order to make this happen, the IEC/EN 61508 functional safety standard uses a risk-based approach to determine the safety integrity requirements. A Safety Integrity Level (SIL) is assigned to each safety function, which specifies the risk reduction required for each defined hazardous event.

The same concept applies to cybersecurity. The so-called IEC 62351 “Information Security for Power System Control Operations” is the main reference for cyber security in the electrical substation and covers the cyber security of the electrical infrastructure in several aspects: access control, communications and protocols, even register, and others.

According to Figure 3, certification takes place at three levels: smart grid operator certification, smart grid system integration certification and smart grid component certification [10]. Taking into account that cybersecurity is a daily concern and cyber threats evolve over a time, the lifecycle includes this issue by considering component and system maintenance in the form of the block ‘continuous certification maintenance’.

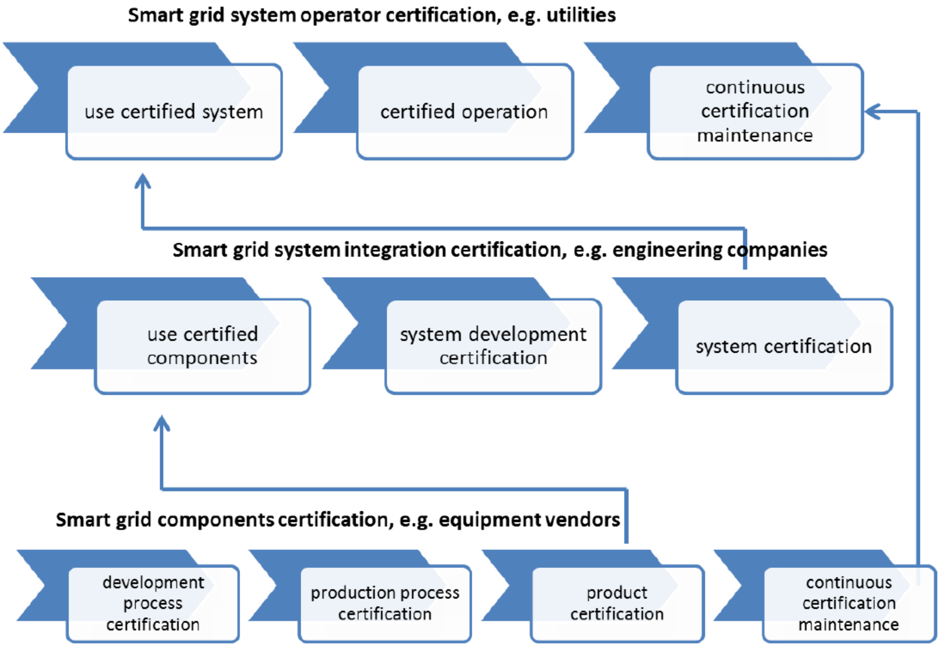

Smart grid system operator certification, e.g. utilities
use certified system
certified operation
continuous certification maintenance
Smart grid system integration certification, e.g. engineering companies
use certified components
system development certification
system certification
Smart grid components certification, e.g. equipment vendors
development process certification
production process certification
product certification
continuous certification maintenance

Figure 3. Smart grid chain of trust [8]

A smart grid is different to standard ICT components in terms of certification due to its system design complexity [8]**¡Error! No se encuentra el origen de la referencia.**. Two of the main reasons behind are the several interconnections on many parts of the system and its geographical distribution. However, they should not affect the chain of trust.

2.3.2 Stakeholders

Manufacturers: these stakeholders include, for example, Original Equipment Manufacturers (OEM) that designs and specifies products under its own company name and brand and system manufacturers. The manufacturers could demand the AMASS platform to integrate the safety aspects in its internal design and development process. Also, these stakeholders could need to comply with the safety standards for the industrial domain (such as IEC 61508) using the AMASS tool for the safety assessment and compliance management. The AMASS tool should help the manufacturer to manage the requirements and the documentation generated for the safety assessment. Technical supporting and maintenance of the AMASS platform is essential for this kind of customers.

Providers: a wide range of providers of components, tools, equipment as well as service providers cover all important business segments in the industrial automation domain. They include, for example, the fields of electrical drive technology, instrumentation and control technology, software for automation, system integration and end-to-end solutions for factory automation. These stakeholders need to comply with safety requirements and must be sure that their components, tools or equipment satisfy the market entry requirements. Also, in some safety critical cases, they could need the approval from the certification authority which certifies that the equipment or tool comply with the regulation. They would benefit from the AMASS platform that helps them to handle the requirements and the safety assessment and certification process.

Consultants and Assessors: safety consultants/assessors have to analyse the activities and processes of different manufacturers and providers. In this sense, these stakeholders would need a platform that adapts to the safety assessment of the diverse customers. The AMASS tool should also help them to reduce and forecast costs, resources and time required for the safety assessment.

Regulators, Certification Bodies and Standard Organizations: these stakeholders concern about the product compliance respect to the standards. In this sense, they would need a platform that supports the standard compliance and certification processes.

2.3.3 Business Process

Based on the definition of usage scenarios provided in D1.1 [9], a number of generalized industrial automation business cases have been defined. By doing so, a certain number of non-resolved issues might be settled bringing additional value to the industrial automation domain. Furthermore, since the following business cases are specified as general statements, they could be applied to the rest of the industrial domains targeted in AMASS:

- BC1: Reduce efforts and costs for managing compliance with IEC 61508 and IEC 62351
- BC2: Reduce efforts and costs to achieve safety and security co-assessment

In these two business cases, AMASS provides value proposition (as mention in section 2.2) to the customers of this domain.

2.3.3.1 BC1: Reduce efforts and costs for managing compliance with IEC 61508 and IEC 62351

Certification according to the IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) and IEC 62351 (Information Security for Power System Control Operations) standards is a growing requirement for manufacturers in the energy industry. The need of demonstrating compliance with legal requirements together with the increasing need to justify that the required functional safety has been achieved is the order of the day. Due to the large set of requirements, the compliance with those standards can be a burdensome task.

The functional safety standard deals with *managing* the risk of both random and systematic failures whereas IEC 62351 details security requirements for power system management and information exchange, including communications network and system security issues, TCP/IP and MMS profiles, and security for ICCP and Sub-station automation and protection.

In order to manage the compliance with the aforementioned standards, tool support will be provided. This implies registration of evidences and managing its evolution, traceability and change impact. Besides, the reuse of assurance/certification dossiers for future projects will be enabled. AMASS tool platform will enable an easier understanding of those industry standards and an easier checking for compliance. One of the main objectives is to reduce the assurance/certification effort by reducing the effort for managing compliance with targeted standards.

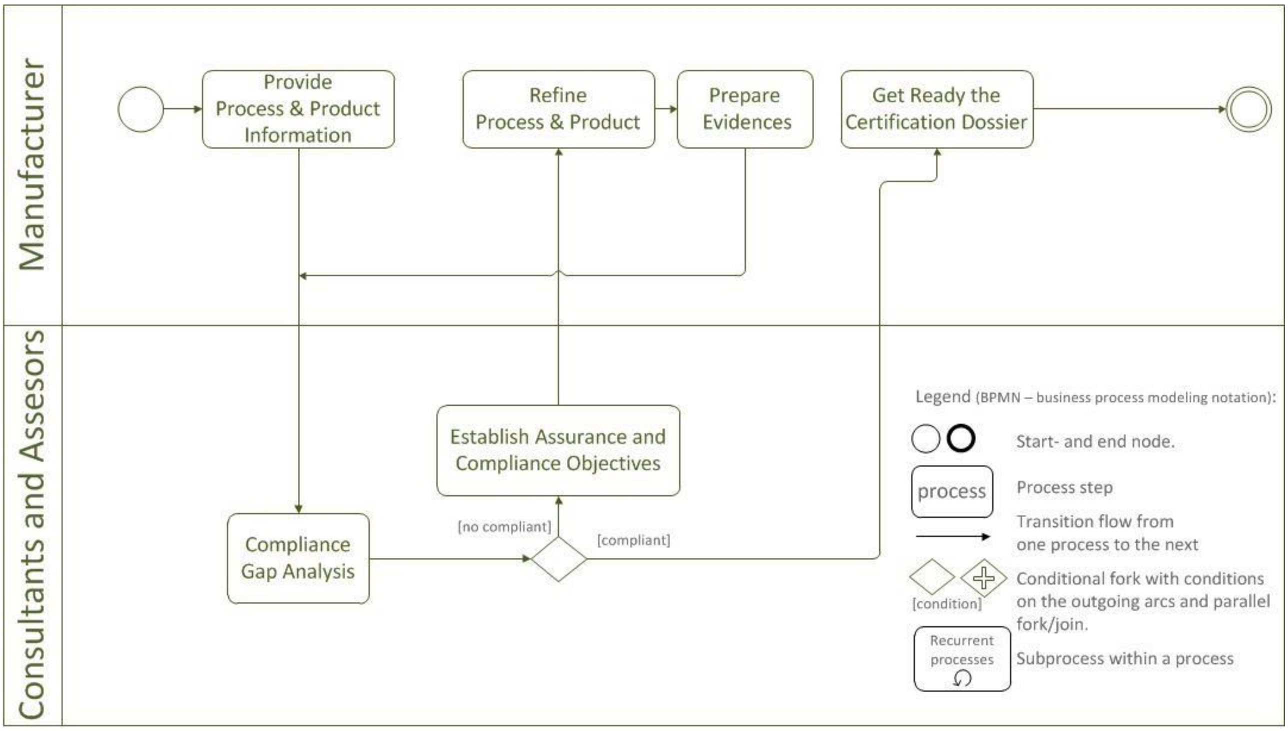

Manufacturer
Consultants and Assesors
Provide Process & Product Information
Refine Process & Product
Prepare Evidences
Get Ready the Certification Dossier
Establish Assurance and Compliance Objectives
Compliance Gap Analysis
[no compliant]
[compliant]
Legend (BPMN – business process modeling notation):
Start- and end node.
process
Process step
Transition flow from one process to the next
[condition]
Conditional fork with conditions on the outgoing arcs and parallel fork/join.
Recurrent processes
Subprocess within a process

Figure 4. Industrial Automation Business Case 1: Reduce efforts and costs for managing compliance with IEC 61508 and IEC 62351

The workflow illustrated in Figure 4 consists of the following steps:

- The (IACS) Manufacturer initiates the project by providing process and product information of the system.
- For that existing product, a Gap Analysis is conducted so the current Safety and Security Integrity Levels can be estimated. If any gaps that need to be filled are discovered i.e. the current product does not comply with a certain predefined safety or security integrity level, then required assurance and compliance objectives will be identified. The manufacturer corrects those gaps by refining the process and product with the necessary process/product measures.
- Once the process and product have been refined according to the previous objectives, evidences are prepared so the consultants and assessors can evaluate them. Afterwards, compliance gap analysis is carried out once again until those objectives are achieved.
- As soon as the product under development is considered IEC 62351 and IEC 61508 compliant for a certain Safety and Security Integrity Level, the certification dossier is prepared and delivered to the certification bodies.

By means of the AMASS tool platform, time, cost and risks of assurance and (re)certification activities safety/security-critical RTUs will be significantly reduced via evolutionary and model-based approaches.

2.3.3.2 BC2: Reduce efforts and costs to achieve safety and security co-assessment by applying model-based development

The safety and security fields have been mostly treated as two different fields so far. Therefore, the need to understand how requirements and measures from one concern may impact the other one is of vital importance. To do so, two main approaches are considered: **unification** versus **integration**. Unification stands for a single methodology where the outcome is a single set of requirements describing safety and security. Conversely, the so-called integration or harmonization approaches investigate the similarities and differences of both concerns and tries to bring them into alignment by producing separate safety and security requirements. Once they are properly defined, the interaction between each other is shown in order to identify possible conflicts.

In the industrial automation domain, we are interested in following the second approach (integration) due to two main reasons:

- Industrial automation technology manufacturing can imply the integration of multiple components involving multiple industrial actors with likely heterogeneous practices,
- Safety and security have different standards, underlying specific processes which can be followed at different stages of the product lifecycle.

Figure 5 summarises the main activities of a typical CPS aggregated safety-security co-assessment process where two core stakeholders are depicted: the manufacturer and the (component) provider. Note that it also includes the system development process because that is closely interlinked with the safety and security co-assessments activities. For example, the safety and security requirements from which they are coming have a direct influence on the product. Also, evidence for demonstrating safety and security are based on the test results of the product. This makes it impossible to look at the safety and security co-assessment without considering the development process.

Another important aspect is that we include the process of the component provider interwoven in the whole system safety-security assessment process, followed by the manufacturer. One of the AMASS goals is to reduce the recurring safety and security assessment efforts for component assurance (which forms a part of the system assessment and certification).

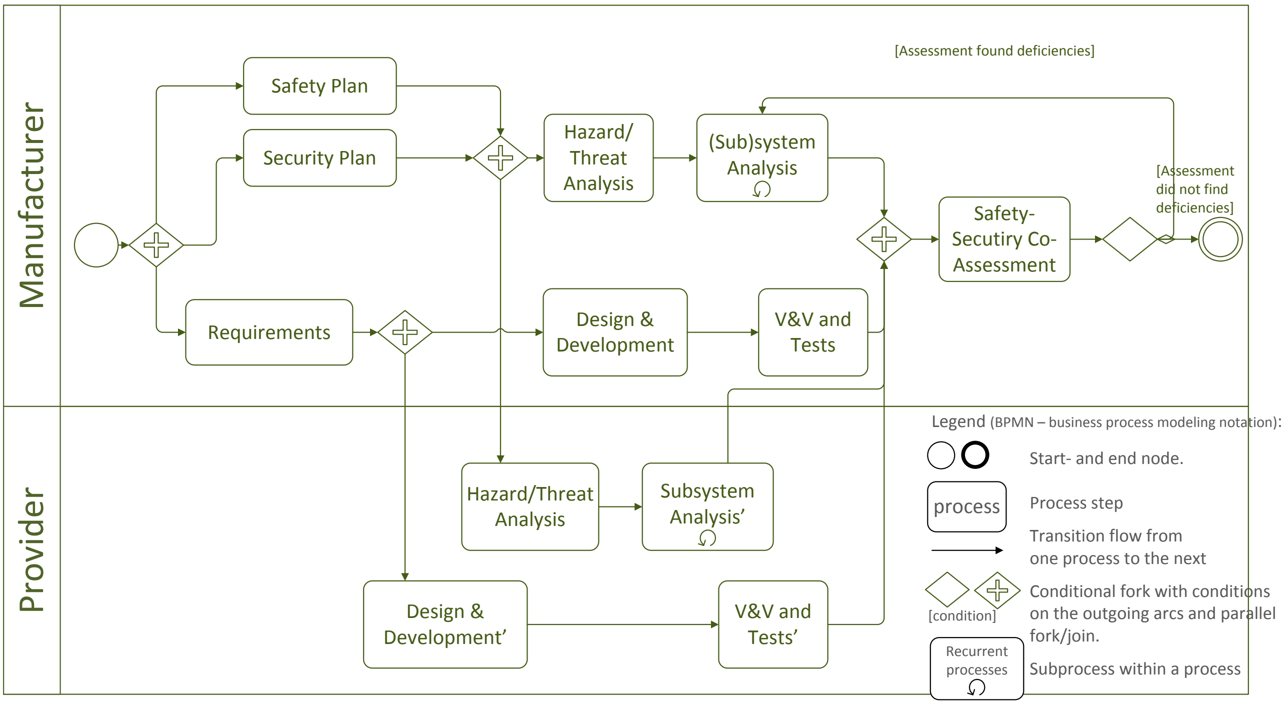

Manufacturer
Provider
Safety Plan
Security Plan
Requirements
Hazard/ Threat Analysis
(Sub)system Analysis
Design & Development
V&V and Tests
Safety- Secutiry Co- Assessment
[Assessment found deficiencies]
[Assessment did not find deficiencies]
Hazard/Threat Analysis
Subsystem Analysis’
Design & Development’
V&V and Tests’
Legend (BPMN – business process modeling notation):
Start- and end node.
process
Process step
Transition flow from one process to the next
[condition]
Conditional fork with conditions on the outgoing arcs and parallel fork/join.
Recurrent processes
Subprocess within a process

Figure 5. Industrial Automation Business Case 2: Safety and Security Co-Assessment

Overall, it should be noted that security assurance practices are less well established in industrial automation domain as compared to functional safety practices. This can be largely attributed to the extremely short period of time that has passed from publication of the security standard (IEC 62351 mentioned above). As a consequence, a comprehensive integration of the functional safety and security analysis is very important and it is currently a challenging issue. However, it also represents a significant market opportunity for the AMASS project in the industrial automation domain, where there is currently a lack of methods and tools that facilitate comprehensive integration of safety and security assessment processes.

The workflow can be summarised as follows:

- The (IACS) Manufacturer initiates the project within AMASS tool platform using guidance and templates provided by the platform. They specify constraints and requirements that must be met by individual providers and, where necessary, additional guidance (incl. templates) for providers.
- The Manufacturer develops the safety and security plans according to the standards recommendations. This includes assurance schemes about policies and standards, safety and security assurance processes and planned artefacts to be released. This is released to the providers in order to design or configure their systems according to the safety and security framework.
- The Manufacturer uses these AMASS templates and techniques for the integration of evidence, justification and associated contextual information and to perform hazard/threat co-analyses. Safety and a security risk analyses are realized separately by safety and security experts: safety-related scenarios are identified based on failure mode analysis and security-related scenarios are identified based on an analysis of threats and vulnerabilities that lead to unsafe states. Then, the scenarios are ranked according to frequency and impact. The two sets of safety and security requirements are next integrated and examined together in order to identify possible interactions. The treatment step addresses the different interactions identified (e.g., conflicting requirements). This step requires collaboration of safety and security experts in order to find solutions that satisfy both sides. New safety and security requirements are considered and interactions are then derived. The system modifications resulting from this first pass may introduce new risks; this is why the process iterates until all interactions are identified and no modifications are needed. Novel methods such as FMVEA (Failure Modes, Vulnerabilities and Effects Analysis) or extended fault trees need to be carried out.
- Having designed the components, suppliers provide safety and security assurance evidence and artefacts associated with individual components to the manufacturer via the AMASS platform. They use generic guidance provided by the platform (including guidance on safety and security co-assessment with the standards) along with the project-specific guidance relayed through the AMASS platform by the manufacturer.
- The integrated system can then be assessed by the Manufacturer (safety-security co-assessment). As the safety and security system views rely on the system architecture model, the required information is extracted (e.g. function interactions, ports and their links, data…) from the architecture model and an initial safety and security views are set up in AMASS tools. Starting from this, safety and security engineers enrich their respective views by adding safety and security dysfunctional behaviour. These two views are then combined to produce a multi-assurance model of the designed system. We can then validate the safety and security properties. If a property is violated (assessment finds deficiencies), the engineers can iterate again to identify the best way to correct the system or subsystem architecture.

The main expected impacts from this business case are to:

- Introduce safety/security concerns in the early phases of product and components development in order to reduce costs.
- Reduce efforts to run safety-security analyses.

2.3.4 Value Proposition

In the Business Model Canvas (section 2.2) we have identified the value proposition that AMASS could provide to the customers. In this section, we analyse the value proposition of AMASS focusing on the industrial automation domain and related to the AMASS Goals and usage scenarios described in [12].

AMASS Goal 1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.

Thanks to AMASS, the designer can introduce the safety and security aspects in the early phases of the process. This will reduce the effort and cost related to the safety and security analysis, compliance and certification processes.

AMASS Goal 2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.

AMASS will allow us the reuse of assurance results for product upgrades and re-certifications. For Component Suppliers and System Manufacturers this will avoid complete recertification or reassessment of suppliers' multi-function subsystems. It should not be mandatory to re-assess subsystems if multiple functions are integrated into one item or when the system is reassessed for product upgrades.

AMASS Goal 3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new CPS products.

AMASS will reduce the risk for new developments/certifications thanks to the integration of safety and security assurance in the design process of the new CPS products and helping us in the estimation of cost/effort for future developments.

AMASS Goal 4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification tool technologies by 60%.

AMASS will reduce efforts to exchange data between tools (any tool that must interact with assurance and certification activities).

2.4 Automotive Domain

2.4.1 Introduction

The automotive domain is currently facing heavy changes and challenges. On one hand the number of produced cars and commercial vehicles per year is growing very dynamically from ~ 58 million in 2000 over 89 million in 2014 to ~100 million by 2017. On the other hand, there are new market players, that either promote different business models compared to the usual "owning model" (like Uber) or are expanding from other domains into the automotive domain like Apple. There are even players that experiment with unmanned vehicles like amazon.

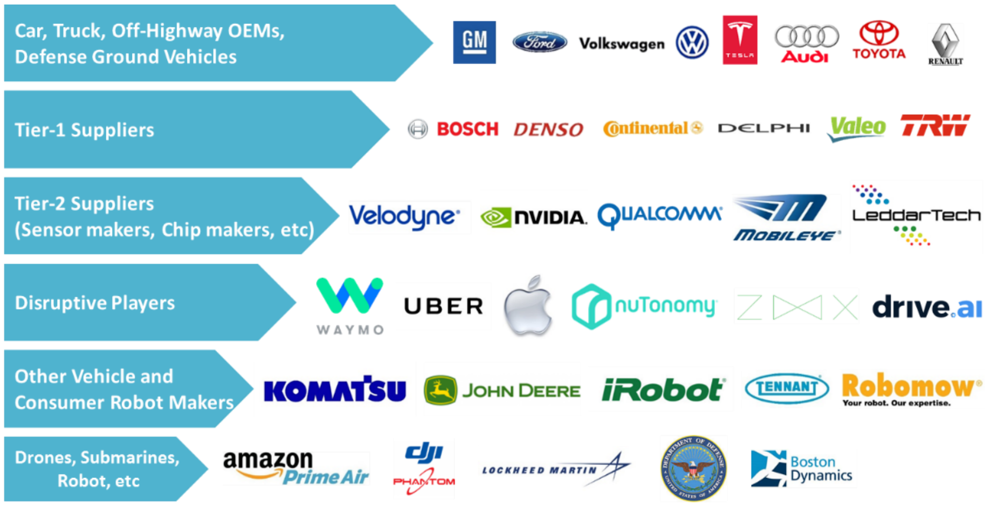


Figure 6. Automotive domain players

This new and fast evolving market situation is driven by key technologies and technical trends:

- Electric Driving
- Advanced Driver Assistance Systems and Autonomous Driving
- Connectivity and Mobile Services
- Cooperative Functions

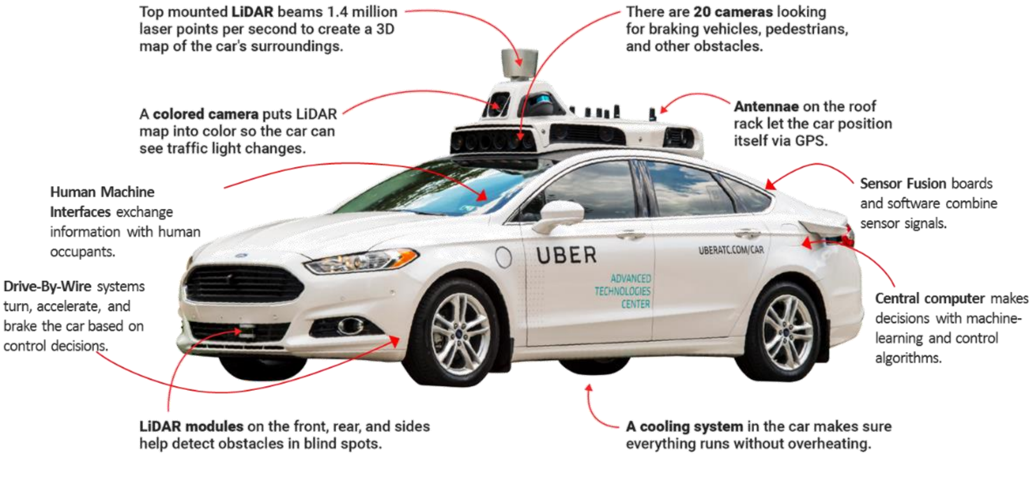

Top mounted LiDAR beams 1.4 million laser points per second to create a 3D map of the car's surroundings.
There are 20 cameras looking for braking vehicles, pedestrians, and other obstacles.
A colored camera puts LiDAR map into color so the car can see traffic light changes.
Antennae on the roof rack let the car position itself via GPS.
Human Machine Interfaces exchange information with human occupants.
Sensor Fusion boards and software combine sensor signals.
Drive-By-Wire systems turn, accelerate, and brake the car based on control decisions.
Central computer makes decisions with machine-learning and control algorithms.
LiDAR modules on the front, rear, and sides help detect obstacles in blind spots.
A cooling system in the car makes sure everything runs without overheating.
UBER
UBERATC.COM/CAR
ADVANCED TECHNOLOGIES CENTER

Image source: http://www.businessinsider.com/how-ubers-driverless-cars-work-2016-9

Figure 7. Automotive domain key technologies and technical trends

All these trends are creating high demands to the electronic systems and especially to the software. For example, inputs of different sensors must be fused together and evaluated in real-time for providing ADAS functions. The same hardware is supposed to be used for multiple purposes (i.e. different functions with potentially different safety requirements) and even for the provision of new functions after delivery of the car.

Furthermore, a large portion of the new requirements and challenges upon such systems are related to functional safety and cyber security. An example is autonomous driving, where the traditional way of demonstrating safety by testing on the road will require an unrealistic amount of test kilometers. Instead new approaches like simulation and in depth safety analysis are required. Cooperative functions where the function requires communication with the environment of the car (e.g. other cars or roadside) provides a surface for security attacks. In case such attacks are performed successfully, they usually have an impact on the functional safety. It is therefore important to analyze both safety and security of new functions by appropriate methods. Solutions must also be provided about how functional safety can be guaranteed in case security requires software updates at already delivered cars (i.e. during operation phase).

Functional safety in the automotive domain is done today according to the ISO 26262 standard which is a specialization of the IEC 61508. This standard undergoes now a major revision, to be expected in 2018. The automotive domain is known to be different from other domains due to the lack of national and international regulators or certification authorities for functional safety as the standard ISO 26262 does not require a certification by a public authority. However, there is a strong presence of audits and reviews (done by roles such as Independent Safety Assessors (ISAs)) requested by the vehicle manufacturers (OEMs) and component suppliers, they are always engaged on a commercial rather than quasi-regulatory basis.

For the aspect of Cyber-Security there is currently no standard available that could be applied out-of-the-box for the automotive domain. A standard development has started in October 2016 in the ISO committee (ISO 21434 “Road Vehicles -- Automotive Security Engineering”). Consequently, the aspect of cyber-security is currently in control of the OEMs; they are producing requirements, best practices or guidelines for their suppliers, but there is still no consolidated approach available. The upcoming new version of ISO 26262 contains a description of a few interaction points between the safety process and a potential cyber-security process.

AMASS will especially elaborate on the following aspects in the automotive domain to improve the state-of-the-art significantly:

- Realization of cooperative functions enabled by car-networking and how safety and security still can be guaranteed in such dynamic scenarios.
- Combined safety and security consideration for assurance.
- Integration of simulation and safety analysis techniques for validation and verification.
- Re-use of components for different safety-critical functions/applications and evolutionary scenarios.

2.4.2 Stakeholders

Stakeholders involve semiconductor manufacturers, tier-suppliers, engineering companies as well as car manufacturers. Inside these Stakeholders, the following roles are active: Safety Manager, Requirements Engineer, System engineer, Safety engineer, HW Engineer, SW Engineer.

The stakeholders’ goals in AMASS context are the following:

- Efforts for achieving functional safety and security and compliance with applicable standards like ISO 26262 contribute significantly to the overall effort of the development of new functions and systems. Reduction of these efforts plays an important role to achieve competitive prices. Since most products are developed as **product families** rather than single products, it is a goal to reduce the safety and security related efforts for members of product families.
- Functional Safety and security activities must be executed in parallel to the product development activities and require access to the engineering data such as models, requirements, test cases etc. To avoid unnecessary effort for duplication of such data and to ensure consistency, tools for safety and security and tools in the development process must interoperate seamlessly. This contributes to the quality and reduction of time and efforts.
- Products undergo product evolution. The goal is to reduce safety related efforts after **product modification** by limiting the efforts to only those parts that need to be re-evaluated to keep the safety and security claims of the product.

- By achieving the above, the process for functional safety and security is reduced in terms of effort required, which is translated in less time needed and as such contribute to the goal of having a shorter time-to-market for the products.

2.4.3 Business Process

Based on the usage scenarios provided in D1.1 [9], following generalized automotive business cases have been defined:

- BC1: Enable efficient collaboration between stakeholders in the supply chain
- BC2: Safety- and Security-oriented Process Line
- BC3: Process- and Product-based Safety and Security Assurance

2.4.3.1 BC1: Enable efficient collaboration between stakeholders in the supply chain (for safety)

A deep supply chain characterizes the automotive domain. Organizations in this supply chain must collaborate with each other. Especially in functional safety, it is important that the safety case at the end is assembled together with information that must be provided by the different stakeholders and which must be consistently integrated.

Figure 8 shows an overview of the collaboration in the supply chain for functional safety.

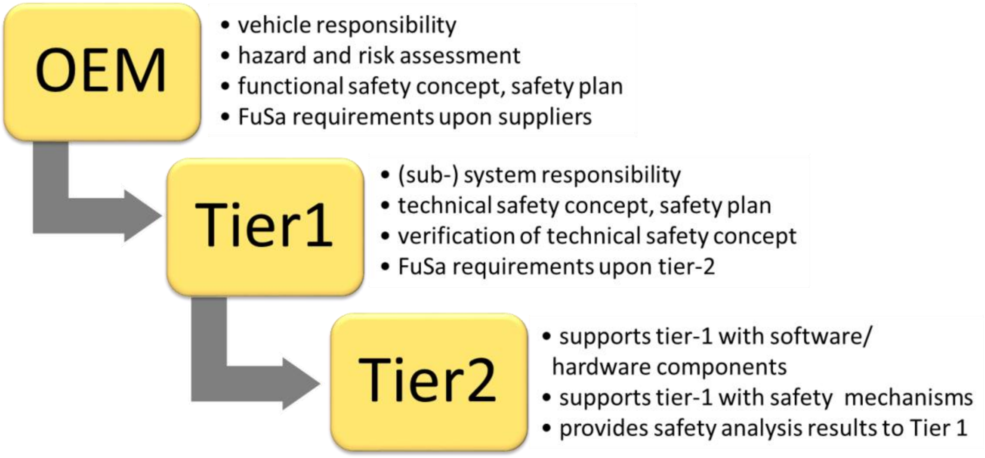

OEM
• vehicle responsibility
• hazard and risk assessment
• functional safety concept, safety plan
• FuSa requirements upon suppliers
Tier1
• (sub-) system responsibility
• technical safety concept, safety plan
• verification of technical safety concept
• FuSa requirements upon tier-2
Tier2
• supports tier-1 with software/ hardware components
• supports tier-1 with safety mechanisms
• provides safety analysis results to Tier 1

Figure 8. Automotive supply chain and functional safety (FuSa) activities

As shown in Figure 8, different information has to be exchanged:

- (System-) design information including architecture and functions
- Safety goals and safety requirements including their allocation to architectural elements
- Information on safety mechanisms
- Safety analysis information like failure modes and failure rates (for HW-elements).

The activities typically are performed along the different phases of a V-Model as depicted in Figure 9.

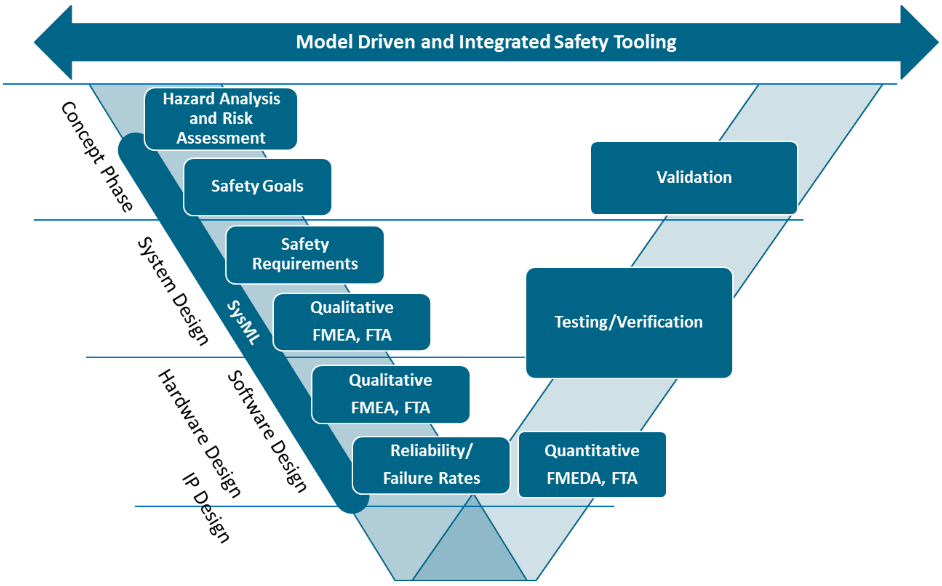


Figure 9. Functional safety activities and work products

The traditional way of enabling this workflow by exchange of documents is error-prone and time consuming. A better approach is to do the data exchange directly with the tools that are also used for the provision of the data. This can be partially done today due to several individual tool connectors that are available. However, a seamless working style is still not possible. Therefore, information must be manually processed and very often be re-entered into different tools.

2.4.3.2 BC2: Safety- and Security-oriented Process Line

On the one hand, we need fully defined processes and adequate evidence to show compliance to demanded standards. On the other hand, detailed processes are supporting engineers specially those who are not familiar with the full set of development steps. The possibility to generate comprehensive evidence that is traceable to the requirements is improved by using complete processes. Safety- and Security-Oriented Process Line (S2OPL) provides the possibility to reuse commonalities of process elements (e.g. process steps). For this reason, assessments may be faster because evidence related to common process steps exists only once and only the change impact has to be checked. Assessors and manufacturers achieve benefits because they save engineering effort (time and costs).

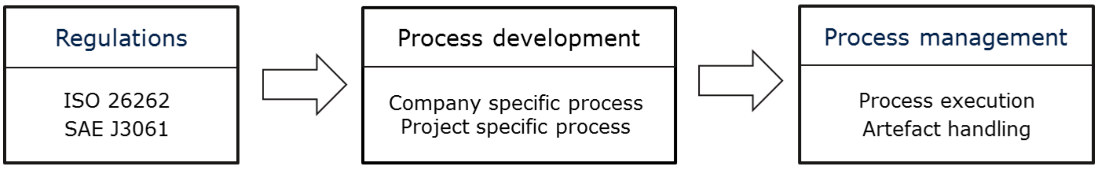


Figure 10. Safety- and Security-oriented Process Line: Workflow

Figure 10 shows the workflow related to S2OPL concerning relevant stakeholders. It starts with input from regulators and standard organizations and leads to the manufacturer who has to define and manage processes. Process management includes process execution and handling of artefacts.

2.4.3.3 BC3: Process- and Product-based Safety and Security Assurance

The relationship between requirements and evidence has to be communicated by clear comprehensive argumentation. Not all affected stakeholders may be in-depth familiar with engineering processes and content of resulting work products. A proper and systematic argumentation will allow faster understanding of needed argumentation. This will lead to shorter review cycles and concise feedback. In AMASS we will improve the methodology concerning process- and product-based argumentation. Two types of argumentation have different goals and are used by different stakeholders. For example, auditors will check process-based argumentation in a process audit. The argumentation has to point out that the process is compliant to relevant standards e.g. ISO 26262 for safety and SAE J3061 for security. Furthermore, the OEM will use product-based argumentation in a functional safety assessment to show that the product is safe. Product based argumentation concerning security may be passed to end-users to show the product is secure.

To overcome the complexity a systematic reuse approach like argumentation patterns directly related to process steps will be defined. The goal is to establish a clear relationship between the process and the argumentation. Therefore, a systematic approach is required to argue development processes, which deal with dependency issues concerning safety and security.

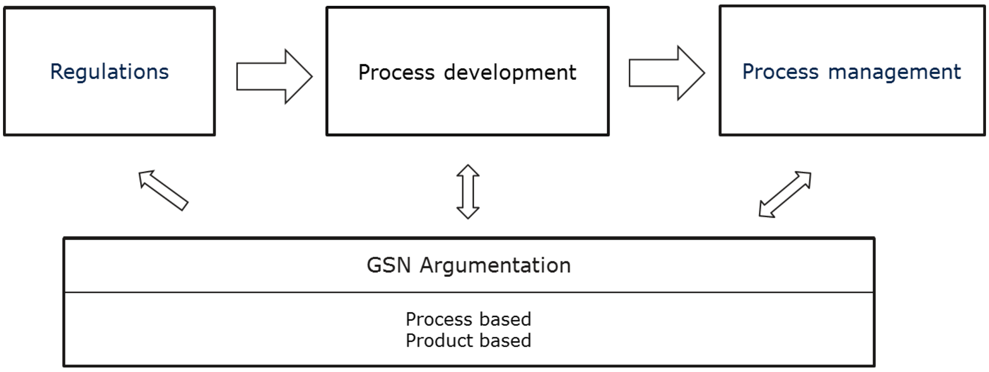


Figure 11. Process- and Product-based Safety and Security Assurance: Workflow

Figure 11 shows how GSN argumentation extends the S2OPL approach. The elaborated artefacts are basis for process- and product-based argumentation, which allows stakeholders to argue in various ways.

2.4.4 Value Proposition

The value proposition of AMASS in the automotive domain is the following:

AMASS Goal 1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.

- Introduce safety/security concerns in the early phases of product development in order to reduce costs
- Introduce safety/security co-assessment
- Reduce efforts and costs for managing compliance with targeted standards
- Reduce efforts and costs for safety/security assurance and certification
- Reduce efforts to run safety/security analyses

AMASS Goal 2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.

- Reuse of assurance results for product upgrades and re-certifications: For Component Suppliers and System Manufacturers: Avoid complete recertification or reassessment of suppliers' multi-function subsystems. It should not be mandatory to re-assess subsystems if multiple functions are integrated into one item or when the system is reassessed for product upgrades.

AMASS Goal 3: *to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new CPS products.*

- N/A

AMASS Goal 4: *to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification tool technologies by 60%.*

- Seamless access to architecture models for performing safety and security analysis – effort for doing safety analysis in case of design iterations is reduced dramatically.
- Seamless integration with requirements management tools for incorporation of safety requirements and their verification – quality and consistency increases.
- Tool supported exchange of safety concepts between OEM and tier supplier including filters for confidential information – will reduce the collaboration and integration effort and help with the production of safety cases.
- Tool integration will reduce the risk of data loss and data inconsistency.

2.5 Railway Domain

2.5.1 Introduction

Railway systems were the first means of mass mechanized movement. They can be classified:

- by rolling stock (either diesel or electric traction): trains may consist of one or more locomotives and a number of cars for passengers or freight, trains may be self-contained passenger trains that don't have separate locomotive
- by traffic characteristics: long distance, regional service, urban transport (mass transit)
- by operation: centralised control, fully signalled operation, drive on sight, driverless automated, etc.

Variations exist among ownership (private/public), organisation (separation of infrastructure and operating companies), implementation (main line/secondary line, single track/double track), etc. A number of techniques, technologies and components were developed during a long period of gestation. Maturity gained over time allowed to write down a set of standards that are used for every railway system being designed, manufactured, assembled, deployed and maintained.

AMASS will focus on the application of railways standards for safety assessment and seamless introduction of security aspects.

The path taken by any train is determined by the mechanical guidance system of wheel and rail that can be changed only by points (switches). On a single-track railway, trains can only pass each other at particular locations. It has to be possible to determine the route to be followed and to set the points (switches) accordingly. Moreover, breaking distance is often longer than the visible and clear route in front of the driver. So the sight on the route has to be supplemented by other means in order to indicate to the driver in good time a clear route or a need to stop. To solve these two problems, procedures and techniques have been developed and adapted to the state of the art.

The railway signalling and control system is therefore needed for the safe control of transport processes in rail traffic:

- The signalling system ensures the safe control of transport processes. The safety aspect is of paramount importance.
- The operation control system ensures optimal control of the sequences of main and auxiliary processes in a traffic system.

Both systems use the means and methods of information transmission and information processing. Consideration of safety, reliability and availability are important in both systems. Signalling systems involve the regulation of traffic and the prevention of accidents whereas operation control systems have to prevent effective failures. The technical components of control and signalling systems are similar but any considerations of safety and availability have to be general considerations that take the entire situation into account.

Safety in the railways is mainly handled by three standards:

- EN 50126 is about Safety Management Systems
- EN 50128 is about Safety Software Management
- EN 50129 is about proving the safety of a product in a Safety Case

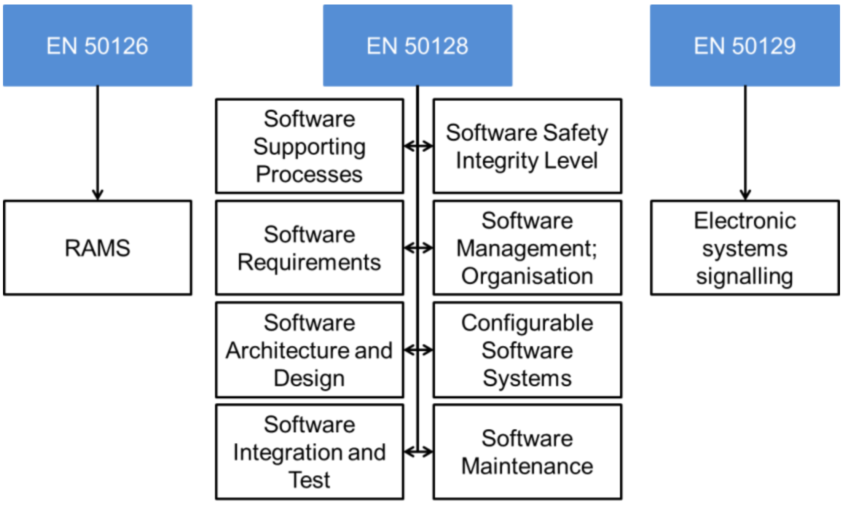

EN 50126
EN 50128
EN 50129
Software Supporting Processes
Software Safety Integrity Level
RAMS
Software Requirements
Software Management; Organisation
Electronic systems signalling
Software Architecture and Design
Configurable Software Systems
Software Integration and Test
Software Maintenance

Figure 12. The standards EN50126, EN50128 EN50129 describe the functional safety in the railway industry [1]

EN 50126 describes all the necessary key elements for a Safety Management System; there must be a company policy, a safety plan, a hazard log, internal audits and a failure reporting and corrective actions system, a risk estimation process, etc. It is then up to the Railway organization to adjust size, amount and complexity of these key elements into a suitable and operative Safety Management System for the product and organization in question.

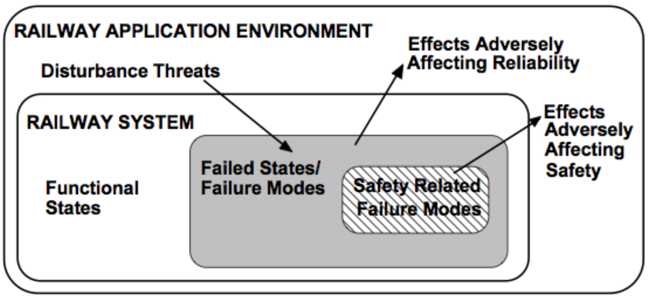

RAILWAY APPLICATION ENVIRONMENT
Disturbance Threats
Effects Adversely Affecting Reliability
RAILWAY SYSTEM
Effects Adversely Affecting Safety
Functional States
Failed States/ Failure Modes
Safety Related Failure Modes

Figure 13. Effects of failure within a system (EN50126)

Safety is expressed in terms of Safety Integrity Level (SIL) ranging from 0 to 4. There are several methods used to assign a SIL that are used in combination and may include risk matrices, risk graphs, etc.

Safety critical functions are SIL3/SIL4 functions such as the emergency brake or the logic in interlocking systems.

2.5.2 Stakeholders

As far as the systems of railway domain are concerned, stakeholders' map depends on the national organization (different from one country to another) and possibly on the kind of railway line (urban or main line). The main stakeholders involved are potentially:

- **Manufacturer** (Alstom, Bombardier, Siemens, etc.): companies designing, developing, manufacturing and integrating equipment/systems that are either safety related or safety critical. Reliability, Availability, Maintainability and Safety, as well as performance issues represent the main factors impacting on all phases of the product lifecycle.

[1] These standards implement the IEC61508 for this industry.

- **Infrastructure Managers and Railway undertaking** (BR, DB, NYCT, RATP, SNCF, etc.): the company, either public or private, in charge of the governance and the exploitation of the railway system. The service operating company may require a certificate for any safety-related or safety critical system, or instead go for an internal qualification (in this case, dedicated in-house services are in charge of performing “certification-like” verification & validation).
- **Certification body**: (CERTIFER, Veritas, TÜV, etc.): their concern is *a minima* the system’s compliance to the railway standards. Some bodies cover only strict standards compliancy while others require a deep understanding of the technological aspects and their associated failures. The certification body is in charge of providing the certificates. The certification body can also be asked to play the role of the national technical agency.
- **National technical agency**: (STRMTG, EPSF, etc.): this national agency is in charge of compiling all evidences for a complete line, in order to enable the supervision body to issue a decree authorizing its exploitation. The agency may also use an independent expert (selected by the government of the country where the railway system is operated – in France, EOQA) to participate to the writing of the report/technical certificate.
- **Supervision body**: (prefecture, etc.) this body in charge of authorizing the exploitation of a line, based on the report/technical certificate provided by the related national technical agency.
- **Standardization body** (European Railway Agency) this body is responsible for the standards creation and update in Europe.

To complete the picture, other levels of verification bodies can be listed:

- Comité Français d’Accréditation (COFRAC) in France, in charge of evaluating the French Certification bodies like CERTIFER, Veritas with regard to EN 17020 and EN 17065 standards.
- European cooperation for Accreditation (EA): cross-audits among European certification bodies

2.5.3 Business Process

Based on the usage scenarios provided in D1.1 [9], following generalized railway business case has been defined:

- BC1: Managing compliance with EN50126 though project lifetime

2.5.3.1 BC1: Managing compliance with EN50126 though project lifetime

This business process is focused on the interaction between the manufacturer, the exploiting company and the certification body, for the certification of a railway system. Other interactions happen at a different level and do not constitute the objective of the business case.

The business process involves five parties:

- Design team
- Verification team
- Validation team
- Safety team
- Independent safety assessor (ISA)

The business process is represented as separate processes because many interactions are performed cyclically. In particular, the independent safety assessor is involved continuously once the system is defined and designed: (s)he is invited to make comments on the documentation that is provided to him/her regularly.

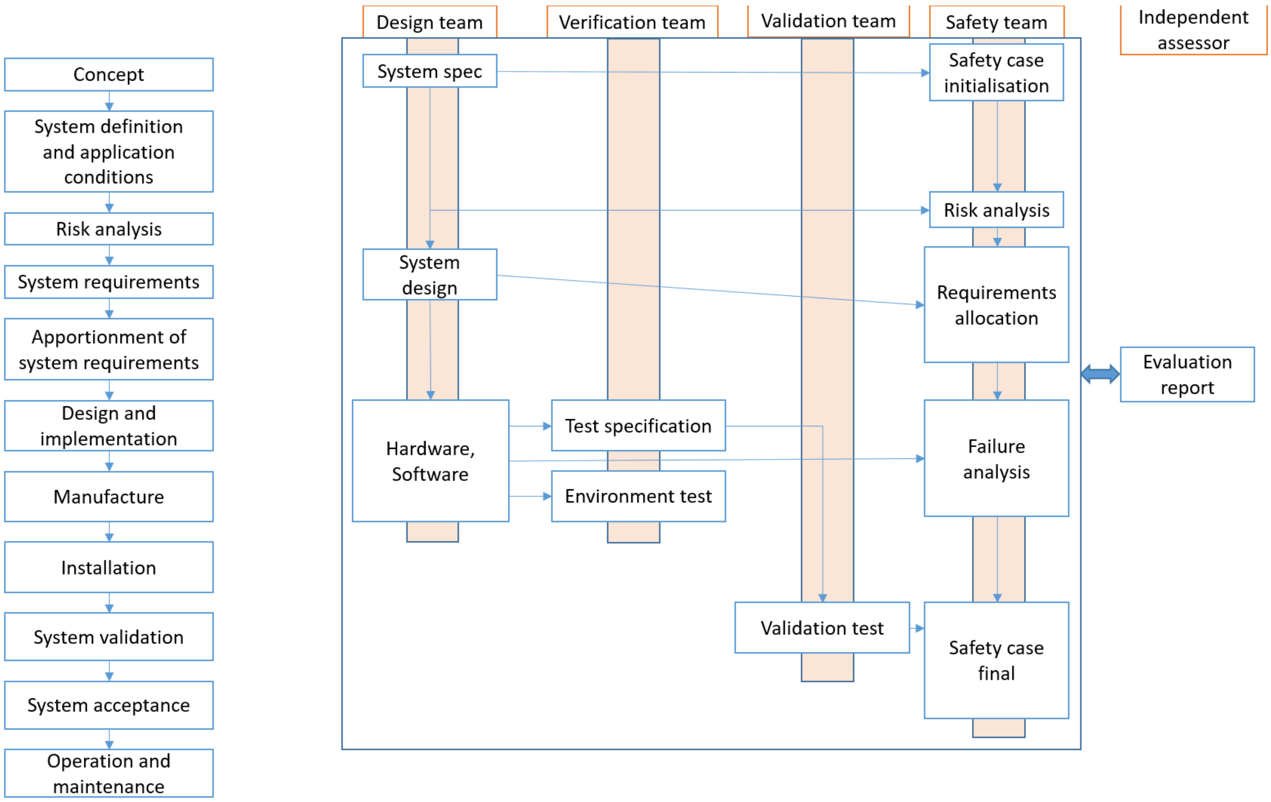


Figure 14. Project safety management as a collective process involving 5 roles

A project is organized in fourteen (14) phases according to the EN50126 standard. These phases appear on the left of Figure 14 (in order to keep the figure clear and manageable, three phases are not shown: performance measure, modification/retrofit, removal).

During the first five phases, the system is defined (system specification and safety case documents are initiated). The risk analysis allows to define feared events and to determine safety integrity levels. Functional and safety requirements are then allocated on the global system architecture.

During the design phase:

- the hardware is fine-tuned. Its manufacturing file is completed. Environmental tests are specified (EMC, fire/smoke, etc.) as well as serial tests.
- The software is developed, verified and tested.
- Integration testing are performed at system level, as well as design tests.

During the validation and acceptance phases, the final safety tests are performed. The Safety Case is completed, including quality insurance report and technical safety proof. Traceability elements are integrated to the report as an annex.

2.5.4 Value Proposition

The value proposition of AMASS in the railway domain is the following:

AMASS Goal 1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.

- Improving the code review process to lower verification costs and risks (better level of confidence in the software). Code peer review for safety critical functions is of paramount importance, as no certified code generator is used in the toolchain.

- Integrating seamlessly security study into existing safety case. Security is not yet part of the safety case, but given the global tendency to have all systems connected (IoT, etc.), new risks due to this forthcoming connectivity have to be taken into account and introduced/combined to existing risks analysis.

AMASS Goal 2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.

- N/A (improvements on code review are expected to be fully automatic and hence replay-able at will, so reusing previous assurance results is not particularly interesting).

AMASS Goal 3: *to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new CPS products.*

- N/A

AMASS Goal 4: *to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification tool technologies by 60%.*

- N/A

2.6 Avionics Domain

2.6.1 Introduction

Most avionics systems (e.g., airborne flight control, braking, and cockpit display) are typical examples of safety-critical, real-time systems. They often operate in environments with diverse ranges of temperature, humidity, air pressure, vibration and movement, and are subject to the effects of age, maintenance, and weather. Typical characteristics required of such systems are reliability, fault tolerance, and deterministic timing guarantees.

Most if not all aspects of design, production, maintenance and operation of avionics systems are subject to extensive regulation. Certification is a critical element in the safety-conscious culture on which aviation is based. The purpose of avionics certification and related industry standards is to document a judgement that an airborne system meets all applicable regulatory requirements, can be manufactured properly and finally installed safely on board in an aircraft.

AMASS will focus on two aspects: the application of aerospace industrial standards for safety assessments and the reuse of assurance artefacts from automotive technology into the avionics domains.

Air transport is a highly regulated industry. Certification (in civil aviation) is the formal recognition and legal statement (written certificate), by the state authority, that an aeronautical product complies with the applicable regulations. An "aeronautical product"' means an aircraft, turbine engine or propeller. In addition, "parts and appliances" means any instrument, equipment, mechanism, part, apparatus, hardware accessories, software, and including communication equipment that is used or intended to be used in operating or controlling an aircraft in flight. Since 2003 the European Agency for Safety in Aviation (EASA) has been acting under the European Commission. It has direct Authority over aircraft manufacturers, equipment suppliers, repair stations and operators all over the European Union.

Industry standards provide recognized means to develop certifiable systems, software and hardware, to conduct activities and/or produce certification artefacts (written records of evidence of process/product results), and to contribute to systems certification and safety processes. EASA uses industry standards adapted to its own certification rules and advisory material to provide guidance in terms of interpretative material or acceptable means of compliance with applicable regulations. A short list of industry standards used by EASA is (see Figure 15):

- *Software:* RTCA DO-178C – EUROCAE ED-12C – Software Considerations in Airborne Systems and Equipment Certification, with supplements:
  - RTCA DO-330 – Software Tool Qualification Considerations
  - RTCA DO-331 – Model-Based Development and Verification
  - RTCA DO-332 – Object-Oriented Technology and Related Technique
  - RTCA DO-333 – Formal Methods
- *Hardware:* RTCA DO-254 – EUROCAE ED-80 – Design assurance guidance for airborne electronic hardware
- *Environmental:* RTCA DO-160G – EUROCAE ED-14G – Environmental Conditions and Test Procedures for Airborne Equipment
- *Safety:* SAE ARP 4761 – EUROCAE ED-135 – Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment
- *System:* SAE ARP 4754A – EUROCAE ED-79A – Guidelines for development of civil aircraft and systems

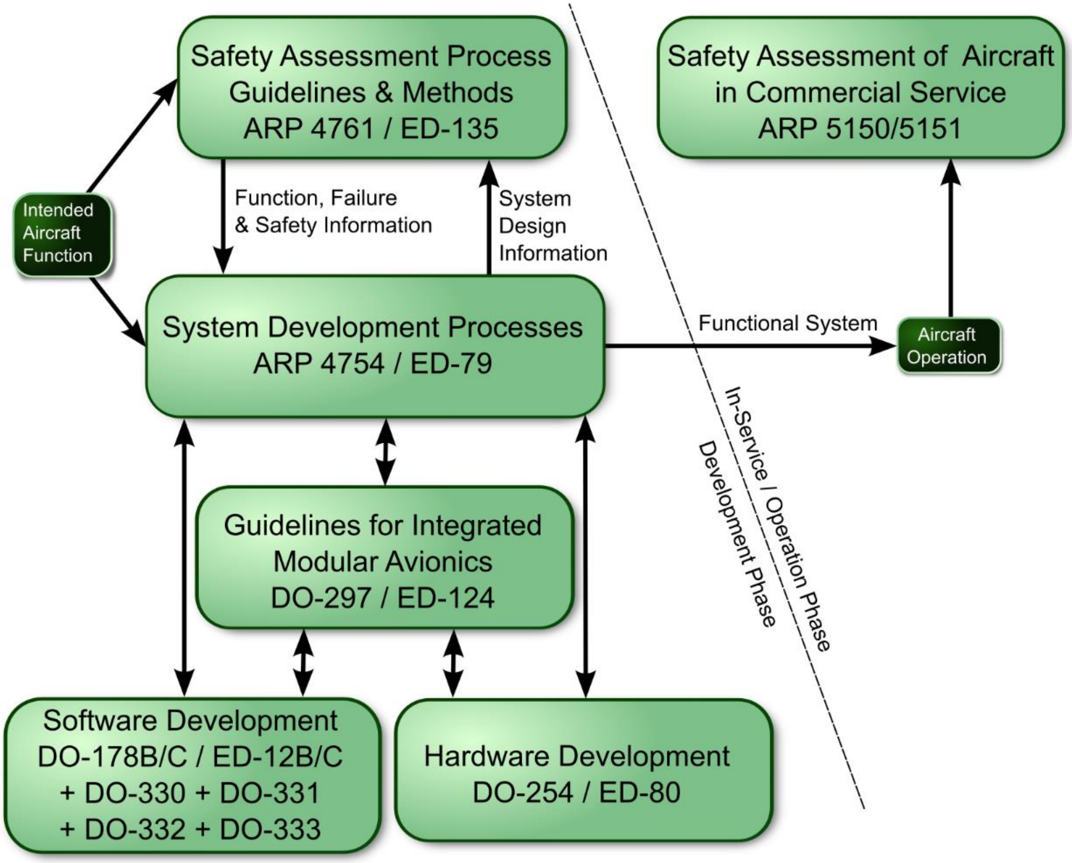

Safety Assessment Process Guidelines & Methods ARP 4761 / ED-135
Safety Assessment of Aircraft in Commercial Service ARP 5150/5151
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
System Development Processes ARP 4754 / ED-79
Functional System
Aircraft Operation
In-Service / Operation Phase
Development Phase
Guidelines for Integrated Modular Avionics DO-297 / ED-124
Software Development DO-178B/C / ED-12B/C + DO-330 + DO-331 + DO-332 + DO-333
Hardware Development DO-254 / ED-80

Figure 15. Industry standards structure for development and safety assurance of avionics

These industry standards provide guidance for all planned and systematic actions used to substantiate, at an adequate level of confidence, that errors have been identified and corrected. Systems and items (one or more hardware and/or software elements treated as a unit, having bounded and well-defined interfaces) are assigned “development assurance levels (DAL)” based on failure condition classifications associated with aircraft-level functions implemented in the systems and items. The rigor and discipline needed in performing the supporting processes will vary corresponding to the assigned development assurance level. The system DAL is assigned based on the most severe failure condition classification associated with the applicable aircraft-level function(s).

The Item DAL is allocated based on the overall system architecture through allocation of risk determined using the PSSA (Preliminary System Safety Assessment per SAE ARP-4761). For items that support multiple aircraft functions, the applicable safety requirement should be based on the most severe of the effects resulting from failure or malfunction of any supported aircraft function or any combination of supported functions.

2.6.2 Stakeholders

Aircraft or rotorcraft 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. 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 the AMASS platform helping them to handle the allocated requirements and the associated compliance evidences.

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. 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 the AMASS platform helping them to handle the data packages in conformance with the applicable certification requirements.

Equipment or component provider: a supplier who seeks to establish the compliance of the hardware and/or software elements that it provides with requirements from the avionics system manufacturer who integrates them into the wider system. The aircraft manufacturers, system manufacturers and equipment/component providers exchange and share numerous pieces of information that 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 the AMASS platform helping them to cope consistently with the induced complexity, in particular to manage information traceability and to enable delta recertification.

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. AMASS tools will help airworthiness authorities 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.

Standards organisation: a domain-independent organisation whose primary activities are concerned with the development, coordination, 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.

2.6.3 Business Process

Based on the usage scenarios provided in D1.1 [9], following generalized avionics business cases have been defined:

- BC1: Reduce efforts for safety assessments of avionics systems
- BC2: Reduce assurance and certification efforts to reuse technology from the automotive domain
- BC3: Reduce efforts for V&V-based assurance of avionics systems

2.6.3.1 BC1: Reduce efforts for safety assessments of avionics systems

Handling the large amounts of data required for the assurance process in avionics 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 AMASS platform can support the handling of verification and validation data in such a way that the airworthiness certification assessment becomes faster and easier.

The highly aggregated safety assessment process for avionics is depicted in Figure 16. 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.

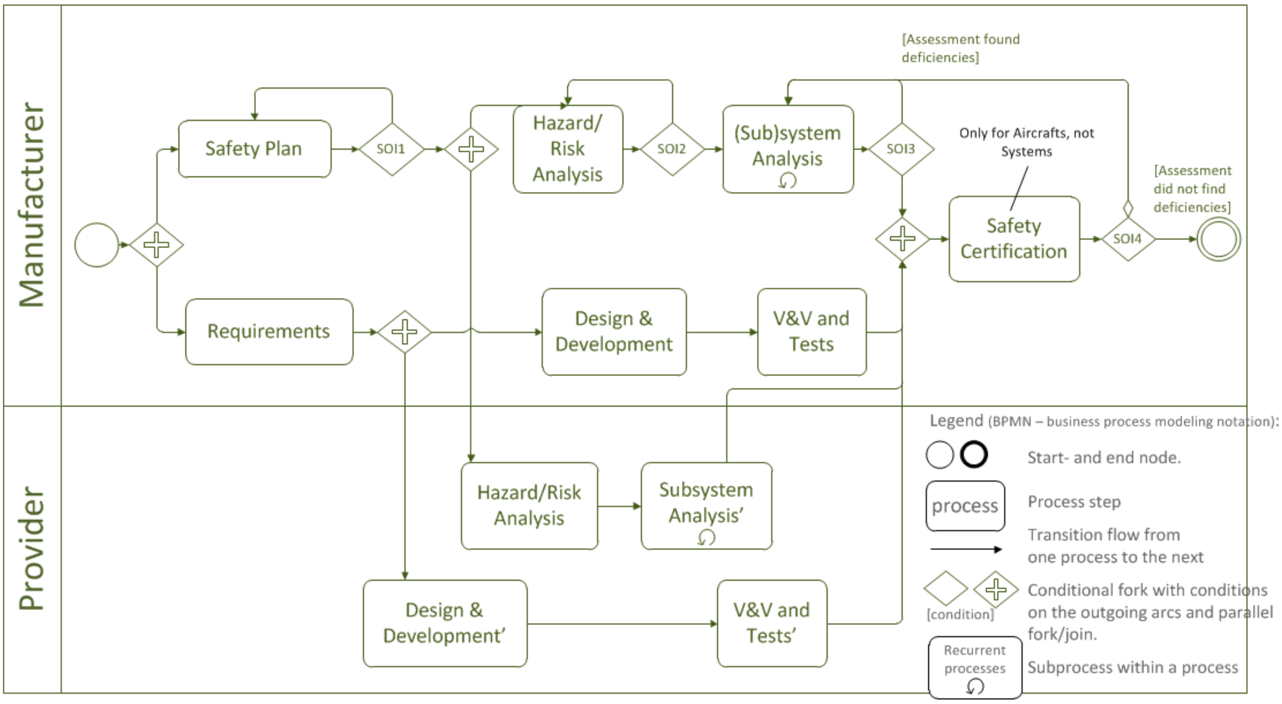

Manufacturer
Provider
[Assessment found deficiencies]
Safety Plan
SOI1
Hazard/ Risk Analysis
SOI2
(Sub)system Analysis
SOI3
Only for Aircrafts, not Systems
[Assessment did not find deficiencies]
Safety Certification
SOI4
Requirements
Design & Development
V&V and Tests
Hazard/Risk Analysis
Subsystem Analysis'
Design & Development'
V&V and Tests'
Legend (BPMN – business process modeling notation):
Start- and end node.
process
Process step
Transition flow from one process to the next
[condition]
Conditional fork with conditions on the outgoing arcs and parallel fork/join.
Recurrent processes
Subprocess within a process

Figure 16. Safety assessment business process for the avionics domain

The workflow can be summarised as follows:

- An important aspect is included in the overall safety assessment process: the process of the component supplier. One of the goals 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 16 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 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 (SOI 1-4) during the development process:
    - SOI #1: Planning Review is conducted when the initial planning process is completed, to determine whether the applicant's plans and standards satisfy the objectives of the standards, both hardware and software.
    - SOI #2: Development Review is conducted when the design process and resulting data are sufficiently complete and mature to ensure that enough evidence exists to show effective implementation of the plans and application of the standards.
    - SOI #3: Verification Review is conducted when the verification process and resulting data are sufficiently complete and mature to ensure that representative data exists to show effective implementation of the plans and application of the standards.
    - A common understanding of SOI #2, respectively SOI #3, is to consider them associated with the top-down, i.e. design portion of the development for SOI #2 to be conducted, and the bottom-up, i.e. verification portion of the development for SOI #3 to be conducted, respectively.
    - SOI #4: Final [Certification] Review is conducted when all the development activities are completed for the final configuration identified and considered applicable and valid for the intended to be certified equipment, system, hardware and software.

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.

Significant reduction of the effort could be achieved by using AMASS formal safety analysis tools and methods and by leveraging of Models-Based Safety Assessment (MBSA) annex to the ARP 4761, which is the safety assessment guideline for aerospace.

2.6.3.2 BC2: Reduce assurance and certification efforts to reuse technology from the automotive domain

In the aviation domain, it is essential to use highly reliable components for avionic systems to match the requirements of a certification. The EUROCAE document ED-80 (RTCA DO-254) "Design Assurance Guidance for Airborne Electronic Hardware" does describe the objectives and activities for each process of the life cycle of electronic hardware that includes circuit board assemblies, application specific integrated circuits, programmable logic devices, etc. EUROCAE ED-14G (RTCA DO-160G) "Environmental Conditions and Test Procedures for Airborne Equipment" does define environmental tests conditions and procedures for airborne equipment.

The majority of airborne electronic hardware is composed of commercial off-the-shelf (COTS) parts ranging from simple passive components to highly complex integrated circuits. ED-80 / DO-254 states that the basic for using COTS components is the use of an electronic components management in conjunction with the design process. Each component has to be qualified by the manufacturer to establish its reliability. Furthermore, service experience is used to show the quality and again the reliability of COTS components. Demonstration of compliance of a regulation is done by collecting evidence that the objectives and requirements are satisfied.

The automotive domain has its own standards and requirements for proving compliance of a component. For example, the Automotive Electronics Council (AEC) defines in AEC Q100 stress test qualification for integrated circuits. Mapping results of an automotive product qualification to the aviation domain will reduce the effort to achieve certification of an avionic system.

The cross domain reuse of evidence and artefacts from automotive assurance processes is assisted by AMASS tools and methods. Evidence management, traceability and seamless integration will reduce the efforts for reusing automotive components significantly.

2.6.3.3 BC3: Reduce efforts for V&V-based assurance of avionics systems.

Verification and validation assurance involves majority of the effort for many complex avionics systems. There are two main approaches about how to reduce the effort: by reuse and by automation.

Reuse of the previous assurance results from different domain is part of the BC2. The reuse of the previous assurance results within the same domain is not targeted by the avionics case study.

The automation of the verification and validation assurance could be performed on many levels from validation of System requirements to generation of test cases for executable object code.

In Figure 17, the targeted software process objectives from DO-178C for automation are highlighted by starting with four different colours corresponding to four different technologies. While both requirement-based and design-based test case generation tools are or can be qualified, most requirement semantic analysis and formal verification tools are not qualified yet.

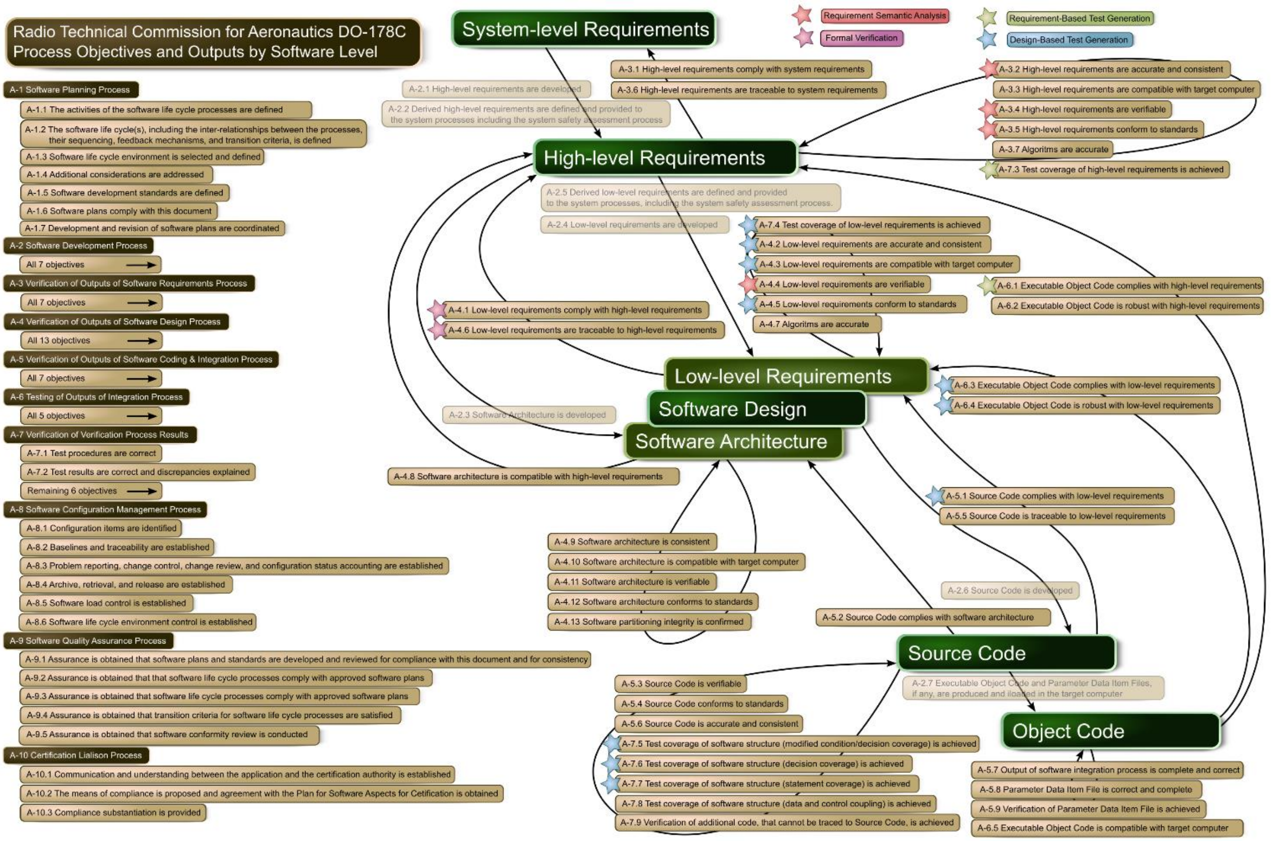

Radio Technical Commission for Aeronautics DO-178C
Process Objectives and Outputs by Software Level
A-1 Software Planning Process
A-1.1 The activities of the software life cycle processes are defined
A-1.2 The software life cycle(s), including the inter-relationships between the processes, their sequencing, feedback mechanisms, and transition criteria, is defined
A-1.3 Software life cycle environment is selected and defined
A-1.4 Additional considerations are addressed
A-1.5 Software development standards are defined
A-1.6 Software plans comply with this document
A-1.7 Development and revision of software plans are coordinated
A-2 Software Development Process
All 7 objectives
A-3 Verification of Outputs of Software Requirements Process
All 7 objectives
A-4 Verification of Outputs of Software Design Process
All 13 objectives
A-5 Verification of Outputs of Software Coding & Integration Process
All 7 objectives
A-6 Testing of Outputs of Integration Process
All 5 objectives
A-7 Verification of Verification Process Results
A-7.1 Test procedures are correct
A-7.2 Test results are correct and discrepancies explained
Remaining 6 objectives
A-8 Software Configuration Management Process
A-8.1 Configuration items are identified
A-8.2 Baselines and traceability are established
A-8.3 Problem reporting, change control, change review, and configuration status accounting are established
A-8.4 Archive, retrieval, and release are established
A-8.5 Software load control is established
A-8.6 Software life cycle environment control is established
A-9 Software Quality Assurance Process
A-9.1 Assurance is obtained that software plans and standards are developed and reviewed for compliance with this document and for consistency
A-9.2 Assurance is obtained that that software life cycle processes comply with approved software plans
A-9.3 Assurance is obtained that software life cycle processes comply with approved software plans
A-9.4 Assurance is obtained that transition criteria for software life cycle processes are satisfied
A-9.5 Assurance is obtained that software conformity review is conducted
A-10 Certification Lialison Process
A-10.1 Communication and understanding between the application and the certification authority is established
A-10.2 The means of compliance is proposed and agreement with the Plan for Software Aspects for Cetification is obtained
A-10.3 Compliance substantiation is provided
System-level Requirements
Requirement Semantic Analysis
Formal Verification
Requirement-Based Test Generation
Design-Based Test Generation
A-3.1 High-level requirements comply with system requirements
A-3.6 High-level requirements are traceable to system requirements
A-2.1 High-level requirements are developed
A-2.2 Derived high-level requirements are defined and provided to the system processes including the system safety assessment process
A-3.2 High-level requirements are accurate and consistent
A-3.3 High-level requirements are compatible with target computer
A-3.4 High-level requirements are verifiable
A-3.5 High-level requirements conform to standards
A-3.7 Algoritms are accurate
A-7.3 Test coverage of high-level requirements is achieved
High-level Requirements
A-2.5 Derived low-level requirements are defined and provided to the system processes, including the system safety assessment process.
A-2.4 Low-level requirements are developed
A-7.4 Test coverage of low-level requirements is achieved
A-4.2 Low-level requirements are accurate and consistent
A-4.3 Low-level requirements are compatible with target computer
A-4.4 Low-level requirements are verifiable
A-4.5 Low-level requirements conform to standards
A-4.7 Algoritms are accurate
A-6.1 Executable Object Code complies with high-level requirements
A-6.2 Executable Object Code is robust with high-level requirements
A-4.1 Low-level requirements comply with high-level requirements
A-4.6 Low-level requirements are traceable to high-level requirements
Low-level Requirements
Software Design
Software Architecture
A-6.3 Executable Object Code complies with low-level requirements
A-6.4 Executable Object Code is robust with low-level requirements
A-2.3 Software Architecture is developed
A-4.8 Software architecture is compatible with high-level requirements
A-5.1 Source Code complies with low-level requirements
A-5.5 Source Code is traceable to low-level requirements
A-4.9 Software architecture is consistent
A-4.10 Software architecture is compatible with target computer
A-4.11 Software architecture is verifiable
A-4.12 Software architecture conforms to standards
A-4.13 Software partitioning integrity is confirmed
A-2.6 Source Code is developed
A-5.2 Source Code complies with software architecture
Source Code
A-5.3 Source Code is verifiable
A-5.4 Source Code conforms to standards
A-5.6 Source Code is accurate and consistent
A-2.7 Executable Object Code and Parameter Data Item Files, if any, are produced and loaded in the target computer
Object Code
A-7.5 Test coverage of software structure (modified condition/decision coverage) is achieved
A-7.6 Test coverage of software structure (decision coverage) is achieved
A-7.7 Test coverage of software structure (statement coverage) is achieved
A-7.8 Test coverage of software structure (data and control coupling) is achieved
A-7.9 Verification of additional code, that cannot be traced to Source Code, is achieved
A-5.7 Output of software integration process is complete and correct
A-5.8 Parameter Data Item File is correct and complete
A-5.9 Verification of Parameter Data Item File is achieved
A-6.5 Executable Object Code is compatible with target computer

Figure 17. Different technologies can automate some DO-178C objectives

Since qualification of more complex formal methods tools is very difficult, most of these tools are used in advisory mode only. Therefore, there is no certification credit take for the proven absence of defects. On the other hand, any defect detected can be easily verified and fixed manually. Since formal methods could be deployed in earlier development stages, when no test cases are written, signification reduction of development cycles is achieved.

2.6.4 Value Proposition

The value proposition of AMASS in the avionics domain is the following:

<u>AMASS Goal 1</u>: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.

- Automation of safety assessment – methodology, SysML modelling tools and model-based safety assessment tools.
- Automation of requirement semantic analysis instead of manual reviews – conformance to standards, verifiability, consistency, non-redundancy, feasibility.
- Automation of formal verification of the requirements against system architecture and system design.
- Reduction of number of development cycles by early V&V assurance.
- Reduction of cost of due to poor quality.

<u>AMASS Goal 2</u>: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.

- Reuse of assurance results from automotive domain.

- Reuse of V&V assurance results – software components, requirements on components and corresponding argumentation.
- Reuse of safety assessment results – argumentation methods.

AMASS Goal 3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new CPS products.

- Automation of requirement semantic analysis – reduction of propagated defects and dependability analysis.
- Automation of formal verification of requirements against system architecture and system design – reduction of propagated defects and dependability analysis.
- Semi-automated safety assessment and risk analysis.

AMASS Goal 4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification tool technologies by 60%.

- Methodology of seamless connection between the different tools (e.g. ForReq, Simulink, SysML modelling tools, verification and safety assessment tools).
- Methodology of seamless integration of tools for requirement semantic analysis.
- Harmonization of formal methods tools – harmonization of assurance and V&V results.
- Methodology of seamless integration of tools for safety assessment.

2.7 Space Domain

2.7.1 Introduction

The Space Industry relates to the design and manufacturing of systems that go into Earth´s orbit or into deeper space. It is a highly qualified industry, mainly due to the hostile environment where the components must live in, while providing the quality of service according to space standards and required by the application.

Space components must be designed to withstand extreme temperatures and high levels of radiation that may change the state of electronic devices. Microprocessors, semiconductor memory and other electronic devices must be protected against Single Event Effects (SEE) caused by radiation, and its design must guarantee that the system performs correctly during the whole mission, since there is no possibility of repair after launch.

The main areas of application of space systems are:

- Communications
- Navigation Systems
- Observation & Scientific Research
- Space Exploration
- Launchers
- Military

The high complexity of space systems makes virtually impossible for a simple company or even government agencies to encompass a whole space mission. Most missions are a joint effort of several companies, governments and space agencies that work in a customer-supplier fashion.

Space systems have evolved significantly during the last decades, from very simple passive devices to complex systems with intelligence capabilities. The increasing demand for on-board computing power in satellites and the new exploration missions with rovers is currently introducing technologies quite new to the space market, such as multi-core processors or SoC (System on Chip). These technologies open the door to in-flight software. In-flight software is a kind of embedded, real time software, and it is becoming more and more important in space missions, mainly due to its versatility and in-flight reconfiguration capabilities. However, this flexibility comes with new challenges that must be overcome.

One of these challenges is to guarantee that the software and its development meet the level of quality required by the space missions. To that purpose, the European Space Agency (ESA) has proposed a series of standards for software development that every partner involved in software activities must follow:

- ECSS-E-ST-40C: This Standard defines the principles and requirements applicable to space software engineering. The formulation of this Standard takes into account the existing ISO 9000 family of documents, and the ISO/IEC 12207 standard.
- ECSS-Q-ST-80C: This Standard contributes to provide adequate confidence to the customer and to the supplier that the developed or procured/reused software satisfies its requirements throughout the system lifetime. In particular, that the software is developed to perform properly and safely in its operational environment, meeting the quality objectives agreed for the project.
- OSRA (On-Board Software Reference Architecture): This architecture is designed for covering the needs of an OBSW development. It is sustained by the principles of component- and model-based software engineering. The SAVOIR-FAIRE (Space Avionics Open Interface Architecture - Fair Architecture and Interface Reference Elaboration) working group is intended to elaborate OSRA, and different ESA Research and Development activities have implemented the architecture and its specification.

ECSS-E-40 is based on the customer–supplier concept. This concept may be applied recursively, as would typically be the case for space projects with ESA as the customer at the top level, and then a chain of customer–supplier relationships extending downwards to the prime contractor and then to the lower levels of subcontractors. Reviews are the main interaction points between the customer and the supplier.

The assessment and certification process of in-flight software involves checking that all ECSS requirements for software development are met, from both an engineering perspective (ECSS-E) and product quality assurance (ECSS-Q). The supplier must provide proof of compliance while the customer (or the Agency) should be able to verify compliance in an efficient way. This is traditionally done based on scheduled meetings and documentation. However, the growing complexity of space systems and the collaborative spirit of the space industry demand a more advanced methodology to guarantee that all requirements related to safety, security and assurance between customer and supplier are met.

2.7.2 Stakeholders

Agency: the European Space Agency (ESA) is usually the prime contractor of the space missions. It defines each mission parameters and requirements and flows them down to the different subcontractors (ground segment, launch equipment and flight components). It also acts as a supervisory entity, making sure that all the components are designed and developed according to the applicable space standards.

Customer: in the context of in-flight software for space applications, the customer is usually the system designer and hardware/software integrator. The customer derives the software requirements from the system specification and flows them down to the software supplier. It is normally the responsible for integration testing and validation.

Supplier: in this context, the supplier is responsible for developing the software according to the customer requirements and applicable space standards. The level of testing and integration support is usually agreed with the customer.

2.7.3 Business Process

Based on the definition of usage scenarios provided in D1.1 [9], a number of generalized space business cases have been defined:

- BC1: Reduce efforts and costs for managing compliance with ECSS standard.
- BC2: Managing Software dependability and safety

2.7.3.1 BC1 Reduce efforts and costs for managing compliance with ECSS standard

Companies working for the European space industry must declare compliance metrics documenting conformance to individual ECSS standard requirements applicable to the project (see Figure 18 and Figure 19). Normally the compliance statement is a reference to the project documentation explaining how the project ensures fulfilment of the requirements. The referenced project documentation should be a tailoring of company standard processes for that specific project.

1. Generate compliance to ECSS standard requirements metrics.
2. Perform compliance gap analysis.
3. Re-use processes, procedures, methods, templates and forms between project activities performed by the company organisation.
4. Publish company processes to make them available to the company organisation.

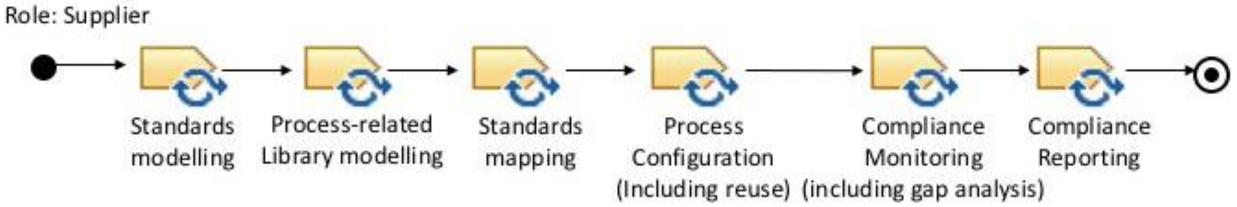

Role: Supplier
Standards modelling
Process-related Library modelling
Standards mapping
Process Configuration (Including reuse)
Compliance Monitoring (including gap analysis)
Compliance Reporting

Figure 18. Compliance management and reuse

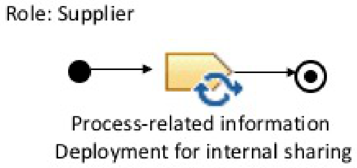


Figure 19. Process-related information sharing

2.7.3.2 BC2: Managing Software dependability and safety

Figure 20 describes the process followed for the safety assessment in the space domain. In this process, two different stakeholders shall interact and Safety and Dependability properties will be managed from the different perspectives of the stakeholders. The activities related to the safety assessment performed by the stakeholders are the following:

- **Customer**: Analyses the system requirements, flows them down to the SW supplier, and performs safety and dependability analysis and the final integration and verification.
- **Supplier**: Specifies the SW technical description based on SW requirements, performs the SW RAMS analysis, designs and develops the software and performs verification and validation at SW level.

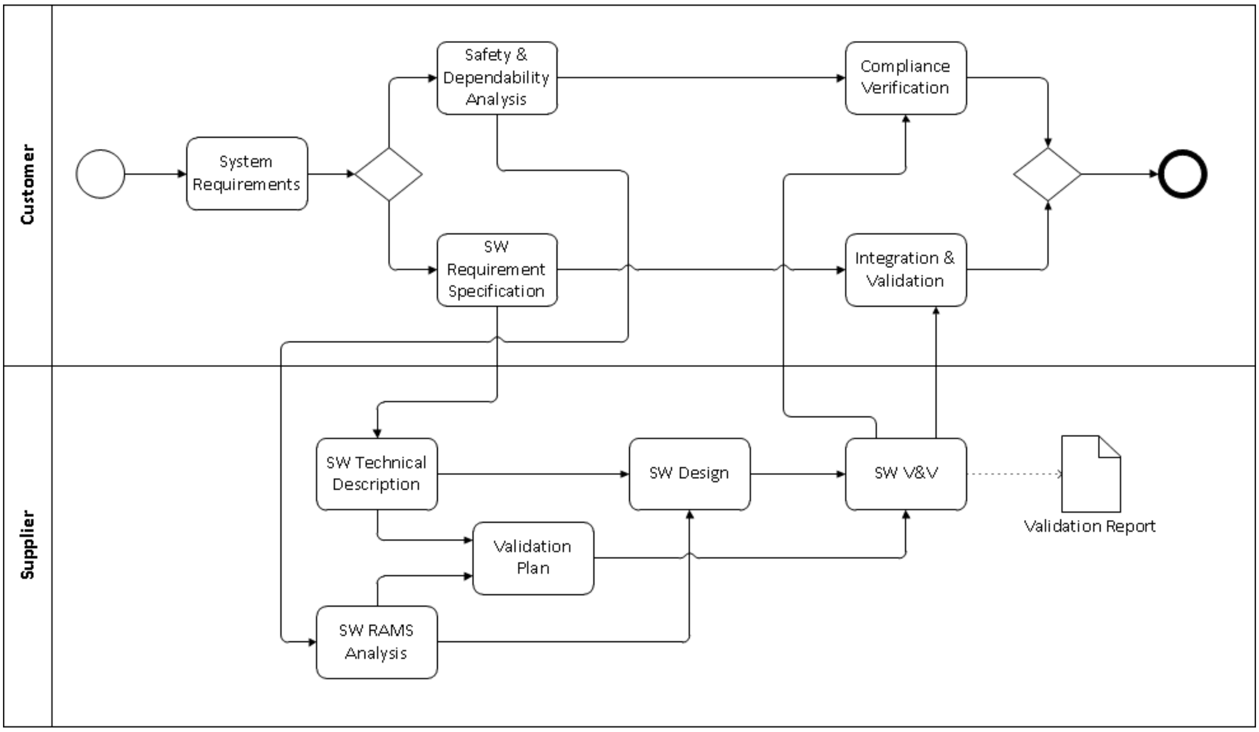


Figure 20. Safety assessment business process for the space domain

2.7.4 Value Proposition

The value proposition of AMASS in the space domain is the following:

AMASS Goal 1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.

- Validating the code while flying: to not to stop or invalidate the mission or the results if a change in code is needed (make the software confidence). Code peer review for safety critical functions is of mandatory, as no certified code generator is used in-flight.
- Reduce efforts and costs for managing compliance with targeted standards: by validating only the parts that have been modified instead of the whole code. Assurance that the no-modified code is still compliant with the standards.

AMASS Goal 2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.

- Reuse of process-related assurance results. AMASS will support the reuse of already successful artefacts resulting from compliance-related processes execution, for instance, approved development plans can be identified to be reused into other projects which will reduce the cost of future projects.
- Reuse of product-related assurance results. AMASS will support the systematic reuse of previously developed and assure products. For instance, software components can be reused in terms of unit design specifications and corresponding argumentation in other projects.

AMASS Goal 3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new CPS products.

- N/A

AMASS Goal 4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification tool technologies by 60%.

- N/A

2.8 Air Traffic Domain

2.8.1 Introduction

The Air Traffic Domain comprises many complementary services, all aimed to the safety and efficiency of the air transport operations. Such services mainly provide two categories of functions: regulatory functions and technical-operative functions.

The regulatory functions include activities like aircraft certification, personnel licensing, generation of operating rules, practices and standards to govern air traffic, etc.

The technical-operative functions include the production of operational performance standards for air traffic technologies and infrastructures.

The main air traffic services can be grouped, as an indication, under the following areas:

- Air Traffic Control (on the airport control zone, including ground surveillance, on the approach paths, on the en-route controlled airspace).
- Communications (mainly air-ground and ground-ground).
- Navigation, which provides en-route navigation (DVOR, DME) and approach and landing aids (DME and ILS); GPS and inertial systems are also main components of such service.
- Weather information (about meteorological conditions, winds hear and wake turbulence, volcanic ash, but also possible bird strikes).

Within Air Traffic Management (ATM) domain, the radio-navigation equipment (often defined Navigation Aids, or NavAids) are currently the most widespread systems for providing aircrafts with exact location in space and time. They are CPS based on the joint contribution from the physical electromagnetic fields which govern the positioning mechanism and sophisticated computation processes.

Among such systems, the DME system is a Distance Measuring Equipment, which provides pilots with distance information between the aircraft and the location of the DME ground equipment. Basically, the airborne DME transmitter interrogates the DME ground station, which replies after a fixed and known delay. An additionally, variable delay is proportional to the distance between the airborne interrogator and the ground station: from this variable delay, it is possible to compute such distance. The system is used for both en-route and terminal area guidance.

Nowadays, in addition to its original scope, DME has been identified as one of the most promising solutions for the new APNT (Alternative Position, Navigation, and Timing) programs: APNT solutions are aimed to mitigate the effects of a satellite navigation (SATNAV) service disruption and are conceived to support RNAV/RNP (aRea NAVigation: it is a method of navigation which permits the operation of an aircraft on any desired flight path, not only on point-to-point straight paths). RNAV/RNP is one of the pillars of the future flight concepts, aimed to optimize en-route trajectories and operations, to avoid long holding or taxiing times of aircrafts, to reduce route length (and so time, fuel consumption, air-space occupancy, CO^2 emissions, etc.). Typical APNT architectures based on DME are "DME/DME" and "DME/DME/IRU" (IRU: Inertial Reference Unit), both adequate to provide the accuracy level required by RNAV (and, under certain conditions, by RNP, where RNP stands for Required Performance Navigation and is an evolution of RNAV).

DME, as well as other navaid systems, is subject to the strict ICAO (International Civil Aviation Organization) accuracy requirements and to severe constraints in terms of service integrity/continuity/availability. This makes some aspects of DME design technology (requirement-to-design mapping, testing, validation, certification) predominant issues. This is especially true for the core subsystem dedicated to assure the integrity of the system, the Monitoring subsystem: it measures the quality and the performance of the radiated signal, as well as the internal parameters of the equipment. Based on such assessment the

subsystem automatically and autonomously defines the reliability of the positioning service provided to aircrafts, extending such assessment to making the service unavailable.
According to the EUROCONTROL Safety Assessment Methodology (SAM), the complete software-lifecycle safety assurance is covered by the following ATM regulations, norms and standards:

A. RTCA Inc. DO-178B. Software Considerations in Airborne Systems and Equipment Certification. RTCA Inc. / EUROCAE. DO-178B/ED-12B. 1992.

B. RTCA, EUROCAE. DO-278 / ED-109. Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance. RTCA Inc. / EUROCAE. DO-278/ED-109. 3/5/2002.

C. RTCA Inc. / EUROCAE. DO-278A/ED-109A. Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems. December 2011.

D. Eurocontrol. ESARR6. Eurocontrol Safety Regulatory Requirement 6 Software in ATM Functional Systems. May 2010.

E. Eurocontrol. ESARR4. Eurocontrol Safety Regulatory Requirement 4 Risk Assessment and Mitigation in ATM. April 2001.

F. EUROCAE. ED-153. Guidelines for ANS Software Safety Assurance. August 2009.

G. RTCA Inc. / EUROCAE. DO-178C / ED-12B. Software Considerations in Airborne Systems and Equipment Certification. December 2011.

H. RTCA Inc. / EUROCAE. DO-330 / ED-215. Software Tool Qualification Considerations. December 2011 - January 2012.

I. RTCA Inc. / EUROCAE. DO-331 / ED-216. Model-Based Development and Verification Supplement to DO-178C and DO-278A / Model-Based Development and Verification Supplement to ED-12B and ED-109A. December 2011 - January 2012.

J. RTCA Inc. / EUROCAE. DO-332 / ED-217. Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A / Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A. December 2011 - January 2012.

K. RTCA Inc. DO-333 / ED-218. Formal Methods Supplement to DO-178C and DO-278A / Model-Based Development and Verification Supplement to ED-12C and ED-109A. December 2011.

For a safety-critical system such as DME, model-based formal approaches to the validation and verification of SW design (and re-design) represent an answer to the already mentioned safety issues and result in an increase in overall safety and maintainability of such CPS.

The ATM department of Thales Italia (THI) will drive an industrial case study aimed to re-engineer, through the usage of tools and methods provided by the AMASS project, both the SW of the DME Monitoring subsystem and the SW development processes, applying the CNS/ATM safety certification standards (EUROCAE ED-109', 'RTCA DO-278', 'EUROCAE ED-153').

2.8.2 Stakeholders

As far as the systems of Navigation domain are concerned, the main involved stakeholders are, potentially:

- Standardisation organizations: EUROCONTROL and EUROCAE, in cooperation with ICAO, IATA etc.
- Manufacturers
- ATM (Air Traffic Management) service providers: ANSPs. E.g.: AENA-ES, DCAC-FR, DFS-DE, ENAV-IT, FAA-US, NATS-UK, etc.
- Service and system users: airports, airlines, jetliners manufacturers etc.

Standardisation organizations: their concern is the system's compliance to the standards, resulting in their interest in a platform that supports the standard compliance and certification processes.

Manufacturers: systems, which play a key role in positioning techniques and in air traffic management procedures, are intrinsically "safety critical". For companies, which design, develop and manufacture such systems, Safety, Performance, Maintainability and Certification issues represent the main factors impacting on all phases of the product lifecycle.

Methods and tools provided by AMASS will therefore improve all the involved processes: specification, (re-)design, development, implementation, validation, maintenance, upgrade, integration of legacy SW , etc.

The above improvements will boost the efficiency of the quality processes, guaranteeing that the whole Software Development Process follows the correct procedure according to the CNS/ATM standards.

Costs and efforts for the whole development cycle will also be reduced by introducing the qualification & certification principles, as well as safety information, already at architecture level.

Service Providers and Users: ATM authorities, in charge of governing and providing an efficient ATM service, as well as the beneficiary of such services (through the use of the relevant systems), shall be interested in a platform which can guarantee higher levels of safety assurance for systems and equipment.

In the concrete, higher safety levels in the air-navigation domain result in:

- lower risk of deviation from the planned or required route
- lower risk of separation-loss
- lower risk of collisions

2.8.3 Business Process

Based on the definition of usage scenarios provided in D1.1 [9], two generalized business cases, concerning the NavAids sector of the Air Traffic domain, have been defined:

- BC1: Reduce efforts and costs for safety assessments of NavAids systems, in compliance with 'EUROCAE ED-109', 'RTCA DO-278' and 'EUROCAE ED-153'
- BC2: Reduce efforts and costs for SW certification (and re-certification)

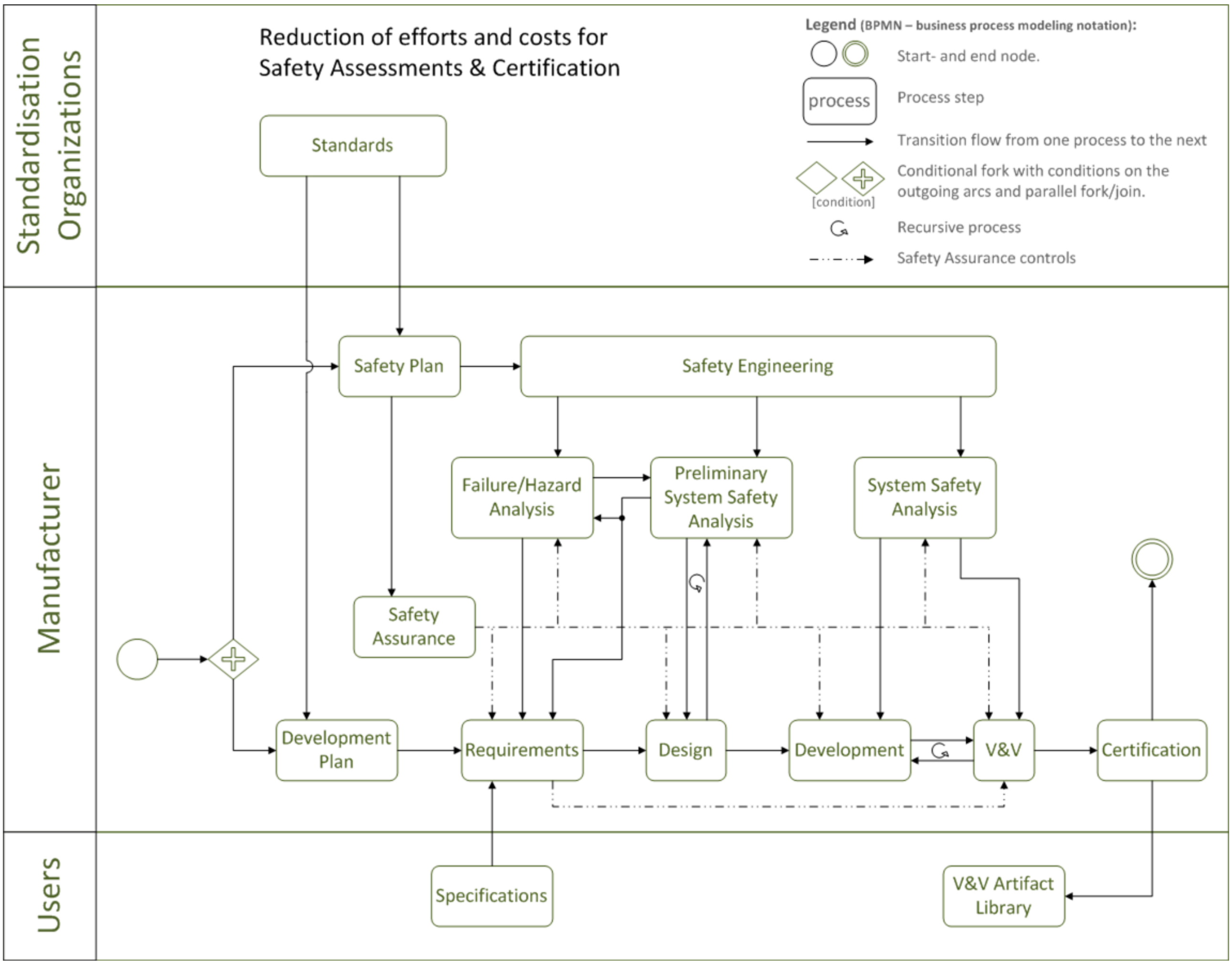

Standardisation Organizations
Manufacturer
Users
Reduction of efforts and costs for Safety Assessments & Certification
Legend (BPMN – business process modeling notation):
Start- and end node.
process
Process step
Transition flow from one process to the next
[condition]
Conditional fork with conditions on the outgoing arcs and parallel fork/join.
Recursive process
Safety Assurance controls
Standards
Safety Plan
Safety Engineering
Failure/Hazard Analysis
Preliminary System Safety Analysis
System Safety Analysis
Safety Assurance
Development Plan
Requirements
Design
Development
V&V
Certification
Specifications
V&V Artifact Library

Figure 21. Safety assessment business process for the air traffic domain

2.8.3.1 BC1: Reduce efforts and costs for safety assessments of NavAids systems, in compliance with 'EUROCAE ED-109', 'RTCA DO-278' and 'EUROCAE ED-153'

Figure 21 shows the typical process flow which underlies the safety assessment and certification of a safety critical software system like a NavAid system.

Some key-factors are highlighted by the diagram:

- the final result of the safety process is not a pure hazard analysis report. On the contrary, the hazard analysis must be introduced in the early phases of the development, to influence the design of the system and to ensure that it is safe, not only that the risks are identified and quantified;
- the safety engineer is not an isolated figure: the safety process involves the safety engineer, software engineer, system engineer, software quality engineer, configuration management engineers, test & evaluation engineers, verification & validation engineers, etc.;
- both Safety Analysis (SA) and Verification & Validation processes have a recursive impact on Design and on Development, respectively;
- **Safety Planning** must anticipate and influence all the software lifecycle phases: requirements, design, coding and testing. Such approach is crucial, in that the risks associated with the software often remain hidden until late in the system design.

It is clear from the diagram that the **Safety Plan** (and its operating procedures, grouped under the umbrella of “Safety Engineering”) must provide that (from FAA Safety Handbook):

i. software application concepts are examined to identify hazards/risks within safety critical software functions;

ii. requirements and specifications are examined for hazards (e.g. identification of hazardous commands, processing limits, sequence of events, timing constraints, failure tolerance, etc.);

iii. design and implementation is properly incorporated into the software safety requirements;

iv. appropriate verification and validation requirements are established to assure proper implementation of software system safety requirements;

v. test plans and procedures can achieve the intent of the software safety verification requirements;

vi. the whole software safety program is properly monitored and controlled;

vii. results of software safety verification efforts are satisfactory and recorded into a Safety Assessment Report to be stored into a library associated to the system/product and available to all the stakeholders.

Summarizing, a sort of "circular" process must be implemented, where one of the first steps, relevant to safety constraints, consists in flowing down the hazard control measures into requirements. This results, in its turn, in a feedback trail between the consequent design (including the implemented software safety requirements), the risk associated to the requirement and a new iteration of the FHA/SA (affecting the requirements).

Such process also provides an audit trace between safety-critical requirements and tests (V&V process), providing in turn:

- evidence for each functional hazard, mitigated by comparing to requirements;
- evidence for each functional hazard, mitigated by comparing to design;
- verification of Safety requirement Implementation through test;
- capability of executing residual risk assessment;
- capability of verifying accordance of the developed software with applicable standards and criteria.

Possible concerns, associated to the flow-down process mentioned above, can arise from incomplete and/or inconsistent analysis of the system: this emphasizes the opportunity of dealing with such concerns by the adoption of formal methods for requirements analysis and the inherent flow-down mechanism mentioned above. Formal methods, although not able to quantitatively predict a level of reliability, provide a methodology which gives the highest degree of assurance for a dependable software system.

Formal methods support is expected to be provided by the AMASS platform, already for the early phases of a system lifecycle, for requirement definition, models validation, etc., as shown in Figure 22.

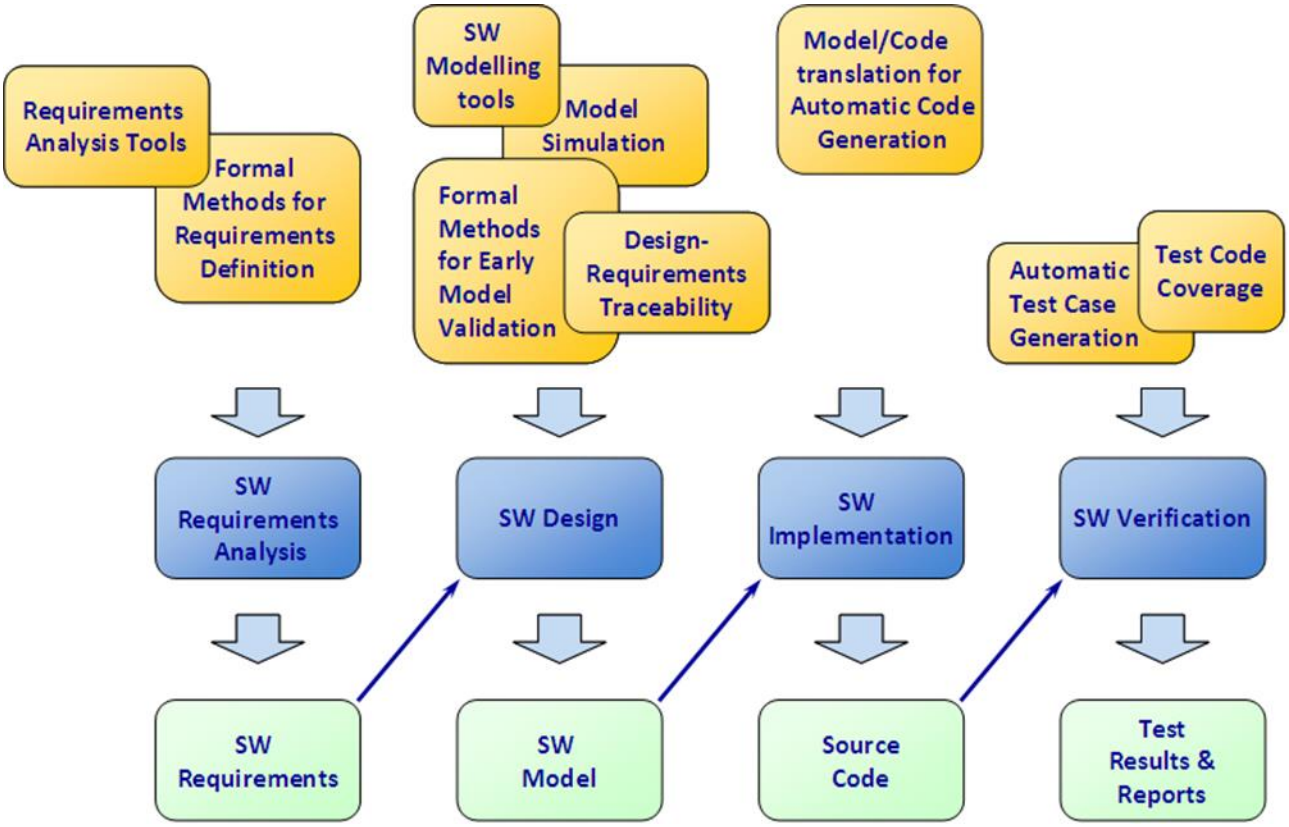

Requirements Analysis Tools
Formal Methods for Requirements Definition
SW Modelling tools
Model Simulation
Formal Methods for Early Model Validation
Design-Requirements Traceability
Model/Code translation for Automatic Code Generation
Automatic Test Case Generation
Test Code Coverage
SW Requirements Analysis
SW Design
SW Implementation
SW Verification
SW Requirements
SW Model
Source Code
Test Results & Reports

Figure 22. System design lifecycle phases

Requirement analysis tools are also expected for the initial phase of the system lifecycle, to designate a requirement as “safety critical”. Requirement traceability and code coverage are also AMASS tools essential to support safety assessment/assurance and software certification.

It is evident from Figure 21 that the only stakeholder directly involved alongside the manufacturer within the process flow, at least in the first and main instance, belongs to the “users” category. Users are key responsible for “specifications”, which are the origin of the starting software-safety analysis and sometimes, unfortunately, of some initial failure mechanisms. Actually, “specifications” are the first source of “requirements” and a specification error (an omission, an improper or misunderstood statement, an inaccurate document, etc.) can mislead the software behaviour: software may be developed "correctly" with regard to the specification, but wrong from a systems perspective. This is probably the single largest cause of software failures and/or errors [source: FAA], which requires a great effort of reciprocal comprehension between users and manufacturers.

2.8.3.2 BC2: Reduce efforts and costs for software certification (and re-certification)

All the considerations expounded at the previous chapter clearly apply also to the software certification process, which is the final result of the V&V procedures within the development process.

2.8.4 Value Proposition

The value proposition of AMASS in the NavAids sector of the Air Traffic domain is the following:

<u>AMASS Goal 1:</u> to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.

- Tools and methods for the early introduction, into the development process, of safety requirements. AMASS is expected to provide, within the assurance processes of the design phase, modeling tools to advance the inclusion of safety information into the architectural design.
- Methods for early models validation and for verification. AMASS is expected to provide methods and tools for early software-design validation, especially through the usage of contracts and formal methods for module interaction definition.

AMASS Goal 2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.

- Tools for automatic generation of reports, checklists and evidences to support the certification. Automatic check to verify that all the DO-278 / ED-109 objectives have been satisfied. AMASS is expected to provide processes suited to guarantee that the software lifecycle follows the correct procedure according to the CNS/ATM standards.
- Architectural Design tool should be integrated with Evidence and Compliance Management tools to be able to reduce the re-certification effort in case of bug correction or any other change for an already certified system.

AMASS Goal 3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new CPS products.

- N/A

AMASS Goal 4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification tool technologies by 60%.

- N/A

3. Requirements

3.1 Introduction

The requirements to be met by the technical AMASS work packages (WP3-WP6) are organized based on which block from the general AMASS architecture they belong to.

A number of steps is followed in the process of creating the high-level requirements. These steps are depicted in Figure 23.

The process for requirements elicitation, analysis, specification, and validation have not been followed in a strict order, rather we forced to do a number of iterations to come to the result as described in this deliverable. All the process has been done in coordination with the project technical work packages (WP3-WP6) and in close relation with the implementation team.

The following project deliverables have been taken into account as inputs for the process:

- D1.1 Case studies description and business impact [9]
- D2.2 AMASS Reference architecture [12]
- D3.1 Baseline and requirements for architecture-driven assurance [1]
- D4.1 Baseline and requirements for multi-concern assurance [2]
- D5.1 Baseline requirements for seamless interoperability [3]
- D6.1 Baseline and requirements for cross/intra-domain reuse [4]

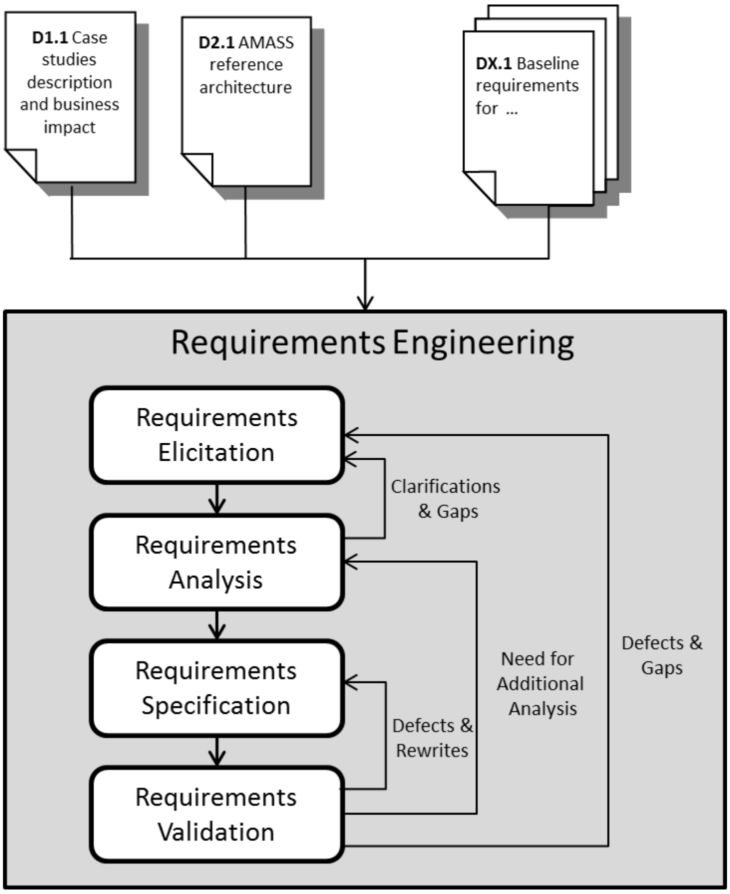

D1.1 Case studies description and business impact
D2.1 AMASS reference architecture
DX.1 Baseline requirements for …
Requirements Engineering
Requirements Elicitation
Requirements Analysis
Requirements Specification
Requirements Validation
Clarifications & Gaps
Need for Additional Analysis
Defects & Gaps
Defects & Rewrites

Figure 23. Requirements engineering steps followed

In order to describe the AMASS requirements, we will refer to AMASS-related actors (see Figure 24). The actors are in some of these groups:

- **Management**: It includes managers from the most important hierarchically (Project Manager) to the Assurance Manager, which is an AMASS-specific actor artificially created to represent a manager who is in charge of managing all the processes and activities involved in the AMASS platform usage. This group also includes an IT Manager who is in charge of managing and setting the AMASS tool platform, as an IT infrastructure.
- **Engineers**: Any actor involved in the execution of development, V&V and safety-security analysis activities. We separate safety and security engineers, since some activities may need to distinguish according to the targeted concern (safety and security).
- **Assessors**: Two kind of assessors need to be distinguished: internal to the company and external or independent assessor.

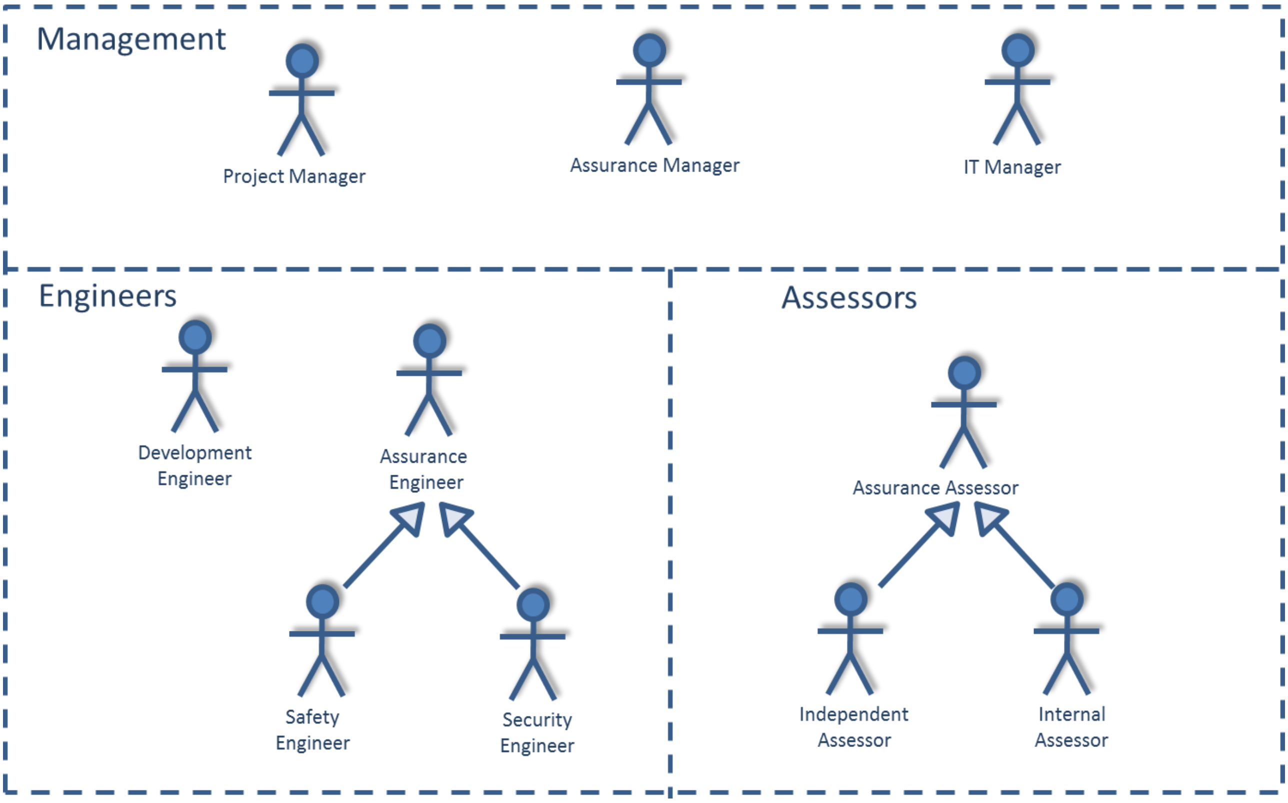


Figure 24. Actors of the AMASS Tool Platform

The requirements definition will follow the template shown in Table 1:

Table 1. Template for requirements

Id [Original ID - The ID used in your requirements management system. A single project cannot have two requirements with the same original ID]	**Short Description]** [Short description of the requirement]
Description	[Detailed definition of the requirement]
Assigned WP	[The Work Package this requirement is assigned to. It might me assigned to several work packages or even be a transversal requirement]
Relation to other requirements	[ID of the other requirements which this requirement has a relation]
Actor	[A person in a certain role or different system interacting with the system of interest: Assurance Manager, Product Engineer[2], Assurance Assessor (Independent/Internal), System Administrator, Configuration Manager]
Priority	[MoSCoW priority][3]
Type	[Functional or Non-functional][4]
Non-functional category	[Cost/Price, Design Constraint, Memory Storage, Performance, Physical Power Consumption, Reliability, Safety, Security, Standard Compliance, Usability]
Rationale	[Rationale, the why behind this requirement]

[2] Development Engineer, V&V Engineer, Assurance Engineer

[3] Must have, Should have, Could have, and Won't have but would like

[4] Non-functional requirements describe the quality of functional requirements

3.2 High Level Requirements related to AMASS Platform Basic Building Blocks

3.2.1 System Component Specification

Table 2. High Level Requirements for System Component Specification

WP3_SC_001	System abstraction levels browsing
Description	The user must be able to browse along the different abstractions levels (system, subsystem, and component).
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Development Engineer, Assurance Engineer, Assurance Assessor, Assurance Manager
Priority	Must
Type	Functional
Rationale	By browsing the different abstraction levels it is then possible to apply related activities, like editing and verification.

WP3_SC_002	System abstraction levels editing
Description	The user must be able to edit the different abstractions levels (system, subsystem, and component).
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Development Engineer, Assurance Engineer
Priority	Must
Type	Functional
Rationale	The ARTA shall provide features for system architecture editing, to later enable architecture-driven assurance.

WP3_SC_003	Modelling languages for component model
Description	The system should be able to support different modelling languages to model the component/subsystem/system.
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Development Engineer, Assurance Engineer
Priority	Should
Type	Functional
Rationale	End-users typically make use of different modelling languages (UML, AADL, Matlab/Simulink).

WP3_SC_004	Formalize requirements into formal properties
Description	The system must be able to formalize requirements into formal properties (i.e., expressions in a language with a formal semantics such as for example temporal logics)
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Product Engineer, Assurance Engineer
Priority	Must
Type	Functional
Rationale	Formalization of requirements can enable application of formal verification.

WP3_SC_005	Requirements allocation
Description	The system must provide the capability for allocating requirements to parts of the component model. More in general, requirements traceability shall be enabled.
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Development Engineer, Assurance Engineer
Priority	Must
Type	Functional
Rationale	Requirement traceability is especially relevant when developing safety-critical systems.

WP3_SC_006	Specify component behavioural model (state machines)
Description	The system must allow the specification of component behavioural model.
Assigned WP	WP3
Relation to other requirements	
Actor	Development Engineer, Assurance Engineer
Priority	Must
Type	Functional
Rationale	Behavioural models allows model-driven support for verification

WP3_SC_007	Fault injection (include faulty behaviour of a component)
Description	The system must allow the user to specify faults and fault injections (i.e., how faults affect the nominal behavioural model).
Assigned WP	WP3
Relation to other requirements	WP3_SC_006
Actor	Assurance Engineer
Priority	Must

Type	Functional
Rationale	The specification of fault injection allows the model-based analysis of the behavioural models (e.g., for automatic generation of fault trees and FMEA tables).

3.2.2 Assurance Case Specification

Table 3. High Level Requirements for Assurance Case Specification

WP4_ACS_001	Assurance case edition
Description	The system shall be able to edit an assurance case in a scalable way.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Non-functional
Rationale	Scalable editing of an assurance case. Stakeholder need: Working efficiently and effectively.

WP4_ACS_002	Argumentation architecture
Description	The system shall be able to edit a modular structure (argument architecture) associated with a system and/or component.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Edit an argument architecture associated with a system and/or component. Stakeholder need: Working efficiently and effectively.

WP4_ACS_003	Drag and drop argumentation patterns
Description	The system shall be able to instantiate in the actual assurance case an argument pattern (concerning safety and security) selected from the list of patterns stored.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Easy drag and drop selection from the list of stored patterns. Stakeholder need: Working efficiently and effectively.

WP4_ACS_004	Provide guidelines for argumentation patterns
Description	The system should be able to provide guidelines to use and instantiate argument pattern (concerning safety and security) presented in the actual assurance case.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Should
Type	Functional
Rationale	Providing guidelines for argumentation patterns. Stakeholder need: Working efficiently and effectively.

WP4_ACS_005	Provide a structured language to the text inside the claims
Description	The system could be able to provide support for language formalization inside argument claims.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Could
Type	Functional
Rationale	Providing support for language formalization inside arguments claims. Stakeholder need: Working efficiently and effectively.

WP4_ACS_006	Provide guidelines for argumentation
Description	The system could be able to provide guidelines about the assurance case edition based on the system/component development phase status.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Could
Type	Functional
Rationale	Provide guidelines for argumentation. Stakeholder need: Working efficiently and effectively.

WP4_ACS_007	Argumentation import/export
Description	The system could be able to import/export argumentations to SACM.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Could

Type	Functional
Rationale	Import/export argumentation to SACM. Stakeholder need: Working efficiently and effectively.

WP4_ACS_008	Traceability of the dependability case
Description	The system should provide the dependability case reviewers the ability of tracing an overall dependability case (GSN) goal to the requirement within the dependability profile for a given system element and the attribute of interest with which goal is associated.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Should
Type	Functional
Rationale	Traceability of the dependability case. Stakeholder need: Working efficiently and effectively

WP4_ACS_009	Find high level claims
Description	The system shall be able to find high level claims, which are sufficiently cohesive to be supported by extremely diverse strands of argument, supported by diverse types of evidence.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Find high level claims. Stakeholder need: Working efficiently and effectively

WP4_ACS_010	Composition of the overall argument
Description	The system should provide the capability of generating a compositional assurance case argument.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Should
Type	Functional
Rationale	Capability of generating a compositional assurance case argument. Stakeholder need: Working efficiently and effectively.

WP4_ACS_011	Assurance case status report
Description	The system could provide the capability for querying the assurance case in order to detect: 1) undeveloped goals, 2) fallacies.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Could
Type	Functional
Rationale	Capability for querying the assurance case. Stakeholder need: Detection of undeveloped goals and fallacies.

WP4_ACS_012	Formal validation of assumptions and context when arguments modules are connected
Description	The system could be able to indicate the validation of assumptions contained in argument modules every time the modules are connected and/or modified
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Could
Type	Functional
Rationale	Need of formal validation when arguments modules are connected/modified. Stakeholder need: Working efficiently and effectively.

WP4_ACS_013	Provide quantitative confidence metrics about an assurance case in a report
Description	The system could produce a status report indicating a quantitative confidence metric for assurance case.
Assigned WP	WP4
Relation to other requirements	WP4_ACS_011
Actor	Safety Engineer together with Security Engineer
Priority	Could
Type	Functional
Rationale	Providing quantitative confidence metrics for assurance case. Stakeholder need: Working efficiently and effectively.

3.2.3 Evidence Management

Table 4. High Level Requirements for Evidence Management

WP5_EM_001	Evidence characteristics specification
Description	The AMASS Tool Platform shall allow an assurance engineer to specify the characteristics of assurance evidence.
Assigned WP	WP5

Relation to other requirements	WP5_EM_002, WP5_EM_004, WP5_EM_010
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	The characteristics of the artefacts used as assurance evidence must be recorded for CPS assurance and certification purposes.

WP5_EM_002	**Evidence traceability**
Description	The AMASS Tool Platform shall allow an assurance engineer to specify relationships between evidence artefacts.
Assigned WP	WP5
Relation to other requirements	WP5_EM_009
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Relationships between evidence artefacts might have to be recorded for several purposes, e.g. impact analysis and certification.

WP5_EM_003	**Evidence change impact analysis**
Description	When an evidence artefact is changed, the AMASS Tool Platform shall indicate how the change impacts other evidence artefacts.
Assigned WP	WP5
Application Domain	General
Relation to other requirements	WP5_EM_002, WP5_EM_011
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	Changes in some evidence artefact might affect others. This must be analysed.

WP5_EM_004	**Evidence evaluation**
Description	The AMASS Tool Platform shall allow an assurance manager engineer to specify information about the results from evaluating an evidence artefact.
Assigned WP	WP5
Relation to other requirements	WP5_EM_010
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	It can be necessary to evaluate the properties and quality of evidence artefacts (e.g. completeness and consistency).

WP5_EM_005	Evidence information import
Description	The AMASS Tool Platform shall be able to import information about evidence artefacts.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_004, WP5_TI_005, WP5_TI_006, WP5_TI_007, WP5_TI_008, WP5_TI_009, WP5_TI_010
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	Information about evidence artefacts might be originally created in external tools.

WP5_EM_006	Evidence information export
Description	The AMASS Tool Platform shall be able to export information about evidence artefacts.
Assigned WP	WP5
Relation to other requirements	WP5_TI_002, WP5_TI_004, WP5_TI_005, WP5_TI_006, WP5_TI_007, WP5_TI_008, WP5_TI_009, WP5_TI_010
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	External tools might need to collect information about evidence artefacts created with the AMASS Tool Platform.

WP5_EM_007	Derivation of evidence characterization model
Description	The AMASS Tool Platform shall derive an evidence characterisation model from the baseline of an assurance project.
Assigned WP	WP5
Relation to other requirements	WP6_CM_002
Actor	Assurance manager
Priority	Should
Type	Functional
Rationale	When specifying information about evidence artefacts, an overall structure of the information can be derived from the baseline of an assurance project.

WP5_EM_008	Visualization of chains of evidence
Description	The AMASS Tool Platform shall display the chains of evidence to which an evidence artefact belongs.
Assigned WP	WP5
Relation to other requirements	WP5_EM_002
Actor	Assurance manager, Assurance engineer
Priority	Could
Type	Non-functional

Non-functional category	Usability
Rationale	Showing traceability between evidence artefacts in the form of chains of evidence can help users to gain insights into artefact relationships on a single information source.

WP5_EM_009	Suggestion of evidence traces
Description	When specifying relationships for an evidence artefact, the AMASS Tool Platform shall suggest evidence artefacts to which the first evidence artefact might relate.
Assigned WP	WP5
Relation to other requirements	WP5_EM_002
Actor	Assurance engineer
Priority	Could
Type	Functional
Rationale	Evidence trace specification can be difficult, time-consuming, and error-prone due to the amount of evidence information in an assurance project. Suggestion of evidence traces can facilitate the activity.

WP5_EM_010	Evidence lifecycle information storage
Description	The AMASS Tool Platform shall allow an assurance engineer to specify the events that have occurred during the lifecycle of an evidence artefact.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	It can be necessary to keep track of all the events occurred during an evidence artefact’s lifecycle.

WP5_EM_011	Interactive evidence change impact analysis
Description	The AMASS Tool Platform shall allow an assurance manager to indicate what evidence artefacts are actually impacted by the changes to a given evidence artefact.
Assigned WP	WP5
Relation to other requirements	WP5_EM_003
Actor	Assurance manager
Priority	Should
Type	Functional
Rationale	A user should not only know what evidence artefacts are impacted by changes in another artefact, but also select what evidence artefact are actually impacted.

WP5_EM_012	Evidence trace verification
Description	The AMASS Tool Platform shall analyse the quality of the relationships between evidence artefacts.
Assigned WP	WP5
Relation to other requirements	WP5_EM_002
Actor	Assurance engineer, Assurance manager
Priority	Could
Type	Functional
Rationale	Evidence trace specification can be difficult, time-consuming, and error-prone due to the amount of evidence information in an assurance project. Verification of evidence traces can be essential.

WP5_EM_013	Link of evidence to other assets
Description	The AMASS Tool Platform shall allow an assurance manager to link evidence artefacts with other assurance assets.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	Evidence artefact relate to other assurance assets, e.g. process assets.

WP5_EM_014	Evidence resource specification
Description	The AMASS Tool Platform shall allow an assurance engineer to indicate the location of the resource that an evidence artefact represents in the system.
Assigned WP	WP5
Relation to other requirements	WP5_EM_015
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Evidence artefacts are usually stored physically and originally in some external resource.

WP5_EM_015	Resource part selection
Description	When indicating the location of the resource that an evidence artefact represents in the system, the AMASS Tool Platform shall allow an assurance engineer to select a part of the resource (e.g. a section inside a document or a component model file within a large system model).
Assigned WP	WP5
Relation to other	WP5_EM_014

requirements	
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need identified in D5.1 (As a tool user working with evidence management I want to point to specify information about a Section of a given document (e.g., a System Requirement specified inside a MS Word document) so that I can refer/point out to this section for change management, traceability, etc.).

WP5_EM_016	Evidence report generation
Description	The AMASS Tool Platform shall be able to automatically generate reports, checklists, and evidence for certification purposes.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	Need reflected in the CS9

3.2.4 Compliance Management

Table 5. High Level Requirements for Compliance Management

WP6_CM_001	Modelling of standards
Description	The AMASS tools shall be able to model a set of industrial standards (including the parts, objectives, practices, goals/requirements, criticality levels from the standards)
Assigned WP	WP6
Relation to other requirements	WP6_CM_002
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Standards are composed of hundreds of pages and usually contain thousands of requirements. To be compliant with the standards, manufacturers/suppliers have to fulfil the requirements. By digitalizing the information/requirements contained in the standards in a common format (which can be retrieved, elaborated, and stored), compliance management becomes easier since the fulfilment becomes traceable. Stakeholder need: Facilitate the visualization and management of standards-related information/requirements.

WP6_CM_002	Tailoring of Standards models to specific projects
Description	The AMASS tools shall enable the tailoring of Standards models to specific

	project (e.g., by establishing the parts of the Standard that apply to a given assurance project).
Assigned WP	WP6
Relation to other requirements	WP6_CM_001
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	In order to get the certificate from certification bodies, a two-stage certification process is typically adopted. First, manufacturers/suppliers have to illustrate how, within their specific project, they plan to comply with the requirements included in the standards. This is a very demanding task as applicants usually have to negotiate their interpretation. Stakeholder need: To facilitate the specification of how to comply with a standard in a specific project.

WP6_CM_003	Correlating processes to the requirements
Description	The AMASS tools shall enable the correlation of compliance requirements with processes for compliance checking of the requirements in order to allow the users (e.g., safety assessors, compliance officers) to get a view of which compliance requirements are related to the specific task of a process, possibly with some specific criteria. This will save time and costs involving the identification of compliance requirements pertaining specific processes.
Assigned WP	WP6
Relation to other requirements	WP6_CM_001, WP6_CM_002
Actor	Assurance Managers, Safety (Security, etc.) Assessor
Priority	Must
Type	Functional
Rationale	Within large process repositories, it is tedious and error prone to manually scan process models to decide about their relevance to certain compliance rules. Providing tools and techniques that help that systematically access process repository (e.g. safety processes from databases) and querying for processes based on the specific criteria can be considered as a valuable support to establish connection between the safety processes and compliance rules. Correlating the rules with processes allows automated compliance checking, yet in loosely coupled fashion.

WP6_CM_004	Triggering compliance Checking
Description	The AMASS tools shall provide the functionality for automatically triggering the requirements for (re)checking the compliance of safety processes against rules – especially, when there is change in the standards/ regulations.
Assigned WP	WP6
Relation to other	N.A.

requirements	
Actor	Assurance Managers
Priority	Must
Type	Functional
Rationale	Usually checking is triggered by users. The compliance support system should be proactive in telling the user about the need to (re)check. Whenever, a safety requirement (or a process) is changed, the system should advise the assurance managers a re-run of compliance checking. This allows an instant response to changes in the rules repository or the process repository and providing a tight follow up on the compliance status of safety processes.

WP6_CM_005	Compliance Monitoring
Description	The AMASS tools shall support web-based monitoring of compliance status to be filtered by any custom criteria
Assigned WP	WP6
Relation to other requirements	WP6_CM_004, WP6_CM_006
Actor	Project and Assurance managers
Priority	Must
Type	Functional
Rationale	Standards may consist of hundreds of pages and applicants typically have to show compliance with thousands of requirements contained in them. Additionally, project assurance is usually a collaborative task and information should be at disposal for interested parties. Stakeholder need: To control compliance status.

WP6_CM_006	Compliance Status to Externals
Description	The AMASS tools shall enable the export in a human-readable format (e.g., HTML) of compliance status report in order to allow external users (e.g. Safety Assessors) to get a (read-only) view of the Compliance status, with the possibility to filter by any custom criteria.
Assigned WP	WP6
Relation to other requirements	WP6_CM_003, WP6_CM_005
Actor	Safety (Security, etc.) Assessor; Interested parties in the organization.
Priority	Must
Type	Functional
Rationale	In order for a system to get the approval for operation, a compliance status report should be generated. Due to the complexity of the standards-related practice, having the possibility of filtering by any custom criteria will facilitate the work of the assessor or any other interested user. Stakeholder need: To reduce cost and time in the certification process.

WP6_CM_007	Useful Feedback Upon Violations
Description	The AMASS tools shall enable the assurance managers/safety case officer to

	have more information on the possible causes of violations of requirements not just only the YES/NO type answer. This information (read-only) shall be provided in the compliance status report.
Assigned WP	WP6
Relation to other requirements	N.A.
Actor	Assurance manager, Safety (Security, etc.) Assessor
Priority	Must/Optional
Type	Functional
Rationale	The localization of problematic parts of the processes where the violations have occurred can provide support in taking corrective measures. However, a binary decision on whether the safety process is compliant or not (YES/ NO Type answer) is not sufficient. Whenever there is a violation of the requirements, an explanation of the (possible) causes must be reported to the users. Such reports must be in a format that non-technical people can understand. Essentially, the violation report (with explanation) should be exhaustive i.e., every possible violation of the rule is detected. For example, if some steps in the V&V is not carried out then, reasons should be provided that why such steps were not performed. Providing explanation of a subset of violation would incur another round of compliance verification costing time and efforts of compliance officers'/assurance managers. Besides, violation explanation can provide pointers to quickly rectify potential non-compliance issues.

WP6_CM_008	Process Compliance (informal) management
Description	The AMASS tools shall enable users to visualize process compliance. This means showing the links between the requirements and the applicant's evidence (during the planning as well as execution phase). This visualization could be done via compliance maps (matrix) or via arguments aimed at justifying the satisfaction of the requirements coming from the standards.
Assigned WP	WP6
Relation to other requirements	WP6_CM_007, WP6_CM_009
Actor	Safety Engineer
Priority	Must
Type	Functional
Rationale	To demonstrate compliance, manufacturers/suppliers must show that they have fulfilled the requirements. This can be illustrated via compliance maps (matrix) or argumentation. Stakeholder need: To show compliance of development process with lifecycles depicted in standards.

WP6_CM_009	Process Compliance (formal) management)
Description	The AMASS tools shall enable users to formally check process compliance.
Assigned WP	WP6
Relation to other	WP6_CM_005, WP6_CM_008

requirements	
Actor	Safety Engineer
Priority	could
Type	Functional
Rationale	To demonstrate compliance, manufacturers/suppliers must show that they have fulfilled the requirements. A formal and automatically generated proof might be more reliable. Stakeholder need: To show compliance of development process with lifecycles depicted in standards.

WP6_CM_010	Compliance map generation from argument evidences
Description	The system should be able to detect when a claim about a requirement from a standard (compliance claim) is supported by an evidence and generate the compliance indicator in a transparent way.
Assigned WP	WP6
Relation to other requirements	N.A.
Actor	(Safety) Project Manager
Priority	Should
Type	Functional
Rationale	Generate the compliance indicator from argument evidences. Stakeholder need: Working efficiently and effectively.

3.2.5 Access Manager

Table 6. High Level Requirements for Access Manager

WP5_AM_001	User authentication
Description	The AMASS Tool Platform shall require users to be authenticated for Platform access.
Assigned WP	WP5
Relation to other requirements	WP5_AM_002, WP5_AM_004, WP5_AM_005
Actor	User
Priority	Must
Type	Non-functional
Non-functional category	Security
Rationale	Only authorised users must access the AMASS Tool Platform.

WP5_AM_002	User access
Description	The AMASS Tool Platform shall provide users with different options for data access and for action permission.
Assigned WP	WP5
Relation to other	WP5_AM_001, WP5_AM_004, WP5_AM_005

requirements	
Actor	User
Priority	Should
Type	Non-functional
Non-functional category	Security
Rationale	Need identified in D5.1 (As a tool manager I want to grant access to users according to (a) tool functionality, (b) type of information (e.g., specific project, date range) so that users get access according to their profiles).

WP5_AM_003	User action log
Description	The AMASS Tool Platform shall maintain a log with all the actions performed by the users.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	User, IT manager, Project manager
Priority	Must
Type	Functional
Rationale	Need identified in D5.1 (As a tool auditor I want to know any change on the data managed by the tools including authors, date and content so that I can assess its confidence and traceability).

WP5_AM_004	User profiles
Description	The AMASS Tool Platform shall allow users to have different profiles for Platform access.
Assigned WP	WP5
Relation to other requirements	WP5_AM_001, WP5_AM_002, WP5_AM_005
Actor	User
Priority	Should
Type	Non-functional
Non-functional category	Security
Rationale	A given user should be able to access the AMASS Tool Platform playing different roles.

WP5_AM_005	Access rights groups
Description	The AMASS Tool Platform shall allow users to belong to different access rights groups.
Assigned WP	WP5
Relation to other requirements	WP5_AM_001, WP5_AM_002, WP5_AM_004
Actor	User
Priority	Should

Type	Non-functional
Non-functional category	Security
Rationale	A given user should be able to access the AMASS Tool Platform playing different roles.

3.2.6 Data Manager

Table 7. High Level Requirements for Data Manager

WP5_DM_001	Multi-platform availability
Description	The AMASS Tool Platform shall be accessible from desktop, Web, and cloud environments.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	User
Priority	Should
Type	Non-functional
Non-functional category	Design constraint
Rationale	Need identified in D5.1 (As a tool user working with some functionalities (e.g., compliance management, reports, metrics) I want to get access to information from Web so that I can know this information in real-time as it is being edited by any other user. The Platform should also be available for other platforms).

WP5_DM_002	Simultaneous data access
Description	The AMASS Tool Platform shall allow users to access data simultaneously.
Assigned WP	WP5
Relation to other requirements	WP5_DM_003
Actor	User
Priority	Must
Type	Non-functional
Non-functional category	Design constraint
Rationale	Need identified in D5.1 (As a tool user I want to access the tools data concurrently with other users so that the integrity of the data is guaranteed and that I am aware of the concurrence modifications rules and effects).

WP5_DM_003	Consistent data access
Description	When users are accessing data simultaneously, the AMASS Tool Platform shall manage the possible conflicts.
Assigned WP	WP5
Relation to other requirements	WP5_DM_002
Actor	User

Priority	Should
Type	Functional
Rationale	Simultaneous data access can lead to data conflicts, which should be managed.

WP5_DM_004	Real-time data access feedback
Description	The AMASS Tool Platform shall provide users with feedback about how data is being accessed by other users on real time.
Assigned WP	WP5
Relation to other requirements	WP5_DM_002
Actor	User
Priority	Could
Type	Functional
Rationale	The users might need to be aware of how other users are accessing the same data

WP5_DM_005	System artefact information storage
Description	The AMASS Tool Platform shall be able to store information about any type of system artefact.
Assigned WP	WP5
Relation to other requirements	WP5_EM_001
Actor	System engineer, Assurance engineer
Priority	Must
Type	Functional
Rationale	CPS development, assurance and certification require the management of a wide range of system artefact types, and information about artefact of all these types might have to be stored in the AMASS Tool Platform.

WP5_DM_006	Standard formats storage
Description	The AMASS Tool Platform shall be able to store system artefacts represented in standard formats (OSLC RM, ReqIF, UML, SysML, FMI, FMU…).
Assigned WP	WP5
Relation to other requirements	WP5_EM_001
Actor	System engineer, Assurance engineer
Priority	Must
Type	Non-functional
Non-functional category	Standard Compliance
Rationale	CPS development, assurance and certification can require the management of a wide range of system artefact types in standard formats, and information about artefact of all these types in the standard formats might have to be stored in the AMASS Tool Platform.

WP5_DM_007	Data versioning
Description	The AMASS Tool Platform shall support data versioning.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	User
Priority	Must
Type	Functional
Rationale	Data in the AMASS Tool Platform can change over time, and such changes must be tracked.

WP5_DM_008	Secure data access
Description	The AMASS Tool Platform shall provide a secure standard API for data access.
Assigned WP	WP5
Relation to other requirements	WP5_AM_001
Actor	User
Priority	Should
Type	Non-functional
Non-functional category	Security
Rationale	When accessing data in the AMASS Platform from another tool via an API, such access must be secure.

3.3 High Level Requirements related to Architecture-Driven Assurance (STO1)

3.3.1 System Architecture Modelling for Assurance

Table 8. High Level Requirements for System Architecture Modelling

WP3_SAM_001	Trace component with assurance assets
Description	The supplier of a component must be able to trace all the assurance information with the specific component.
Assigned WP	WP3
Relation to other requirements	WP3_SC_001
Actor	Assurance Engineer
Priority	Must
Type	Functional
Rationale	Traceability between system architecture entities and assurance-related information is mandatory to enable architecture-driven assurance.

WP3_SAM_002	Impact assessment if the component changes
Description	The system shall provide the capability for a component change impact analysis.
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Development Engineer, Assurance Engineer, Project Manager, Assurance Manager
Priority	Shall
Type	Functional
Rationale	Impact analysis allows to estimate development and (re) certification costs.

WP3_SAM_003	Compare different architectures according to different concerns which have been specified before
Description	The system must be able to compare different system architectures based on predefined criteria, focusing on system requirements/properties.
Assigned WP	WP3
Relation to other requirements	WP3_SC_001
Actor	Development Engineer, Assurance Engineer, Project Manager, Assurance Manager
Priority	Must
Type	Functional
Rationale	Comparison of different system architectures increase the opportunities of cost reductions.

WP3_SAM_004	Integration with external modelling tools
Description	The system could interact with external tools for system design and development (e.g., Rhapsody, AutoFocus, Compass) to get the system architecture.
Assigned WP	WP3
Relation to other requirements	WP3_SC_003
Actor	Development Engineer, Assurance Engineering
Priority	Could
Type	Functional
Rationale	Requirement needed to improve the interoperability between similar tools for system design and development.

3.3.2 Assurance Patterns Library Management

Table 9. High Level Requirements for Assurance Patterns Library Management

WP3_APL_001	Drag and drop an architectural pattern
Description	The system should be able to instantiate in the component model and architectural pattern selected from the list of patterns stored.
Assigned WP	WP3
Relation to other requirements	WP3_SC_002
Actor	Development Engineer, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Architectural pattern allow adoption of common proved solutions and reuse of components and argumentation fragments.

WP3_APL_002	Edit an architectural pattern
Description	The system should be able to edit, store and retrieve architectural patterns.
Assigned WP	WP3
Relation to other requirements	WP3_SC_002
Actor	Development Engineer, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Architectural patterns allow adoption of common proved solutions and reuse of components and argumentation fragments.

WP3_APL_003	Use of architectural patterns at different levels
Description	The system should be able to apply to the component model architectural patterns at different levels: reference architectures , Safety/Security Mechanisms (security controls).
Assigned WP	WP3

Relation to other requirements	WP3_SC_002
Actor	Development Engineer, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Architectural patterns allow adoption of common proved solutions and reuse of components and argumentation fragments.

WP3_APL_004	**Architectural Patterns suggestions**
Description	The system could provide the user suggestions about a certain safety/security mechanism stored as architectural patterns.
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Assurance Engineer, System Architect
Priority	Could
Type	Functional
Rationale	Support for design evaluation and trade-off based on certain properties.

WP3_APL_005	**Generation of argumentation fragments from architectural patterns/decisions**
Description	The system should be able to generate arguments fragments based on the usage of specific architectural patterns in the component model.
Assigned WP	WP3
Relation to other requirements	WP3_APL_002, WP3_APL_003
Actor	Product Engineer, Assurance Manager
Priority	Should
Type	Functional
Rationale	Architectural patterns allow adoption of common proved solutions and reuse of components and argumentation fragments.

3.3.3 Contract Based Assurance Composition

Table 10. High Level Requirements for Contract Based Assurance Composition

WP3_CAC_001	**Validate composition of components by validating their assurance contract**
Description	The system shall be able to validate the composition of two or more components by validating the compatibility of the component contracts.
Assigned WP	WP3
Relation to other requirements	WP3_CAC_002
Actor	Development Engineer, Assurance Engineer
Priority	Shall
Type	Functional

Rationale	Validation of contracts compatibility supports component compositions.

WP3_CAC_002	Assign contract to component
Description	The system shall allow to associate a contract to a component. Then, the system shall allow to drop a contract from a component.
Assigned WP	WP3
Relation to other requirements	WP3_SC_001
Actor	Development Engineer, Assurance Engineer
Priority	Shall
Type	Functional
Rationale	This is a mandatory requirement to enable contract-based design.

WP3_CAC_003	Structure properties into contracts (assumptions/guarantees)
Description	The system must be able to support the specification of assumptions and guarantees to be used in component contracts based on component properties.
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Development Engineer, Assurance Engineer
Priority	Must
Type	Functional
Rationale	Semi-Automatic support for contract specification can be used as evidence for component qualification.

WP3_CAC_004	Specify contract refinement
Description	The system shall enable users to specify the refinement of contracts along the hierarchical components architecture.
Assigned WP	WP3
Relation to other requirements	WP3_SC_001, WP3_CAC_002
Actor	Development Engineering, Assurance Engineering
Priority	Shall
Type	Functional
Rationale	Contracts refinement specification is an important part of contract-based design; it allows formal verification of contracts refinement.

WP3_CAC_005	General management of contract component assignments
Description	The system should enable users to have a view of the association between contracts and components for the entire system architecture (thus, not only a view on the single contract assignment for each component).

Assigned WP	WP3
Relation to other requirements	WP3_CAC_002
Actor	Development Engineering, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Requirement needed to increase usability and to speed up the system design process, related to the contract assignment.

WP3_CAC_006	Refinement-based overview
Description	The system should enable users to have a hierarchical view of the contract refinements along the system architecture.
Assigned WP	WP3
Relation to other requirements	WP3_CAC_004
Actor	Development Engineering, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Requirement needed to increase usability and to speed up the system design process, related to the contract refinement.

WP3_CAC_007	Overview of check refinements results
Description	The system should enable users to have an overview in terms of status of check refinement of all the defined contracts.
Assigned WP	WP3
Relation to other requirements	WP3_CAC_004, WP3_CAC_006, WP3_CAC_008
Actor	Development Engineering, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Requirement needed to speed up the system design process, related to the contract refinement.

WP3_CAC_008	Contract-based validation and verification
Description	The system must provide support for contract-based system validation and verification, including refinement checking, compositional verification of behavioural models, contract-based fault-tree generation.
Assigned WP	WP3
Relation to other requirements	WP3_CAC_004, WP3_CAC_006
Actor	Development Engineering, Assurance Engineering
Priority	Must
Type	Functional
Rationale	Requirement needed to reduce costs related to validation activities.

WP3_CAC_009	Improvement of Contract definition process
Description	The operation of contract definition should be improved in terms of time spent.
Assigned WP	WP3
Relation to other requirements	WP3_CAC_003
Actor	Development Engineering, Assurance Engineering
Priority	Should
Type	Non-Functional
Rationale	Requirement needed to speed up the system design process, related to the contract assignment.

WP4_CAC_010	Contract-based trade-off analysis
Description	The system could provide the capability to evaluate safety and security requirements on different system architectures to perform trade-off analysis based on the contract specification.
Assigned WP	WP4
Relation to other requirements	WP3_CAC_008
Actor	Safety Engineer together with Security Engineer
Priority	Could
Type	Functional
Rationale	The results of the trade-off analysis can be used as evidence in a contract-based multi-concerns assurance case.

WP3_CAC_011	Overview of contract-based validation for behavioural models
Description	The system could enable the user to have an overview of the contract-based validation and verification results and to inspect the related system execution traces (if any).
Assigned WP	WP3
Relation to other requirements	WP3_CAC_008
Actor	Development Engineering, Assurance Engineering
Priority	Could
Type	Functional
Rationale	Requirement needed to speed up the system design process, related to behavioural models.

WP3_CAC_012	Browse Contract status
Description	The user shall be able to browse the contracts associated within a component and their status (fulfilled or not).
Assigned WP	WP3

Relation to other requirements	WP3_CAC_008
Actor	Development Engineering, Assurance Engineering
Priority	Should
Type	Functional
Rationale	Requirement needed to increase usability and speed up the system design process, related to the contract assignment.

WP3_CAC_013	Specify contracts defining the assumption and the guarantee elements
Description	The system must provide the capability to create a contract defining two new properties (assumptions/guarantees) implicitly associated to that contract.
Assigned WP	WP3
Relation to other requirements	WP3_CAC_008
Actor	Development Engineering, Assurance Engineering
Priority	Must
Type	Functional
Rationale	Requirement needed to increase usability and speed up the system design process, related to the contract assignment.

3.3.4 V&V Based Assurance

Table 11. High Level Requirements for V&V Based Assurance

WP3_VVA_001	Traceability between different kinds of V&V evidence
Description	The system shall provide the ability to trace immediate evidence (obtained during the execution of the left-hand side of the V-model) with direct evidence (obtained during the execution of the right-hand side of the V-model). For instance: a contract-based, component-based specification should be traced with the corresponding analysis-results.
Assigned WP	WP3
Relation to other requirements	WP3_SC_003
Actor	Assurance Engineer
Priority	Should
Type	Functional
Rationale	Traceability between system architecture entities and evidence information is needed to support the assurance case.

WP3_VVA_002	Trace model-to-model transformation
Description	The system shall be able to trace all component model transformations executed during V&V model-based analysis.
Assigned WP	WP3
Relation to other requirements	N.A.

Actor	Development Engineer, Assurance Manager
Priority	Must
Type	Functional
Rationale	Traceability about model-transformation for V&V can be referred in the assurance-case as evidence.

WP3_VVA_003	Validate requirements checking consistency, redundancy, … on formal properties
Description	The system shall be able to validate formal requirements/properties.
Assigned WP	WP3
Relation to other requirements	WP3_SC_004
Actor	Product Engineer, Assurance Manager
Priority	Must
Type	Functional
Rationale	Support for requirements validation can be provided as part of the assurance case.

WP3_VVA_004	Trace requirements validation checks
Description	The system shall be able to trace requirements validations.
Assigned WP	WP3
Relation to other requirements	WP3_SC_004
Actor	Product Engineer, Assurance Manager
Priority	Must
Type	Functional
Rationale	Support for requirements validation can be used as evidence in the assurance case.

WP3_VVA_005	Verify (model checking) state machines
Description	The system shall be able to verify that the component behavioural model matches with the specification.
Assigned WP	WP3
Relation to other requirements	WP3_SC_006
Actor	Product Engineer, Assurance Manager
Priority	Must
Type	Functional
Rationale	Support for requirements validation can be used as evidence in the assurance case.

WP3_VVA_006	Automatic provision of HARA/TARA-artifacts
Description	The system shall provide the capability for automating HARA (Hazard Analysis

	Risk Assessment)/TARA (Threat Assessment & Remediation Analysis)-related artefacts (e.g., FTA, FMEA, attack trees).
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Assurance Engineer
Priority	Must
Type	Functional
Rationale	Support for V&V activities can be used as evidence in the assurance case.

WP3_VVA_007	**Generation of reports about system description/verification results**
Description	The system shall generate reports about system/subsystem/component verification results.
Assigned WP	WP3
Relation to other requirements	N.A.
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Reports can be used as evidence in the assurance case.

WP3_VVA_008	**Automatic test cases specification from assurance requirements specification**
Description	The system should be able to generate automatically the test cases specification based on the requirements definition.
Assigned WP	WP3
Relation to other requirements	WP3_SC_004
Actor	Development Engineer, Assurance Engineer
Priority	Shall
Type	Functional
Rationale	To reduce costs related to verification activities and to provide support for argumentation in the assurance case.

WP3_VVA_009	**Capability to connect to tools for test case generation based on assurance requirements specification of a component/system**
Description	The system shall be able to connect to external tools to execute the test cases already specified.
Assigned WP	WP3
Relation to other requirements	WP3_VVA_008
Actor	Product Engineer, Assurance Manager
Priority	Shall
Type	Functional

Rationale	Support for V&V activities can be used as evidence in the assurance case.

WP3_VVA_010	Model-based safety analysis
Description	The system shall allow the user to generate fault trees and FMEA tables from the behavioural model and the fault injection.
Assigned WP	WP3
Relation to other requirements	WP3_SC_006, WP3_SC_007
Actor	Assurance Engineer
Priority	Must
Type	Functional
Rationale	Support for V&V activities can be used as evidence in the assurance case.

WP3_VVA_011	Simulation-based Fault Injection
Description	The system should allow the user to generate fault injection simulations from the fault trees and FMEA tables.
Assigned WP	WP3
Relation to other requirements	WP3_SC_006, WP3_SC_007
Actor	Assurance Engineer
Priority	Should
Type	Functional
Rationale	Support for V&V activities can be used as evidence in the assurance case. Support for the dependability evaluation of the system. Trade-off of safety concepts.

WP3_VVA_012	Design Space Exploration
Description	The system could support the design space exploration of a system for a certain safety/security criticality level.
Assigned WP	WP3, WP4
Relation to other requirements	N.A.
Actor	Assurance Engineer, System Architect
Priority	Could
Type	Functional
Rationale	Support for design evaluation and trade-off based on certain properties. These constraints may be contradictory and correspond to different dimensions (cost, safety, timing, etc.). Furthermore, the task of considering all system constraints during system design manually is quite exhaustive.

3.4 High Level Requirements related to Multi-Concern Assurance (STO2)

3.4.1 Dependability Assurance Modelling

Table 12. High Level Requirements for Dependability Assurance Modelling

WP4_DAM_001	Capability to model relationships between concerns
Description	The system shall be able to provide an assurance case which records the relationships between dependability attributes and how they are affected because of design decisions.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Record relationships between concerns. Stakeholder need: Working efficiently and effectively.

WP4_DAM_002	Capability to capture conflicts occurring during system development and the trade-off process
Description	The system shall provide the capability for modelling a dependability case which captures the conflicts that occur during system development and the trade-off process to justify why the taken design decisions are the most optimal ones.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Capture conflicts occurring during system development and the trade-off process. Stakeholder need: Working efficiently and effectively.

3.4.2 Contract-Based Multi-concern Assurance

Table 13. High Level Requirements for Contract Based Multi-concern

WP4_CMA_001	The AMASS tools must support specification of variability at the argumentation level
Description	The system shall provide the capability for modelling arguments in the assurance case about multi-concern and multi-context. The multi-concern and multi-context argumentation could follow a variability modelling a solution. If GSN-like modelling elements are considered, the diamond for representing alternatives as well as the octagon for extrinsic

	variability could be considered.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Provide the capability for modelling a multi-concern and multi-context assurance case. Stakeholder need: Working efficiently and effectively.

WP4_CMA_002	Component contracts must support multiple concerns
Description	The system shall provide a contract specification language that supports the formalization of both safety and security requirements.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	The specification of multiple-concerns contracts enable the contract-based trade-off analysis.

WP4_CMA_003	Contract based multi-concern assurance
Description	The system must support features that support contract based assurance with respect to multiple concerns; i.e. it must be possible to specify relations between safety contracts, security contracts and other-concerns-related contracts in order to take care of the influence of system modifications for mitigating the risks associated with one quality attribute on the contract belonging to another quality attribute.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Support features that support contract based assurance with respect to multiple concerns.

3.4.3 System Dependability Co-Analysis/Assessment

Table 14. High Level Requirements for System Dependability Co-Analysis/Assessment

WP4_SDCA_001	System dependability co-architecturing and co-design

Description	The system shall provide features, which allow architecture modelling collaboration and co-designing a system or component with a balanced combination of different goals addressing various quality attributes.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Provide features, which allow architecture modelling collaboration and co-designing.

WP4_SDCA_002	System dependability co-verification and co-validation
Description	The system shall support efficient system or component co-verification and co-validation with respect to multiple quality attributes.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Support efficient system or component co-verification and co-validation.

WP4_SDCA_003	The system shall allow combinations of safety and security analysis
Description	The system shall allow combinations of safety and security analysis.
Assigned WP	WP4
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Must
Type	Functional
Rationale	Allow combinations of safety and security analysis.

3.5 High Level Requirements related to Seamless Interoperability (STO3)

3.5.1 Tool Integration Management

Table 15. High Level Requirements for Tool Integration Management

WP5_TI_001	Automatic data collection
Description	The AMASS Tool Platform shall automatically collect data from external tools.
Assigned WP	WP5

Relation to other requirements	WP5_EM_006
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Need identified in D5.1 (As a tool auditor I want automatic collection of lifecycle and status data in a transparent way as part of workflow; As a tool user I want data to move through process with minimal manual intervention).

WP5_TI_002	Automatic data export
Description	The AMASS Tool Platform shall be able to automatically export data to external tools.
Assigned WP	WP5
Relation to other requirements	WP5_EM_007
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Need identified in D5.1 (As a tool auditor I want automatic exchange of lifecycle and status data in a transparent way as part of workflow; As a tool user I want data to move through process with minimal manual intervention).

WP5_TI_003	Tool chain deployment support
Description	The AMASS Tool Platform shall support the specification, configuration, and deployment of tool chains for CPS assurance and certification on a single environment.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Need reflected in the case studies. All of them refer to the use of several engineering tools whose interaction and data could be integrated.

WP5_TI_004	System analysis tools interoperability
Description	The AMASS Tool Platform shall be able to interoperate with system analysis tools.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in several case studies (e.g. CS1 and CS3).

WP5_TI_005	System specification tools interoperability
Description	The AMASS Tool Platform shall be able to interoperate with system specification tools.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in several case studies (e.g. CS4 and CS7).

WP5_TI_006	V&V tools interoperability
Description	The AMASS Tool Platform shall be able to interoperate with V&V tools.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in in several case studies (e.g. CS4 and CS7).

WP5_TI_007	Version management tools interoperability
Description	The AMASS Tool Platform shall be able to interoperate with version management tools.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies (e.g. CS10).

WP5_TI_008	Quality management tools interoperability
Description	The AMASS Tool Platform shall be able to interoperate with quality management tools.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies (e.g. CS10).

WP5_TI_009	MS Office applications interoperability
Description	The AMASS Tool Platform shall be able to interoperate with MS Office applications (Word, Excel, Visio, etc.).
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Could
Type	Functional
Rationale	Need reflected in the case studies (e.g. CS3).

WP5_TI_010	Interoperability throughout CPS lifecycle
Description	The AMASS Tool Platform shall be able to interoperate with some tool in all CPS lifecycle phases.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies. Some tool to interoperate with has been indicated for practically all the CPS lifecycle phases.

WP5_TI_011	Non-proprietary data exchange
Description	The AMASS Tool Platform shall provide exchange data in non-proprietary formats.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Need identified in D5.1 [3] (As a tool manager I want data to be readily available in non-proprietary formats).

WP5_TI_012	Data entry effort
Description	The AMASS Tool Platform shall allow users to create and enter data only once.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	User
Priority	Should
Type	Non-functional
Non-functional	Usability

category	
Rationale	Need identified in D5.1 [3] (As a tool user I want to create and enter data only once).

WP5_TI_013	Continuous data management
Description	The AMASS Tool Platform shall support continuous data analysis, verification, and integration.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003
Actor	Assurance engineer, Assurance manager
Priority	Should
Type	Non-functional
Non-functional category	Performance
Rationale	Need identified in D5.1 [3] (As a tool manager I want continuous analysis, verification and integration of the data).

WP5_TI_014	Client-server support
Description	The AMASS Tool Platform shall support data and tool integration in client-server architectures.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Client-server architecture are common for tool interoperability and usually suitable.

WP5_TI_015	Service offer and discovery
Description	The AMASS Tool Platform shall allow clients to ask for a server's services and to discover servers.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003
Actor	Assurance engineer
Priority	Should
Type	Functional
Rationale	Clients in a client-server architecture for tool integration should be able to find and exploit servers' services as much as possible.

WP5_TI_016	Performance monitoring
Description	The AMASS Tool Platform shall allow continuous performance monitoring of

	the servers.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003, WP5_TI_014, WP5_TI_015
Actor	Assurance engineer
Priority	Could
Type	Functional
Rationale	Possible performance issues in a client-server architecture for tool integration must be detected.

WP5_TI_017	Standards-based interoperability
Description	The AMASS Tool Platform shall support standard mechanisms for tool interoperability.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Must
Type	Non-functional, Standard Compliance
Rationale	Need identified in D5.1 (As a tool manager I want to minimize the number of data management and lifecycle tools).

WP5_TI_018	Extended standard-based interoperability
Description	The AMASS Tool Platform shall provide extended means to standard mechanisms for tool interoperability.
Assigned WP	WP5
Relation to other requirements	WP5_TI_001, WP5_TI_002, WP5_TI_003
Actor	Assurance engineer
Priority	Must
Type	Functional
Rationale	Sometimes standard means for tool integration are not powerful enough or have limitations in some scenarios.

3.5.2 Collaborative Work Management

Table 16. High Level Requirements for Collaborative Work Management

WP5_CW_001	Collaborative system analysis
Description	The AMASS Tool Platform shall support the collaboration among systems engineers, safety engineers, and security engineers for system analysis.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003
Actor	Systems engineer, Safety engineer, and Security engineer
Priority	Should

Type	Functional
Rationale	Need reflected in the case studies CS1, CS2. CS3, CS4, CS5, CS7, CS8, CS9, CS10, CS11.

WP5_CW_002	Collaborative system specification
Description	The AMASS Tool Platform shall support the collaboration among systems engineers, safety engineers, and security engineers for system modelling.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003
Actor	Systems engineer, Safety engineer, and Security engineer
Priority	Must
Type	Functional
Rationale	Need reflected in the case studies CS1, CS4, CS5, CS7, CS9, CS11.

WP5_CW_003	Collaborative management of compliance with standards and of process assurance
Description	The AMASS Tool Platform shall support the collaboration among systems engineers, assurance managers for management of compliance with standards and of process assurance.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	Systems engineer and Assurance manager
Priority	Must
Type	Functional
Rationale	Need reflected in the case study CS1.

WP5_CW_004	Collaborative re-certification needs & consequences analysis
Description	The AMASS Tool Platform shall support the collaboration among assurance managers and assurance engineers for re-certification needs & consequences analysis.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	Assurance manager and Assurance engineer
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies CS2. CS3, CS4.

WP5_CW_005	Collaborative system V&V
Description	The AMASS Tool Platform shall support the collaboration among systems engineers for system V&V.
Assigned WP	WP5

Relation to other requirements	WP5_TI_003
Actor	Systems engineer
Priority	Could
Type	Functional
Rationale	Need reflected in the case study CS3.

WP5_CW_006	Collaborative model-based systems engineering
Description	The AMASS Tool Platform shall support the collaboration among systems engineers, safety engineers, and security engineers for model-based systems engineering.
Assigned WP	WP5
Relation to other requirements	WP5_TI_003
Actor	Systems engineer, Safety engineer, and Security engineer
Priority	Must
Type	Functional
Rationale	Need reflected in the case studies CS3, CS4, CS5, CS7, CS9, CS10, CS11.

WP5_CW_007	Collaborative assurance evidence management
Description	The AMASS Tool Platform shall support the collaboration among assurance managers and systems engineers for assurance evidence management.
Assigned WP	WP5
Relation to other requirements	WP5_EM_001-016
Actor	Systems engineer and Assurance manager
Priority	Must
Type	Functional
Rationale	Need reflected in the case study CS3.

WP5_CW_008	Collaborative product reuse needs & consequences analysis
Description	The AMASS Tool Platform shall support the collaboration among systems engineers and assurance managers for product reuse needs & consequences analysis.
Assigned WP	WP5
Relation to other requirements	WP6_RA_001-006
Actor	Systems engineer and Assurance manager
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies CS1, CS4, CS7.

WP5_CW_009	Collaborative assurance case specification
Description	The AMASS Tool Platform shall support the collaboration among assurance

	managers and assurance engineers for assurance case specification.
Assigned WP	WP5
Relation to other requirements	WP4_ACS_001-013
Actor	Assurance manager and Assurance engineer
Priority	Must
Type	Functional
Rationale	It should be possible to collaboratively execute all the process supported by the basic building blocks of the AMASS Tool Platform.

WP5_CW_010	Collaborative compliance needs specification
Description	The AMASS Tool Platform shall support the collaboration among assurance managers for compliance needs specification.
Assigned WP	WP5
Relation to other requirements	WP6_CM_002
Actor	Assurance manager
Priority	Could
Type	Functional
Rationale	It should be possible to collaboratively execute all the process supported by the basic building blocks of the AMASS Tool Platform.

WP5_CW_011	Collaborative assurance assessment
Description	The AMASS Tool Platform shall support the collaboration among assurance managers, assurance engineers, and assurance assessors for assurance assessment.
Assigned WP	WP5
Relation to other requirements	N.A.
Actor	Assurance managers, Assurance engineers, and Assurance assessors
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies (e.g. CS1).

WP5_CW_012	Collaborative compliance assessment
Description	The AMASS Tool Platform shall support the collaboration among assurance managers, assurance engineers, and assurance assessors for compliance assessment.
Assigned WP	WP5
Relation to other requirements	WP6_CM_003, WP6_CM_004
Actor	Assurance managers, Assurance engineers, and Assurance assessors
Priority	Should
Type	Functional
Rationale	Need reflected in the case studies (e.g. CS1).

WP5_CW_013	Metrics & measurements reports
Description	The AMASS Tool Platform shall manage metrics and measurements about collaborative work.
Assigned WP	WP5
Relation to other requirements	WP5_CW_001-012
Actor	Assurance manager
Priority	Functional
Type	Should
Rationale	Need identified in D5.1 (As a tool user I want to have metrics and measurements generated and reported).

3.5.3 Tool Quality Assessment and Characterization

Table 17. Tool Quality Assessment and Characterization High Level Requirements

WP5_TQ_001	Tool qualification information needs
Description	The AMASS Tool Platform shall allow an assurance manager to specify the needs regarding qualification for the engineering tools used in a CPS' lifecycle.
Assigned WP	WP5
Relation to other requirements	WP6_CM_002
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	Tool qualification aspects might have to be taken into account in an assurance project.

WP5_TQ_002	Tool quality evidence management
Description	The AMASS Tool Platform shall manage evidence of tool quality.
Assigned WP	WP5
Relation to other requirements	WP5_TQ_001, WP5_EM_001
Actor	Assurance manager
Priority	Must
Type	Functional
Rationale	Evidence of tool quality can be necessary for CPS assurance and certification.

WP5_TQ_003	Tool quality information import
Description	The AMASS Tool Platform shall be to import tool quality information such as tool qualification dossiers.
Assigned WP	WP5
Relation to other requirements	WP5_TQ_001, WP5_EM_004

Actor	Assurance engineer
Priority	Could
Type	Functional
Rationale	Tool qualification information can be available in or through some external tool, including to qualified tool.

WP5_TQ_004	Tool quality needs indication
Description	The AMASS Tool Platform should indicate the tool quality needs that need to be fulfilled in a given assurance project.
Assigned WP	WP5
Relation to other requirements	WP5_TQ_001
Actor	Assurance manager
Priority	Should
Type	Functional
Rationale	An assurance manager should be aware of the tool quality needs to meet in an assurance project.

WP5_TQ_005	Tool quality requirements fulfilment
Description	The AMASS Tool Platform should indicate the degree to which tool quality requirements for the engineering tools used in a CPS' lifecycle have been fulfilled.
Assigned WP	WP5
Relation to other requirements	WP5_TQ_001
Actor	Assurance manager
Priority	Should
Type	Functional
Rationale	An assurance manager should be aware of how the fulfilment of tool quality requirements progresses during an assurance project.

3.6 High Level Requirements related to Cross/Intra-Domain Reuse (STO4)

3.6.1 Reuse Assistant (Cross/Intra-Domain)

Table 18. High Level Requirements for Reuse Assistant (Cross/Intra-Domain)

WP6_RA_001	Intra-Domain, Intra standard, Reuse Assistance
Description	The AMASS tools shall enable partial reuse of compliance artefacts when transiting from one project to another (different criticality level, etc.). The commonality that characterizes the different projects should be recognized and proposed as reusable process structure.
Assigned WP	WP6
Relation to other requirements	WP6_RA_002, WP6_RA_003
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Projects within the same domain might exhibit common requirements, which might be fulfilled by similar process structures. Stakeholder need: Facilitate the reuse of process elements/structures.

WP6_RA_002	Intra-Domain, Cross standards, Reuse Assistance
Description	The AMASS tools shall enable partial reuse of compliance artefacts when transiting from one project to another (different/same criticality level, if applicable, but different standards (e.g., AutomotiveSPICE, ISO 26262).) The commonality that characterizes the different projects should be recognized and proposed as a reusable process structure.
Assigned WP	WP6
Relation to other requirements	WP6_RA_001, WP6_RA_003
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Even if standards are different, projects within the same domain might exhibit common requirements, which might be fulfilled by similar process structures. Stakeholder need: Facilitate the reuse of process elements/structures.

WP6_RA_003	Intra-Domain, Cross versions, Reuse Assistance
Description	The AMASS tools shall enable partial reuse of compliance artefacts when transiting from one project to another (different/same criticality level, if applicable, but different standards (e.g., ISO 26262-2011, ISO 26262-2018).) The commonality that characterizes the different projects should be recognized and proposed as reusable process structure.

Assigned WP	WP6
Relation to other requirements	WP6_RA_001, WP6_RA_002
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Projects within the same domain, same standard but different versions, certainly exhibit common requirements, which might be fulfilled by similar process structures. Stakeholder need: Facilitate the reuse of process elements/structures.

WP6_RA_004	**Cross-Domain Reuse Assistance**
Description	The AMASS tools shall enable partial reuse of compliance artefacts when transiting from one project to another belonging to different domains (e.g., from automotive to avionics). The commonality that characterizes the different projects should be recognized and proposed as reusable process structure.
Assigned WP	WP6
Relation to other requirements	WP6_RA_001, WP6_RA_002, WP6_RA_003
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Projects within different domains might exhibit common requirements, which might be fulfilled by similar process structures. Stakeholder need: Facilitate the reuse of process elements/structures.

WP6_RA_005	**Intra-Domain, Intra standard, Different Stakeholders, Reuse/Integration Assistance**
Description	The AMASS tools shall enable partial reuse of compliance artefacts during the integration (manufacturer/supplier). Assumed process requirements vs. actual process requirements.
Assigned WP	WP6
Relation to other requirements	WP6_RA_002, WP6_RA_003
Actor	Assurance Manager
Priority	Could
Type	Functional
Rationale	Projects within the same domain might exhibit common requirements, which might be fulfilled by similar process structures. Stakeholder need: Facilitate the reuse of process elements/structures.

WP6_RA_006	**Reusable off the shelf components**
Description	The AMASS tool shall provide the capability for reuse of pre-developed

	components and their accompanying artefacts.
Assigned WP	WP3
Relation to other requirements	WP3_SC_002
Actor	Development Engineer, Assurance Engineer, Project Manager, Assurance Manager
Priority	Must
Type	Functional
Rationale	Reuse allows assurance effort reduction.

WP6_RA_007	Provision of metrics about process-related reuse (e.g., size of commonality)
Description	The system could produce a status report indicating a quantitative reuse metric regarding process modelling.
Assigned WP	WP6
Relation to other requirements	WP6_RA_008, WP6_RA_009, WP5_CW_013
Actor	Project manager
Priority	Could
Type	Functional
Rationale	Providing quantitative reuse metrics for process-related reuse. Stakeholder need: Working efficiently and effectively.

WP6_RA_008	Provision of metrics about product-related reuse (e.g., size of commonality)
Description	The system could produce a status report indicating a quantitative reuse metric regarding system modelling.
Assigned WP	WP6
Relation to other requirements	WP6_RA_009, WP6_RA_007, WP5_CW_013
Actor	Project manager
Priority	Could
Type	Functional
Rationale	Providing quantitative reuse metrics for product-related reuse. Stakeholder need: Working efficiently and effectively.

WP6_RA_009	Provision of metrics about assurance case-related reuse (e.g., size of commonality)
Description	The system could produce a status report indicating a quantitative reuse metric regarding assurance case modelling.
Assigned WP	WP6
Relation to other requirements	WP6_RA_007, WP6_RA_008, WP5_CW_013
Actor	Project manager
Priority	Could
Type	Functional

Rationale	Providing quantitative reuse metrics for assurance case-related reuse. Stakeholder need: Working efficiently and effectively.

3.6.2 Semantic Standards Equivalence Mapping

Table 19. High Level Requirements for Semantic Standards Equivalence Mapping

WP6_SEM_001	Semantics-based mapping of standards
Description	The AMASS tools shall enable the mapping of standards based on their semantics.
Assigned WP	WP6
Relation to other requirements	N.A.
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Certain terminological differences contained within standards are irrelevant. The identification of relevant/irrelevant differences may enable the identification of reusable elements/structures. Stakeholder need: Facilitate reuse based on the semantics.

3.6.3 Product/Process/Assurance Case Line Specification

Table 20. High Level Requirements for Product/Process/Assurance Case Line Specification

WP6_PPA_001	The AMASS tools must support variability management at process level
Description	The AMASS tools shall enable the specification/systematization of variability at the process level.
Assigned WP	WP6
Relation to other requirements	WP6_PPA_004, WP6_PPA_005
Actor	Assurance Manager
Priority	Must
Type	Functional
Rationale	Standards are composed of hundreds of pages and usually contain thousands of requirements, which overlap. To be compliant with the standards, manufacturers/suppliers have to fulfil the requirements. Process-related intra-domain as well as cross-domain reuse can be systematized if commonalities and variabilities are systematized. Stakeholder need: Facilitate the management of variable process elements/structure.

WP6_PPA_002	Semi-automatic generation of product arguments
Description	The system should reduce efforts of manual creation of product-based assurance case arguments. This could be done by enabling semi-automatic

	generation of product-based arguments-fragments.
Assigned WP	WP6
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Should
Type	Functional
Rationale	Reducing efforts of manual creation of product arguments. Stakeholder need: Working efficiently and effectively.

WP6_PPA_003	Semi-automatic generation of process arguments
Description	The system should be able to semi-automatic generate fragments of an assurance case for process arguments based on the process followed to develop a component/system.
Assigned WP	WP6
Relation to other requirements	N.A.
Actor	Safety Engineer together with Security Engineer
Priority	Should
Type	Functional
Rationale	Reducing efforts of manual creation of process arguments. Stakeholder need: Working efficiently and effectively.

WP6_PPA_004	The AMASS tools must support management of variability at the component level
Description	The system shall enable users to specify what varies (and what remains unchanged) from one component and its evolved version at component level.
Assigned WP	WP6
Relation to other requirements	WP3_SC_002, WP6_PPA_001, WP6_PPA_005
Actor	Development Engineer, Assurance Engineer
Priority	Shall
Type	Functional
Rationale	Information about variability can be used for impact analysis. Moreover, product-related intra-domain as well as cross-domain reuse can be systematized if commonalities and variabilities are systematized.

WP6_PPA_005	The AMASS tools must support variability management at the assurance case level
Description	The system shall enable users to specify what varies (and what remains unchanged) from one component and its evolved version at component level.
Assigned WP	WP6
Relation to other requirements	WP6_PPA_001, WP6_PPA_004

Actor	Development Engineer, Assurance Engineer
Priority	Shall
Type	Functional
Rationale	Information about variability can be used for impact analysis. Moreover, Assurance case-related intra-domain as well as cross-domain reuse can be systematized if commonalities and variabilities are systematized.

4. Conclusions

This deliverable has presented the business cases and the high-level requirements of the AMASS project. Business Cases give us a first vision of the different scenarios where AMASS solutions could be deployed providing added value to users. On the other hand, high-level requirements collect the stakeholders' needs and define the framework for AMASS development.

Previously to the definition of the Business Cases per domain, the deliverable addresses the most extended methodology named "Business Model Canvas". As first analysis, the Canvas allows us to obtain a holistic view of the AMASS business as a whole, identifying customers, channels, value proposition, key resources, key activities, key partners, cost, and other relevant information. The Canvas offers us an overall vision about how AMASS could provide added value to the stakeholders. Based on an open source model, AMASS improves the efficiency, interoperability and scalability; reducing effort and cost in the safety and security assessment. After the Canvas, several business cases have been defined per domain (Automation, Automotive, Railway, Avionics, Space, Air Traffic). These Business Cases provide a general description of each domain and the stakeholders involved (manufacturers, providers, consultants and assessors, regulators, etc.), defining the interaction between them and identifying how AMASS could provide added value. As a result, several business processes and the value proposition of AMASS in each domain are described, which are future scenarios where the AMASS solution could be deployed.

With respect to the high-level requirements elicitation, several sources have been considered; the case studies defined (WP1) and internal discussions among the technical work packages (WP3-WP4-WP5-WP6). The requirements have been organized according to the blocks of the general AMASS architecture, and for each one a set of fields has been completed: description, assigned WP, relation to other requirements, actor, stakeholder, priority, type and rationale. These requirements are the basis for the AMASS developments. In total, 151 high-level requirements have been specified.

In conclusion, this deliverable presents the information needed for the other work packages to develop AMASS solutions that meet stakeholders' expectations. The Business Cases and the high-level requirements offer the structure for AMASS designers and implementers to guarantee that the AMASS results provide added value for the stakeholders.

Abbreviations

AA	Airworthiness Authorities
AADL	Architecture Analysis & Design Language
ADAS	Advanced Driver Assistance Systems
AEC	Automotive Electronics Council
AENA	Spanish Airports and Air Navigation
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
API	Application Programming Interface
APNT	Alternative Position, Navigation, and Timing
ARP	Aerospace Recommended Practice
ARTA	AMASS Reference Tool Architecture
ASIL	Automotive Safety Integrity Level
ATM	Air Traffic Management
BC	Business Case
BPMN	Business Process Model and Notation
CAAC	Civil Aviation Administration of China
CACM	Cooperative Adaptive Cruise Control
CCL	Common Certification Language
CHESS	Composition with Guarantees for High-integrity Embedded Software Components Assembly
CNS/ATM	Communication, Navigation, Surveillance and Air Traffic Management
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical Systems
CS	Case Study
DAL	Development Assurance Levels
DCAC	General Directorate of Civil Aviation
DFS	German Air Traffic Control
DME	Distance Measuring Equipment
DSP	Digital Signal Processor
DVOR	Doppler VHF Omni Ranging
EASA	European Agency for Safety in Aviation
ECSS	European Cooperation for Space Standardization
ENAV	Italian Company for Air Navigation Services
EUROCAE	European Organization for Civil Aviation Equipment
EMC	ElectroMagnetic Compatibility
EOQA	Expert ou Organisme Qualifié Agréé
EPSF	Établissement Public de Sécurité Ferroviaire
ESA	European Space Agency
FAA	Federal Aviation Administration
FHA	Function Hazard Assessments
FMEA	Failure mode and effects analysis
FMI	Functional Mock-up Interface
FMU	Functional Mock-up Unit
FMVEA	Failure Modes, Vulnerabilities and Effects Analysis
FuSa	Functional Safety
FPGA	Field Programmable Gate Array

FTA	Fault Tree Analysis
GPS	Global Positioning System
GSN	Goal Structuring Notation
GUI	Graphical User Interface
HARA	Hazard Analysis Risk Assessment
HTML	HyperText Markup Language
HW	Hardware
IAC-AR	Interstate Aviation Committee-Aviation Register
IACS	Industrial Automation and Control System
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICCP	Inter-Control Center Communications Protocol
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
ILS	Instrument Landing System
IoT	Internet of Things
IMA	Integrated Modular Avionics
IRU	Inertial Reference Unit
ISA	Independent Safety Assessor
ISO	International Organization for Standardization
IT	Information Technology
LOI	Level Of Involvement
MBD	Model-based design
MBSA	Models-Based Safety Assessment
MCU	MicroController Unit
MoSCoW	Must have, Should have, Could have, and Won't have but would like
MMS	Manufacturing Messaging Specification
MS	MicroSoft
N.A.	Not Applicable
NATS	National Air Traffic Services
OBSW	On Board Software
OEM	Original Equipment Manufacturers
OMG	Object Management Group
OPENCOSS	Open Platform for EvolutioNary Certification Of Safety-critical Systems
OSLC	Open Services for Lifecycle Collaboration
OSRA	On-Board Software Reference Architecture
PL	Performance Level
PLC	Programmable Logic Controller
PSSA	Preliminary System Safety Assessment
RAMS	Reliability, Availability, Maintainability and Safety
ReqIF	Requirements Interchange Format
RM	Requirements Management
RNAV	aRea NAVigation
RNP	Required Performance Navigation
RTCA	Radio Technical Commission for Aeronautics
RTU	Remote Terminal Units
S2OPL	Safety- and Security- Oriented Process Line
SA	Safety Analysis
SACM	Structured Assurance Case Metamodel

SAE	Society of Automotive Engineers
SAM	Safety Assessment Methodology
SATNAV	Satellite Navigation
SCADA	Supervisory Control And Data Acquisition
SEE	Single Event Effects
SIL	Safety Integrity Level
SoC	System on Chip
SOI	Stage of Involvements
SPICE	Software Process Improvement and Capability Determination
SSA	System Safety Assessments
STRMTG	Service Technique des Remontées Mécaniques et des Transports Guidés
STO	Scientific and Technical Objectives
SysML	Systems Modeling Language
SW	Software
TARA	Threat Assessment & Remediation Analysis
TC	Type Certificates
TCP/IP	Transmission Control Protocol/Internet Protocol
UML	Unified Modelling Language
V&V	Verification and Validation
WP	Work Package

References

[1] D3.1 Baseline and requirements for architecture-driven assurance, 30 September 2016

[2] D4.1 Baseline and requirements for multiconcern assurance, 30 September 2016

[3] D5.1 Baseline requirements for seamless interoperability, 30 September 2016

[4] D6.1 Baseline and requirements for cross/intra-domain reuse, 30 September 2016

[5] OPENCOSS project http://www.opencoss-project.eu/

[6] CHESS project http://www.chess-project.org/

[7] SafeCer project http://www.safecer.eu/

[8] http://www.hubnet.org.uk/filebyid/613/SmartGridComms.pdf

[9] D1.1 Case studies description and business impact, 30 November 2016

[10] https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe/at_download/fullReport

[11] D8.5 Dissemination and Training Plan, 28 July 2016

[12] D2.2 AMASS reference architecture, 30 November 2016

Appendix A: Summary of High Level Requirements

High Level Requirements related to AMASS Platform Basic Building Blocks

1.-High Level Requirements for System Component Specification

WP3_SC_001	System abstraction levels browsing
WP3_SC_002	System abstraction levels editing
WP3_SC_003	Modelling languages for component model
WP3_SC_004	Formalize requirements into formal properties
WP3_SC_005	Requirements allocation
WP3_SC_006	Specify component behavioural model (state machines)
WP3_SC_007	Fault injection (include faulty behaviour of a component)

2.-High Level Requirements for Assurance Case Specification

WP4_ACS_001	Assurance case edition
WP4_ACS_002	Argumentation architecture
WP4_ACS_003	Drag and drop argumentation patterns
WP4_ACS_004	Provide guidelines for argumentation patterns
WP4_ACS_005	Provide a structured language to the text inside the claims
WP4_ACS_006	Provide guidelines for argumentation
WP4_ACS_007	Argumentation import/export
WP4_ACS_008	Traceability of the dependability case
WP4_ACS_009	Find high level claims
WP4_ACS_010	Composition of the overall argument
WP4_ACS_011	Assurance case status report
WP4_ACS_012	Formal validation of assumptions and context when arguments modules are connected
WP4_ACS_013	Provide quantitative confidence metrics about an assurance case in a report

3.-High Level Requirements for Evidence Management

WP5_EM_001	Evidence characteristics specification
WP5_EM_002	Evidence traceability
WP5_EM_003	Evidence change impact analysis
WP5_EM_004	Evidence evaluation
WP5_EM_005	Evidence information import
WP5_EM_006	Evidence information export
WP5_EM_007	Derivation of evidence characterization model
WP5_EM_008	Visualization of chains of evidence
WP5_EM_009	Suggestion of evidence traces
WP5_EM_010	Evidence lifecycle information storage
WP5_EM_011	Interactive evidence change impact analysis
WP5_EM_012	Evidence trace verification
WP5_EM_013	Link of evidence to other assets
WP5_EM_014	Evidence resource specification
WP5_EM_015	Resource part selection
WP5_EM_016	Evidence report generation

4.-High Level Requirements for Compliance Management

WP6_CM_001	Modelling of standards
WP6_CM_002	Tailoring of Standards models to specific projects
WP6_CM_003	Correlating processes to the requirements
WP6_CM_004	Triggering compliance Checking
WP6_CM_005	Compliance Monitoring
WP6_CM_006	Compliance Status to Externals
WP6_CM_007	Useful Feedback Upon Violations
WP6_CM_008	Process Compliance (informal) management
WP6_CM_009	Process Compliance (formal) management)
WP6_CM_010	Compliance map generation from argument evidences

5.-High Level Requirements for Access Manager

WP5_AM_001	User authentication
WP5_AM_002	User access
WP5_AM_003	User action log
WP5_AM_004	User profiles
WP5_AM_005	Access rights groups

6.-High Level Requirements for Data Manager

WP5_DM_001	Multi-platform availability
WP5_DM_002	Simultaneous data access
WP5_DM_003	Consistent data access
WP5_DM_004	Real-time data access feedback
WP5_DM_005	System artefact information storage
WP5_DM_006	Standard formats storage
WP5_DM_007	Data versioning
WP5_DM_008	Secure data access

High Level Requirements related to Architecture-Driven Assurance (STO1)

1.-High Level Requirements for System Architecture Modelling for Assurance

WP3_SAM_001	Trace component with assurance assets
WP3_SAM_002	Impact assessment if the component changes
WP3_SAM_003	Compare different architectures according to different concerns which have been specified before
WP3_SAM_004	Integration with external modelling tools

2.-High Level Requirements for Assurance Patterns Library Management

WP3_APL_001	Drag and drop an architectural pattern
WP3_APL_002	Edit an architectural pattern
WP3_APL_003	Use of architectural patterns at different levels
WP3_APL_004	Architectural Patterns suggestions
WP3_APL_005	Generation of argumentation fragments from architectural patterns/decisions

3.-High Level Requirements for Contract Based Assurance Composition

WP3_CAC_001	Validate composition of components by validating their assurance contract
WP3_CAC_002	Assign contract to component
WP3_CAC_003	Structure properties into contracts (assumptions/guarantees)

WP3_CAC_004	Specify contract refinement
WP3_CAC_005	General management of contract component assignments
WP3_CAC_006	Refinement-based overview
WP3_CAC_007	Overview of check refinements results
WP3_CAC_008	Contract-based validation and verification
WP3_CAC_009	Improvement of Contract definition process
WP4_CAC_010	Contract-based trade-off analysis
WP3_CAC_011	Overview of contract-based validation for behavioural models
WP3_CAC_012	Browse Contract status
WP3_CAC_013	Specify contracts defining the assumption and the guarantee elements

4.-High Level Requirements for V&V Based Assurance

WP3_VVA_001	Traceability between different kinds of V&V evidence
WP3_VVA_002	Trace model-to-model transformation
WP3_VVA_003	Validate requirements checking consistency, redundancy, … on formal properties
WP3_VVA_004	Trace requirements validation checks
WP3_VVA_005	Verify (model checking) state machines
WP3_VVA_006	Automatic provision of HARA/TARA-artifacts
WP3_VVA_007	Generation of reports about system description/verification results
WP3_VVA_008	Automatic test cases specification from assurance requirements specification
WP3_VVA_009	Capability to connect to tools for test case generation based on assurance requirements specification of a component/system
WP3_VVA_010	Model-based safety analysis
WP3_VVA_011	Simulation-based Fault Injection
WP3_VVA_012	Design Space Exploration

High Level Requirements related to Multi-Concern Assurance (STO2)

1.-High Level Requirements for Dependability Assurance Modelling

WP4_DAM_001	Capability to model relationships between concerns
WP4_DAM_002	Capability to capture conflicts occurring during system development and the trade-off process

2.-High Level Requirements for Contract Based Multi-concern Assurance

WP4_CMA_001	The AMASS tools must support specification of variability at the argumentation level
WP4_CMA_002	Component contracts must support multiple concerns
WP4_CMA_003	Contract based multi-concern assurance

3.-High Level Requirements for System Dependability Co-Analysis/Assessment

WP4_SDCA_001	System dependability co-architecturing and co-design
WP4_SDCA_002	System dependability co-verification and co-validation
WP4_SDCA_003	The system shall allow combinations of safety and security analysis

High Level Requirements related to Seamless Interoperability (STO3)

1.-High Level Requirements for Tool Integration Management

WP5_TI_001	Automatic data collection
WP5_TI_002	Automatic data export
WP5_TI_003	Tool chain deployment support
WP5_TI_004	System analysis tools interoperability

WP5_TI_005	System specification tools interoperability
WP5_TI_006	V&V tools interoperability
WP5_TI_007	Version management tools interoperability
WP5_TI_008	Quality management tools interoperability
WP5_TI_009	MS Office applications interoperability
WP5_TI_010	Interoperability throughout CPS lifecycle
WP5_TI_011	Non-proprietary data exchange
WP5_TI_012	Data entry effort
WP5_TI_013	Continuous data management
WP5_TI_014	Client-server support
WP5_TI_015	Service offer and discovery
WP5_TI_016	Performance monitoring
WP5_TI_017	Standards-based interoperability
WP5_TI_018	Extended standard-based interoperability

2.-High Level Requirements for Collaborative Work Management

WP5_CW_001	Collaborative system analysis
WP5_CW_002	Collaborative system specification
WP5_CW_003	Collaborative management of compliance with standards and of process assurance
WP5_CW_004	Collaborative re-certification needs & consequences analysis
WP5_CW_005	Collaborative system V&V
WP5_CW_006	Collaborative model-based systems engineering
WP5_CW_007	Collaborative assurance evidence management
WP5_CW_008	Collaborative product reuse needs & consequences analysis
WP5_CW_009	Collaborative assurance case specification
WP5_CW_010	Collaborative compliance needs specification
WP5_CW_011	Collaborative assurance assessment
WP5_CW_012	Collaborative compliance assessment
WP5_CW_013	Metrics & measurements reports

3.- High Level Requirements for Tool Quality Assessment and Characterization

WP5_TQ_001	Tool qualification information needs
WP5_TQ_002	Tool quality evidence management
WP5_TQ_003	Tool quality information import
WP5_TQ_004	Tool quality needs indication
WP5_TQ_005	Tool quality requirements fulfilment

High Level Requirements related to Cross/Intra-Domain Reuse (STO4)

1.-High Level Requirements for Reuse Assistant (Cross/Intra-Domain)

WP6_RA_001	Intra-Domain, Intra standard, Reuse Assistance
WP6_RA_002	Intra-Domain, Cross standards, Reuse Assistance
WP6_RA_003	Intra-Domain, Cross versions, Reuse Assistance
WP6_RA_004	Cross-Domain Reuse Assistance
WP6_RA_005	Intra-Domain, Intra standard, Different Stakeholders, Reuse/Integration Assistance
WP6_RA_006	Reusable off the shelf components
WP6_RA_007	Provision of metrics about process-related reuse (e.g., size of commonality)
WP6_RA_008	Provision of metrics about product-related reuse (e.g., size of commonality)

WP6_RA_009	Provision of metrics about assurance case-related reuse (e.g., size of commonality)

2.-High Level Requirements for Semantic Standards Equivalence Mapping

WP6_SEM_001	Semantics-based mapping of standards

3.-High Level Requirements for Product/Process/Assurance Case Line Specification

WP6_PPA_001	The AMASS tools must support variability management at process level
WP6_PPA_002	Semi-automatic generation of product arguments
WP6_PPA_003	Semi-automatic generation of process arguments
WP6_PPA_004	The AMASS tools must support management of variability at the component level
WP6_PPA_005	The AMASS tools must support variability management at the assurance case level