Validation Strategy

R. Wever (NLR), L. Save (Deep Blue), S. Rozzi (Deep Blue), T. Longhurst (CAA)

This document describes the validation strategy. It explains the approach towards the validation of the ASCOS results, the user expectations and validation objectives. The performance indicators to be used in the validation have been established. Finally the report defines the high level validation plan.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	L. Save (Deep Blue)

Grant Agreement No.	314299
Document Identification	D5.1
Status	Approved
Version	1.2
Date of Issue	31-08-2014
Classification	Public

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	R. Wever et al.	27-06-2014	All	Version for approval by PMT
1.1	L.J.P. Speijker	19-08-2014		Update by ASCOS coordinator
1.2	L.J.P. Speijker	31-08-2014		Comments PMT processed

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	J. Scholte	**5/30/2014**
CAAi	S. Long	**6/4/2014**
JRC	W. Post, R. Menzel	**6/5/2014**
CertiFlyer	G. Temme, M. Heiligers	**6/10/2014**
TU Delft	R. Curran, H. Udluft	**6/4/2014**
Thales Air Systems	B. Pauly	**6/4/2014**
Avanssa	N. Aghdassi	**8/24/2014**
APSYS	S. Bravo Munoz	**8/19/2014**
Organisation Responsible for Approval	Name of person approving the document	Date
Deep Blue	L. Save	**6/27/2014**
NLR	L.J.P. Speijker	**8/31/2014**

Document Distribution

Organisation	Names
European Commission	M. Kyriakopoulos
NLR	L. Speijker, A. Rutten, M.A. Piers, P. van der Geest, A. Roelen, J.J Scholte, J. Verstraeten, A.D. Balk, E. van de Sluis, M. Stuip
Thales Air Systems GmbH	G. Schichtel, J.-M. Kraus
Thales Air Systems SA	B. Pauly
Airbus Defence and Space APSYS	S. Bravo Muñoz, J.P. Heckmann, M. Feuvrier
Civil Aviation Authority UK	S. Long, A. Eaton, T. Longhurst
ISDEFE	M. Martin Sanchez, I. Etxebarria, M. Sánchez
CertiFlyer	G. Temme, M. Heiligers
Avanssa	N. Aghdassi
Ebeni	A. Simpson, J. Denness, S. Bull
Deep Blue	L. Save
JRC	W. Post, R. Menzel
JPM	J. P. Magny
TU Delft	R. Curran, H. Udluft, P.C. Roling
Institute of Aviation	K. Piwek, A. Iwaniuk
CAO	P. Michalak, R. Zielinski
EASA	K. Engelstad
FAA	J. Lapointe, T. Tessitore
SESAR JU	P. Mana
Eurocontrol	E. Perrin
CAA Netherlands	R. van de Boom
JARUS	R. van de Leijgraaf
SRC	J. Wilbrink, J. Nollet
ESASI	K. Conradi
Rockwell Collins	O. Bleeker, B. Bidenne
Dassault Aviation	B. Stoufflet, C. Champagne
ESA	T. Sgobba, M. Trujillo
EUROCAE	A. n'Diaye
TUV NORD Cert GmbH	H. Schorcht
FAST	R. den Hertog

Acronyms

Acronym	Definition
ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
CAA	Civil Aviation Authority
CATS	Causal model for Air Transport Safety
CMA	Continuous Monitoring Approach
CNS	Communication, Navigation, Surveillance
CPS	Certification Process study
CS	Certification Specifications
EASA	European Aviation Safety Agency
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems
E-OCVM	European Operational Concept Validation Methodology
ESD	Event Sequence Diagram
FAA	Federal Aviation Administration
FAST	Future Aviation Safety Team
FDM	Flight Data Monitoring
FT	Fault Tree
ICAO	International Civil Aviation Organisation
KPA	Key Performance Area
KPI	Key Performance Indicator
NASA	National Aeronautics and Space Administration
SESAR	Single European Sky ATM Research
SPI	Safety Performance Indicator
TAS	Total Aviation System
UG	User Group
WP	Work Package

This page is intentionally left blank

Executive Summary

This report defines the validation strategy: it describes the way in which the ASCOS project plans to conduct the validation activities in WP5. Validation is defined as the process by which the "fitness for purpose" of the ASCOS results is evaluated, i.e. to determine if they are suitable for their intended purpose and bring the expected benefits for the user. The scope of the validation will be three ASCOS "products": 1) the newly proposed certification approach developed in WP1 and defined in D1.3 [4]; 2) the continuous safety monitoring process described in D2.3 [9]) and the supporting tool (D2.4) developed in WP2; and 3) the safety risk assessment methodology, risk model and tool delivered by WP3 in D3.2 [8] and D3.3 [29].

The document provides a summary of the current challenges, problems and constraints involved in certification to provide a background for the development of the validation strategy. On the one hand, the need for improvement comes from shortcomings in the existing certification process, and, on the other hand, from developments in the domain of aviation regulation and certification, the introduction of new technologies and operations, and the demand for high(er) levels of safety performance. The three ASCOS "products" to be validated are described, summarising the expected benefits, roles, enablers and limitations. Next, the maturity level of the three ASCOS products is assessed to ensure that the development of the validation plan will be compatible with the ASCOS results' maturity level. The maturity level is assessed as "Initial concept description" and "Feasibility, development and exploration of concepts, demonstrating fitness for purpose of individual concepts". This makes sense since ASCOS is a R&D project that aims to explore preliminary concepts of a novel certification and continued airworthiness approach with an initial evaluation of their feasibility and acceptability. Considering the maturity level of the ASCOS solutions, the aim of the validation shall be to evaluate the fitness for purpose and the expected benefits in order to collect data, user feedback and recommendations. This enables further exploration and refinement, within ASCOS WP1.5, of the new approach into a consolidated new certification process, with supporting risk based methods and tools.

Stakeholders (organisations) were identified that have an interest or a role in the described challenges and the proposed solutions to overcome the identified shortcomings and to address the challenges in the current and future certification process. A list of user expectations with respect to the ASCOS results was collected from ASCOS public material [1], the user group meetings, technical meetings with user group members and earlier ASCOS questionnaires. The list of user expectations is divided into four topics: New certification approach; Continuous safety monitoring process and tool; Safety risk assessment methodology and tool; and Usability and applicability of the proposed ASCOS "products". These user expectations form a basis for the validation objectives and performance framework, i.e. they are the reference to determine if the results are fit for purpose and to evaluate if they bring the expected benefits.

Based on the user expectations the following four validation objectives were formulated.

- Validate that the ASCOS approach towards certification, including the developed supporting processes and tools, offers improvement over the existing certification and approval processes, while increasing the level of safety and safety assurance provided with the current certification approaches.

- Validate that the ASCOS approach towards certification including the developed supporting processes, tools and databases offers improvement for continuous safety monitoring.
- Validate that the ASCOS approach towards certification including the developed supporting processes, aviation safety assessment methodology, risk models and tools for risk assessment and safety based design risk offers improvement in certification activities.
- Validate that the ASCOS approach towards certification including the developed supporting processes, tools and guidance material is acceptable to the stakeholders to adopt the new approach and put it into practice.

A performance framework was developed to be able to assess the performance of the ASCOS results in the validation exercises. This framework was developed from the reviewing the current challenges, user expectations and ASCOS public material [1]. The performance framework consists of a set of Key Performance Areas (KPAs), Key Performance Indicators (KPIs) and metrics. The KPAs are areas of performance that reflect high-level ambitions and expectations of the stakeholders. Seven KPAs are defined: 1. Soundness of the certification safety assurance documentation, 2. Efficiency of the certification process, 3. Cross domain integration, 4. Harmonization, 5. Accommodation of innovation, 6. Operability of ASCOS processes and tools, and 7. Flexibility. In the ASCOS performance framework, KPIs will be used to measure the “fitness for purpose” of the ASCOS results in a specific area. The metrics are the way in which the KPIs are measured or expressed. The KPIs and metrics have been identified for the KPAs for each of the three ASCOS “products”. During the validation exercises feedback will be collected from the involved users by means of a questionnaire, which will be designed in follow-up activities (WP5.2). These KPIs will be addressed in the validation questionnaire.

A list of validation requirements was established, i.e. items that need to be satisfied to prepare for and achieve validation. Three important ones on the list are:

- The ASCOS User Group (UG) represents different stakeholders in the aviation industry and in certification domains. The involvement of UG members is essential for a successful validation. For this purpose it is important to timely contact UG members to secure their willingness and availability in the validation exercises. They need to be contacted prior to the first workshop to clarify aspects such as their expected role and contribution, the required expertise, the planning and set-up of the workshops and the required effort.
- The validation shall take into account the experience and results from the application of the ASCOS results in the WP4 case studies. The WP5 participants shall regularly exchange information with the WP4 case studies about the fitness for purpose and assessed performance/benefits of ASCOS results, using the performance framework defined in the validation strategy.
- The participation of relevant ASCOS partners from WP1, 2, and 3 is required to provide technical and logistical assistance during the preparation of the training material, in relation to the ASCOS software tools needed for the validation exercises and the execution of these tools.

The document concludes with a list of key validation activities, an initial validation planning and a template for the validation plan which is to be developed in follow-up activities (WP5.2).

This page is intentionally left blank

Table of Contents

List of Tables

1 Introduction

1.1 Project background

According to the ASCOS Public material [1], the main objective of the ASCOS project is "to develop novel certification process adaptations and supporting safety driven design methods and tools to ease the certification of safety enhancement systems and operations, thereby increasing safety". It is further mentioned in [1] that the aim of ASCOS is "to ease the efficient and safe introduction of safety enhancement systems and operations with special characteristics that are not yet covered in existing Certification Specifications. Therefore a novel and innovative approach towards certification is required that: 1) Is more flexible with regard to the introduction of new products and operations; 2) Is more efficient, in terms of cost and time, than the current certification processes; and 3) Considers the impact on safety of all elements of the aviation system and the entire system lifecycle in a complete and integrated way. [...] To contribute to a reduction of the accident rate by focusing on novel systems and operations for priority areas that exhibit relatively high risk. The focus of ASCOS is on safety improvements in priority risk areas in the total aviation system. ASCOS addresses safety enhancements that will lead to a reduction of fatal accidents due to: loss of control in flight, aircraft system or component failure or malfunction, aircraft ground handling aircraft damage and Air Traffic Management related incidents/accidents".

In previous Work Packages (WP) the ASCOS project team worked on the following:

- WP1: An analysis of the existing European certification and rulemaking process, followed by a proposal for adaptations in the certification approach to ease certification of safety enhancement systems and operations.
- WP2: The development of a process and supporting tools for continuous safety monitoring, using a baseline risk picture for all the parts of the total aviation system. This included the development of a safety performance indicator framework and the baseline risk picture, i.e. the establishment of the current risk level of the various parts of the total aviation system.
- WP3: The development of a total aviation system safety assessment method and supporting tools that can be used for safety based design of new systems, products and/or operations. This included the development of a risk model based on accident scenarios and an approach to assess future and emerging risks.

The project follows a total system approach, dealing with all aviation system elements in an integrated way over the complete life-cycle. The new certification approach, process and tools for continuous safety performance monitoring and risk assessment will be applied in four case studies in WP4. The case studies concern the certification of aircraft failure management systems, a future ATM/CNS system for improved surveillance, aircraft systems for improved controllability in flight, and aircraft ground handling operations.

The ASCOS User Group is involved in various stages of the project to keep the project focused and to facilitate uptake of project results. They have an important role to play in the validation effort of the ASCOS products. This document presents the validation strategy and methodology (D5.1), which is part of WP5 "Validation".

1.2 Objective

The objectives of this study are:

- To define the scope of the validation exercises,
- To define the validation objectives,
- To describe the expected outcome, and
- To define the performance framework and metrics to be used in the validation.

The validation strategy will be input for the definition and planning of the actual validation activities, and the actual development of the validation experimental plan and scenarios in follow-up activities (WP5.2).

1.3 Document structure

This document describes the validation strategy:

- Chapter 2 explains the validation scope, approach and management, and relevant definitions.
- Chapter 3 describes the problem statement regarding the certification process and explains the constraints and high-level aims of ASCOS.
- Chapter 4 includes the stakeholder analysis, expectation and requirements that form the foundation for the validation activities.
- Chapter 5 describes the contribution and proposed solution by the ASCOS project in the certification domain. It includes an overview of the ASCOS deliverables or products that will be validated, with an assessment of their maturity level.
- Chapter 6 presents the validation objectives.
- Chapter 7 sets the performance objectives, Key Performance Areas, Key Performance Indicators and metrics for the validation activities.
- Chapter 8 defines the validation requirements.
- Chapter 9 concludes the validation strategy with a validation work plan.
- Chapter 10 presents some concluding remarks.

2 Validation approach

2.1 Definition of validation, verification and certification

2.1.1 Validation

In the ASCOS project the term validation is considered as the process by which the fitness-for-purpose of the proposed certification approach, supporting processes and tools is established. The objective of the validation of the ASCOS results is to demonstrate that they are suitable for their intended purpose or use and that they bring the expected benefits for the user in terms of costs and duration of the certification process, repeatability, scalability and so on. In the validation, the evaluation of the "fitness" for purpose of the end results will be done against a performance framework (developed in chapter 7). Validation aims to confirm by different approaches (e.g. testing, reviewing, simulation), providing objective evidence, that a particular user requirement or need is fulfilled. The stakeholders have an important role in the evaluation of the acceptance or suitability of the end product. Another objective of the validation process is to ensure that the requirements (e.g. for tools) are complete and correct and reflect the higher-level user needs. Validation can be translated into the question: "Are we building the right system?". Validation is a higher-level activity compared to verification.

2.1.2 Verification

Verification is the set of activities aimed at testing or demonstrating that the product (e.g. a tool) meets the technical specifications. The verification aims to assess the technical quality and performance of the products. It can be defined as focusing on the technology and answers the question "Are we building the system right?". In the design process first a set of technical requirements or specifications will be developed based on (high-level) user needs. Next, the design and development of the product takes place based on the design specifications. Finally, in the verification process the question that needs to be answered is: does the end product meet the technical specifications? For example, suppose there is a requirement that the software tool should enable the modification of risk model element probabilities. In the verification process it should be proved that the developed tool meets this (technical) specification.

2.1.3 Certification

In this study "certification" is defined as the process and set of activities aiming at the satisfaction of an authority that a "deliverable" (e.g. aircraft, aviation product, service, or organisation) complies with a set of regulations in order to ensure its proper operation and to ensure continued performance of these items during their operational life. For aeronautical products, the approach based on the granting of a type certificate for an approved design is in general a compliance based approach centred on demonstrating satisfaction of detailed,

prescriptive specification. On the other hand, for air navigation services the approach has historically been performance based and is centred on providing evidence that a particular performance level will be obtained.

2.2 ASCOS validation approach

2.2.1 Validation management

ASCOS WP5 "Validation" will provide the validation framework, and plan and conduct the exercises to validate the proposed certification approach, processes, methods and tools developed in WP1 to WP3 of ASCOS. The results of the case studies conducted in WP4 will be incorporated in the WP5 exercises to simulate and validate an overall certification process, and to assess whether the ASCOS results meet the user expectations. Validation results will provide feedback about the fitness for purpose of the ASCOS results and can be used to refine and consolidate the ASCOS results.

The validation methodology applied during WP5 will follow the stepped planning framework approach of the European Operational Concept Validation Methodology (E-OCVM) developed by Eurocontrol. The ASCOS results are not related to an operational concept or system and the associated staged development or life cycle. Hence, the guidelines from E-OCVM for concept validation do not apply directly to the ASCOS results. Nevertheless, the principles and good practice behind the E-OCVM approach were used as inspiration for the development of the ASCOS validation strategy. Consequently, the validation will be broken down in four distinguished phases, which coincide with work packages 5.1, 5.2, 5.3 and 5.4 respectively. These phases will be explained in the following sections.

2.2.2 Phase 1: Validation Strategy.

This phase provides the strategy for the validation: the way in which we plan to achieve the validation. The validation strategy sets the framework for the validation activities and exercises, defining tools, techniques, reference models, methods etc. to plan and execute the validation. The remainder of this document covers the validation strategy. It was decided to follow the validation strategy development (sub)steps from E-OCVM and tailor them to the ASCOS project as follows:

- Step 1: Problem statement and needs (chapter 3).
- Step 2: Stakeholder analysis, expectations, requirements and needs (chapter 4).
- Step 3: Identification of ASCOS solutions, and assessment of their maturity (chapter 5).
- Step 4: Define the validation objectives (chapter 6).
- Step 5: Define the performance framework, KPAs, KPIs, metrics (chapter 7).
- Step 6: Define the validation requirements (chapter 8).
- Step 7: Define the validation work plan (chapter 9).

The current report (D5.1) describes the validation strategy, consisting of the validation expectations and objectives, hypothesis, metrics, and a set of guidelines and templates that form the basis for the definition, preparation and execution of the validation exercises and scenarios.

The validation strategy provides input to the WP5.2 Experimental plan and scenarios. That task will develop specific validation plans for the three main ASCOS products. According to ASCOS Public material [1], the Case Studies conducted in WP4 will represent some parts of these validation plans for the new certification approach, providing useful validation results. The combination of the Case Studies and validation exercises output will provide data for the validation objectives. The Validation Plans will describe all aspects necessary to run the exercises in detail, e.g. exercise objectives, indicators and metrics, scenarios and the roles of the different stakeholders, the activities to be undertaken the method(s), technique(s) and tool(s) to be used and the deliverables that will be prepared. The plan will also include any procedures to be used to ensure the quality of the work.

2.2.3 Phase 2: Experimental Plan and Scenarios

The Validation Plans will be developed for the validation of results from the ASCOS WP1, WP2 and (part of) WP3. It will describe all aspects necessary to run the validation exercises, such as exercise objectives, indicators and metrics, scenarios and the roles of the different stakeholders, the activities to be undertaken, the method(s), technique(s) and tool(s) to be used (also for the posterior data analysis) and the deliverables that will be prepared. The plan will also include procedures to be used to ensure the quality of the work. The validation strategy describes the validation organisation and management at “strategic” level, whereas the validation plans describe the validation activities at the “experiment” level.

2.2.4 Phase 3: Validation exercises execution

The actual validation will take place in WP5.3 “Validation exercises execution”. During this task the validation exercises defined in the Validation Plans (WP5.2) will be executed in order to obtain a set of measurements, user/expert feedback and other data that will be subsequently analysed and reported in the next phase.

2.2.5 Phase 4: Result analysis and reporting

The last phase in the validation will be the analysis of validation results and reporting. This phase will be carried out in WP5.4 and will be briefly described below. It is foreseen that this phase focusses on two activities: analysis of validation results and defining conclusion and recommendations. The analysis and evaluation of the validation data produces an overall view on the fitness for purpose of the ASCOS products (i.e. certification approach and tools). Conclusions shall be related to the validation objectives defined in the

D5.1 validation strategy, while the recommendations should focus on improvements of the ASCOS results. The WP4 case studies results should also be taken into account. It is important that the conclusions and recommendations from the validation are fed back to the WP1.5 where the final (revised) outline certification process will be consolidated. Feedback that will be collected on WP2 and WP3 products will be transferred to WP1 as both WP2 and WP3 will be completed before the end of the validation activities.

The analysis and evaluation of the validation data produces an overall view on the fitness for purpose of the ASCOS products (i.e. certification approach and tools). First, data from the validation exercises need to be collected and analysed. Validation results from the certification process adaptations, the new certification approach, the case studies and the ASCOS tools need to be integrated in the data analysis. The data need to be checked for completeness and correctness. The results of the validation can be a set of quantitative analyses or indicators (e.g. statistics, quantitative model outputs or specific performance indicators) and a set of qualitative results (e.g. a set of statements, observations, assessments, questionnaires).

Secondly, data need to be processed so that they can be related to the performance framework and validation objectives. The validation objectives have a performance criterion, metric or target, which needs to be assessed in the data analysis. For each validation objective it needs to be determined if the available data is sufficient, correct etc. to assess whether or not the objective is satisfied, or to determine the level of performance. The results will be compared with the stakeholders' expectations and project objectives. This comparison will reveal which results can be considered as meaningful and will result in recommendations on improvements.

The results of the data analysis form the basis for the conclusions and recommendations. Conclusions shall be related to the validation objectives defined in the D5.1 validation strategy, because the conclusions need to address the fitness for purpose of the ASCOS results. The recommendations should focus on improvements of the ASCOS results.

Finally, the validation report will be prepared where all results of the entire validation are summarised. It should contain the following information:

- Validation objectives;
- Validation exercises and scenarios (design, platforms and tools used etc.);
- Data analysis and results (quality, completeness, coverage etc.);
- Results related to the performance framework and performance indicators (defined in chapter 7) and the satisfying of objectives, providing evidence for each validation objective. Participants and their involvement;
- Conclusions and recommendations.

3 Problem statement and needs

3.1 Background

For the development of the validation strategy it is important to understand the challenges, problems and constraints in the current certification practices where the ASCOS solutions intend to bring improvement. The challenges were collected by reviewing ASCOS public material [1] and specific deliverables of the ASCOS project that identified and analysed current challenges, shortcomings, and/or bottlenecks in the certification practice and continuous safety monitoring. Section 3.2 summarises the current challenges in three domains: the certification process, continuous safety monitoring and safety risk management. Section 3.3 addresses the constraints relevant to these challenges. These challenges and needs, together with the user expectations (see chapter 4), form the foundation for the performance framework that is going to be used to in the validation (see chapter 7). Therefore, the challenges and needs described in section 3.2 are matched with related Key Performance Areas (KPAs) defined in chapter 7 to show where they are addressed in the performance framework. Appendix B contains a more detailed overview of shortcomings, bottlenecks and issues in certification collected during the project, while Appendix C provides some examples of mentioned issues.

3.2 Current challenges

3.2.1 Certification process

The ASCOS Public material [1] and D1.1 [3] explain the challenges for the current and future certification process and the main conclusions will be summarised in this section. On the one hand, the need for improvement comes from shortcomings in the existing certification process, and on the other hand from developments in the domain of aviation regulation and certification, the introduction of new technologies and operations, and the demand for high(er) levels of safety performance.

ASCOS WP1.1 addressed the analysis of existing regulations and certification processes to identify potential shortcomings and bottlenecks in the current certification processes. The need for improvement of existing certification processes already became clear after the publication of the FAA Commercial Airplane Certification Process Study (CPS) [2]. It provides an evaluation of selected aircraft certification, operations, and maintenance processes. Reference [3] summarises the findings and observations of the CPS, several of which are also applicable to Europe and are still applicable to the situation of today. Other studies, as well as the findings of various accident investigations, confirm the shortcomings in the existing certification processes as identified in the CPS report.

The first finding mentioned in reference [2] is that the human performance assessment (human response to failure conditions and addressing human error in design, operation and maintenance) needs improvement. According to the conclusions of the CPS report, there is no reliable process to ensure that assumptions made in the design and certification safety assessments are valid with respect to operations and maintenance activities

and, furthermore, to ensure that human operators are aware of these assumptions when developing their operations and maintenance procedures. It became clear that aircraft certification standards may not reflect the actual operating environment. Another finding from the CPS that applies to Europe is the aviation safety data management. For example, multiple data collection and analysis programs exist in Europe without adequate coordination or executive oversight. In addition, the interfaces between maintenance, operations, and certification need to be better taken into account. For example, improvement is still possible in capturing the lessons learned from specific experiences in manufacturing, maintenance, and flight operations, and in making these available for the aviation industry. *(Related KPA: 1. Soundness of the Safety Assurance Documentation.)*

Another finding is that inconsistencies exist between the safety assessments conducted for the initial type certificate (TC) and some of those conducted for subsequent alterations to the aircraft as there is no established and detailed enough safety assessment methodology commonly used by all interested parties. *(Related KPA: 4. Harmonisation.)*

Also, current certification processes may take a long time, or can even turn out to be not reasonably feasible. To ease the efficient and safe introduction of safety enhancement systems and operations, a novel and innovative approach towards certification is required that: a) Is more flexible with regard to the introduction of new products and operations; b) Is more efficient, in terms of cost and time, than the current certification processes; and c) Considers the impact on safety of all elements of the aviation system and the entire system life-cycle in a complete and integrated way. *(Related KPA: 1. Soundness of the Safety Assurance Documentation, 2. Efficiency of the Certification Process, 5. Accommodation of innovation.)*

Currently, certification based on prescriptive regulations is primarily used in aircraft certification. In this case solutions must comply with detailed regulations which prescribe parts of the implementation. These effectively are a collective memory based on past experience, and are a very effective way to gradually improve safety. However they may be less suited for the introduction of new concepts and technologies that might not be fully compliant with existing prescriptive regulations, but which could be just as safe or safer. The determination of a certification basis and demonstrating compliance may then take a long time. On the other hand, regulations in the ATM domain are performance based. *(Related KPA: 3. Cross domain integration, 4. Harmonisation, 5. Accommodation of innovation.)*

The aviation system can be regarded as a large system composed of several elements. Safety depends on the elements and on the interfaces between the elements, all of which must be considered during certification because it is the weakest link in the chain that determines aviation safety. The interdependence between the different domains is certainly a driver for improvement of the certification process. In addition to shortcomings in the existing process, further needs for adaptations of the certification process are emerging from the current and future developments in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance. *(Related KPA: 1. Soundness of the Safety Assurance Documentation, 3. Cross domain integration.)*

Moving towards performance based regulation, based upon agreed safety performance in combination with risk based approach to standardisation, is expected to lead to significant improvements in the way that safety risks are controlled [5]. In view of the weak spots identified in the existing certification processes as well as the major regulatory and technological changes currently taking place, novel certification approaches are called for to maintain and improve the affordability of certification processes – both in cost and in duration, to reduce the uncertainties involved, and to make a significant step forward in safety. Multiple solutions may exist, some of which involve approaches in which all safety certification aspects are dealt with in an integrated way from the early design phase of the life cycle towards decommissioning, and which cover the entire aviation system. Other approaches may have a narrower scope, and be targeting specific current certification challenges such as those involved with the treatment of Human Performance aspects in safety assessments and the differences in the approaches followed in ATM certification and aircraft (operations) certification. An issue that deserves specific attention is the increasing integration of the certification processes for a) ATM operational concepts and supporting systems and b) aeronautical products and flight operations. The certification concept for both differs significantly and this might be a cause for future un-clarities with potential safety implications. This is addressed specifically in the ASCOS Deliverables D1.3 and D3.5 *(Related KPA: 1. Soundness of the Safety Assurance Documentation, 2. Efficiency of the Certification Process, 3. Cross domain integration.).*

3.2.2 Continuous Safety Monitoring

Continuous safety monitoring refers to the process for continued airworthiness of aircraft, and maintenance of certificates for air navigation service providers, operators, and manufacturers after they have been certified and while they are being operated / are operating. ASCOS public material [1] explains that there is a need to develop a European wide safety monitoring process that takes into account the existing requirement for states and ANSPs to use (high-level) safety KPIs, while at the same time moving towards a Continuous Monitoring Approach (CMA) employed by all the stakeholders in aviation. The CMA adopted by ICAO is a proactive approach to continuously gather safety data and monitor safety oversight capabilities of Member States. Additionally, safety performance monitoring and measurement is an integral part of safety assurance within ICAO's SMS framework. *(Related KPA: 4. Harmonisation.)*

The CMA principles could be applied to the entire lifecycle and the total aviation systems, or continued airworthiness of aircraft, and maintenance of certificates for air navigation service providers, operators, and manufacturers. This challenge will be addressed by ASCOS by developing and validating a continuous monitoring process in which safety performance indicators will be linked with precursors for main operational issues for commercial air transport operations as identified in the European Aviation Safety plan (EASp) framework [1]. A proper implementation of Continuous Safety Monitoring requires the development of specific safety performance indicators for states, airlines, airports, ANSPs as well as for aviation products designed and manufactured. Performance indicators for aviation safety are relatively new. This is a result of the fact that safety is a somewhat abstract notion and that safety, until recently, was not seen as a performance area that could be actively managed. The widespread introduction of Safety Management System

(SMS) throughout the aviation system has changed this and has resulted in an increasing application of indicators of aviation safety performance. But unlike other performance areas, there is no common framework for safety performance indicators in aviation. Even between stakeholders of the same type (e.g. airlines) there are differences, sometimes fundamental, in the way safety performance is being measured (see [6]). *(Related KPA: 4. Harmonisation).*

During certification many assumptions are made about the operational conditions, crew behaviour (e.g. response times), and system performance. Flight data provides an excellent source for monitoring (trends) in flight operations, system performance and flight crew behaviour which provides feedback on the assumptions made in certification and helps to identify new/changed hazards and assess associated risks. Two possible sources of data that were studied in ASCOS WP2.3 [9] are Flight Data Monitoring (FDM) programs and ATM Safety Data Gathering (ASDG). In most cases events can be defined in the FDM software to monitor flight data in areas that are directly related to for instance operational conditions, crew behaviour and system performance. The data for the events can be compared with the operational, system and behavioural performance as assumed during certification. Both event exceedences and routine events can be used for this purpose (see [9]). *(Related KPA: 1. Soundness of the Safety Assurance Documentation.)*

Integration of safety data from various sources and disciplines is important to understand safety issues, and to enable objective, quantitative risk assessments and risk mitigation. For continuous safety monitoring it could be interesting to validate trends found in various data sources, thus integrating different data, e.g. occurrence data with flight data and vice versa. A challenge in this respect is, first, that there is no standard for reporting forms, so records from (voluntary) reporting programs will differ across the airline industry. The level of detail, completeness and quality of the reports will vary, even within a single airline. Taxonomies used to classify occurrences and the risk levels of occurrences vary by airlines as well. Secondly, the information in the records and narratives may contain very relevant safety information, but it takes a significant effort to analyse large sets of occurrence reports. It takes time and manpower to be able to select the reports relevant to the analysis at hand, and to make an assessment of the relation of the reports to FDM parameters/events. *(Related KPA: 1. Soundness of the Safety Assurance Documentation, 2. Efficiency of the Certification Process.)*

The objective of ASCOS work package 2 ‘Continuous Safety Monitoring’ is to create tools for continuous safety monitoring, using a baseline risk picture for the safety performance of the total aviation system. Introducing a ‘continuous safety monitoring’ process will ensure that new essential safety data is effectively used immediately after it will be available, so that risks will be timely and proactively mitigated.

3.2.3 Safety Risk Management

The current state of the art for the certification of aeronautical products is basically reactive in the sense that changes in certification requirements are often made as a reaction to major accidents or as a reaction to technological advances. Changes to regulations or certification requirements as a results of “past experience” may take several years to implement. In addition, technological and operational advances may develop at such

a pace that it is sometimes difficult to keep regulations up to date or to prepare in time for future developments. A related concern is that safety data will not (yet) be available for new developments, which will hamper the identification of hazards and the assessment of risks. *(Related KPA: 2. Efficiency of the Certification Process, 5. Accommodation of innovation).*

A key step in the proposed improved certification process is an improved hazard identification process, including a 'predictive' approach, aimed at discovering future hazards that are the result of future changes inside or outside the global aviation system, and then initiating mitigating actions before the hazard is introduced [8]. In other words, there is a need to develop a future risk picture. Anticipating on future risks and hazards of (new) aeronautical products, technology and operations by using a 'proactive' and 'predictive' approach helps to make the certification process robust to new developments and support the detection of emerging risks and precursors early in the program [1]. *(Related KPA: 1. Soundness of the Safety Assurance Documentation.)*

Additionally, interfaces between disciplines and aviation domains and the entire system life-cycle needs to be part of a safety assessment methodology to support safety based design to address the increasing integration of the certification processes and to address identified shortcomings [1]. ASCOS D3.1 [7] describes the user needs regarding the safety assessment methodology in more detail. *(Related KPA: 3. Cross domain integration.)*

The need for an integrated risk model in which human factors and cultural aspects are considered in connection with technical and procedural aspects and with specific emphasis on the representation of emerging and future risks (D3.2 [8]) is covered by ASCOS WP3 "Safety Risk Management".

3.3 Constraints

3.3.1 Certification process

The ASCOS deliverable D1.3 [4], a report about the definition and evaluation of innovative certification approaches, provides an initial view of the potential for improving the regulatory framework and supporting certification processes. An important constraint noted in the report is that "drastic changes to the current certification practice will be mostly likely unsuccessful because:

- The requirements and certification practices have been established based on the experience of many decades in which the aviation industry developed into a robust transport system; and
- A decade long process of harmonisation between the leading Agencies around the world has led to a set of requirements that are only marginally different. A process of de-harmonisation would be unacceptable to the stakeholders."

The deliverable D1.3 [4] summarises additional constraints that have to be taken into account regarding the (future) certification adaptions:

- Allow, within each domain, the new certification approach to evolve from the current approach by: keeping the existing approach where no change is required; learning lessons from other domains where this gives improvement; ensuring that bottlenecks and shortcomings are addressed by the proposed approach;
- Avoid unnecessary change, recognising the good approaches already in place;
- Use a common language across all domains based on safety argument concepts (e.g. argument-based as used in OPENCOSS), allowing flexibility to accommodate a variety of approaches across domains.

3.3.2 Continuous Safety Monitoring

The ASCOS report D2.1 [6] about a framework for Safety Performance Indicators (SPI) mentions a number of constraints that has to be taken into account regarding safety performance indicators:

- In order to be able to quantify a proposed safety performance indicator, ECCAIRS data on related occurrences and suitable denominator data from the EASA data warehouse for aviation production data should be used. In Europe, the ECCAIRS software is the standard for reporting system and data is centrally stored in the European data repository. For quantification of the SPIs access to such a large data pool is essential and for that reason it is of vital importance that the SPIs can be unambiguously linked with the ECCAIRS system [6].
- It should be ensured that monitoring of human actions cannot be misused or abused (e.g. for legal purposes), and that it is not intended to monitor the actions of one particular human operator [6].
- A framework of safety performance indicators should be linked with a system that allows the integration of the different performance indicators into an aggregated indication of the safety performance. From the changes in individual safety performance indicators values, the overall change in safety performance need to be assessed. This means that this system needs to link each SPI to accident probability.

In relation to data collection, integration and analysis in support of safety performance indicators and continuous safety monitoring a number of constraints were identified:

- Data collection, integration and sharing can suffer from showstoppers (e.g. underreporting, lack of data confidentiality, lack of protection, misuse of safety data etc.). A limitation is that presently data is not easily accessible to neither industry nor governments. Data protection measures (e.g. just culture policy, de-identification of data, database security) are essential preconditions to foster a good safety reporting culture across aviation stakeholders. The identification and mitigation of showstoppers for a successful and reliable safety monitoring process need to be considered in the “design” of the CMA.
- A constraint is that the exposure data on aircraft usage, movements at airports etc. becomes available in a timely fashion and its classification is compatible with the ECCAIRS (ICAO ADREP) taxonomy. Exposure data from different sources may be required, which needs to be converted in to an ECCAIRS

compatible format. Exposure data by type of operation for helicopters and data on General Aviation flights is currently not available in Europe.

- Consider that some flight data standardisation initiatives are beginning to emerge among European operators and the regulatory authorities, industry and EASA. The EASA led European Operators Flight Data Monitoring (EOFDM) forum and the UK CAA's FDM forum are two such initiatives which are not only enabling operators to implement FDM and get the most benefit out of such a system but are looking at novel ways of combining collective experience and limited de-identified datasets to better identify safety hazards through FDM.
- Integrating safety data from different sources or different types, requires that the definitions (taxonomy) used for occurrences, events etc. are the same. ASCOS results should be in line with a commonly accepted and used taxonomy such as in ECCAIRS.
- Initial experience shows that the quality of the data (correctness and comprehensiveness) is lacking which influences the accuracy/reliability of the SPIs. To address data quality issues, requirements can be gradually introduced to establish a common taxonomy, data format, etc. at operator level. This will influence the manner data is collected and create greater standardisation with regards to taxonomy and compatibility of commercially available safety reporting/management software with that used by the central repository.

3.3.3 Safety Risk Management

In the development of a safety risk assessment methodology, risk model and tool the following constraints have to be considered:

- Relevant activities are the EUROCONTROL's Integrated Risk Picture (IRP), FAA's Safety Risk Management (SRM) activities and the Dutch Causal Model for Air Transport System (CATS). Instead of starting an independent parallel research project, it would be much more beneficial, appreciated and acceptable by end users to build further upon and to stay in line with the aforementioned activities. Similarly, the work and deliverables from the Future Aviation Safety Team (FAST) and EASA EME1.1 approach should be exploited. Finally, focusing on the safety impact of the operational issues as identified in the European Aviation Safety plan (EASp) ensure that the ASCOS solutions are relevant to stakeholders.
- To really make a difference a risk model or tool should be applicable to different aviation domains, covering the entire lifecycle of a product and address all interfaces and interactions between different aviation system domains.
- The safety risk assessment, including risk models, will depend on availability and quality of safety data for model development and quantification. The data collection, integration and analysis constraints identified in the previous section also extend to domain of safety risk management.

4 Stakeholder analysis and expectations

4.1 Background

In preparation for the Validation Strategy the ASCOS team needs to establish the stakeholders that will be involved in the validation of the ASCOS results. Stakeholders are the organisations that have an interest or a role in the described problem statement and the proposed solutions to overcome the identified shortcomings and to address the challenges in the current and future certification process (see chapter 3). In the ASCOS project a User Group (UG) was established representing different stakeholders in the aviation industry and in the certification domain. Participation of stakeholders and/or aviation experts, with experience of certification and approval processes, in the project validation process is essential to achieve a successful validation.

After the short introduction of the stakeholders in section 4.2, the stakeholder analysis in section 4.3 will identify their expectations, priorities and interests and their relation with the ASCOS results. The stakeholder expectations reflect what the stakeholders expect as intended use and benefits of the end products from the ASCOS project.

4.2 Identification of stakeholders

Table 1 shows the identified stakeholders in the context of the ASCOS project, in particular in the area of certification and continued safety of certified products, organisations, services, operations etc. during their operational life. It is assumed that the composition of the ASCOS User Group (UG) and the individual members can provide appropriate input to the validation and that this input will be representative for the stakeholder group in general.

Basically the stakeholder group can be divided in two parties. On the one hand, a group of stakeholders represent the applicants applying for a certificate at the certifying authority. This group will need to work with the proposed certification approach, methods, and tools to certify their aerospace products, technology, service, concept of operation etc. On the other hand, the certifying authorities have to review the certification activities of the applicants. The certifying authority has to fully understand the methods and tools used by the applicant to be able to assess their correct application, and the validity, accuracy etc. of the certification activities. The certifying authority may provide guidance material and/or acceptable means of compliance on how to demonstrate that the compliance or performance based regulations are met. Appendix D presents a regulator's perspective on the ASCOS results in the context of its role in the certification process.

Table 1: List of stakeholders and User Group Members

Stakeholder Group	ASCOS User Group Member
Regulators, regulatory bodies, authorities*	EASA, FAA, CAA-NL, CAA UK, CAA-Poland (CAO), JARUS, SRC
Policy makers	ICAO
Aviation safety and certification advisory bodies	ESASI, ESSI, FAST
Standardisation organisation	EUROCAE, SAE
Single European Sky ATM R&D	SESAR JU
Airlines	IATA
Organisation for the Safety of Air Navigation	EUROCONTROL
Manufacturers	Dassault, Rockwell Collins
Others	ESA, TUVN
*) Representing rulemaking, certifying, inspection and oversight functions.	

ANSPs, airlines, ground handlers and airport operators are indirectly involved in the User Group through membership of e.g. ESSI, SESAR JU, IATA, and FAST. The ASCOS results could be usable for those organisations as part of certification activities, seeking regulatory approval for changes, continued safety monitoring (safety assurance) and Safety Management. Furthermore, they may be involved in the application of ASCOS solutions or affected by these solutions in the context of the cross domain integration and the total aviation system approach envisaged in ASCOS. It is therefore recommended to ensure that ASCOS intermediate validation results will indeed be transferred to those four stakeholders, with the possibility to also collect their feedback A couple of consortium members and User Group members have experience in the ATM, airline and airport operator domain. They could (partly) represent the respective stakeholder group and contribute to the validation by providing feedback from the perspective of that stakeholder group, see also section 9.2.4.

4.3 Overview of stakeholder expectations

The authors of this document established a complete overview of user expectations, needs, and/or requirements with respect to the ASCOS final results. User expectations have been collected from the ASCOS Public material, the user group meetings, technical meetings with user group members and earlier ASCOS questionnaires. Finally, the UG members were contacted to participate in a questionnaire designed to review the list of expectations and to collect their top-5 of expectations (see Appendix F). The received responses on this questionnaire confirmed the relevance, completeness and correctness of the list of user expectations. The summary of most relevant statements and examples from the questionnaire responses are presented in Appendix G.

The user expectations will form a reference in the validation of the ASCOS results together with the stakeholders to determine if the results are fit for purpose and to evaluate if they bring the expected benefits. Therefore, they were also considered during the development of the performance framework (chapter 7).

When reviewing the stakeholder expectations, needs and requirements the boundary between what belongs to validation and what is part of verification is sometimes ambiguous. In the validation, the ASCOS team really aims to focus on the intended application of the new certification approach and supporting tools, to evaluate whether ASCOS results bring the expected benefits, mitigates current bottlenecks/shortcomings and whether the ASCOS results are fit for purpose. The reviewed minutes of meetings and deliverables such as reference [10] contain required tool functionalities which can be considered as the design specification for the tools and methods. In validation the validity of the requirements are checked but the evaluation whether the delivered tool or method meets these required functionalities is out of scope as it is considered verification. Clearly, there is a relation between the user expectations and the technical specifications as these specifications should result in a product that meets the user expectations.

The following tables summarises the user expectations into four topics. For each topic there is a table with the corresponding expectations:

- New certification approach (Table 2);
- Continuous safety monitoring (Table 3);
- Safety based design and risk assessment (Table 4); and
- Usability and applicability of the proposed ASCOS “products” (Table 5).

The stakeholder expectations are associated with Key Performance Areas (KPAs) of the performance framework defined in chapter 7, see Appendix E.

Table 2: Stakeholder expectations – Proposed ASCOS certification approach.

No	Expectation – Proposed ASCOS certification approach	Ref
1	The ASCOS approach towards certification, including the developed supporting processes and tools, *should offer improvements over the existing certification and approval processes* in the areas 1.1 to 1.9 (below), whilst ensuring that at least a similar, and preferably an improved, level of safety assurance is provided as with the current certification approaches.	[1]
1.1	The ASCOS approach should *lower costs* of all involved processes and activities, both to the applicant and certifying authority.	[1], [13]
1.2	The ASCOS approach should *reduce throughput time* of certification processes. E.g. it will accelerate the certification and introduction into service of novel systems, technologies, and operations for which detailed prescriptive requirements are not available.	[1], [13]
1.3	The ASCOS approach should *ease the introduction* of safety enhancement systems and operations with special characteristics that are not yet or not fully covered in existing Certification Specifications;	[1], [13]
1.3.1	It should *improve the ability to analyse and demonstrate acceptable safety for new concepts and technologies*.	[1]
1.3.2	It should *improve flexibility* in demonstrating compliance to (compliance or performance based) regulations in case of new or changed systems, technologies and/or operations.	[1]
1.4	The ASCOS approach should contribute to and support certification of *integrated systems* and *integration of different domains* in a certification approach, which includes:	[1]
1.4.1	Improve the ability *to analyse and consider the entire aviation system* rather than sub-elements in isolation.	[1]
1.4.2	Enable *better addressing interfaces* between various domains in certification, e.g. ATM functions integrated in aeronautical products, and aeronautical products and flight operations.	[13]
1.4.3	*Reduction of uncertainty* regarding safety accountability, roles and responsibilities, in the complex aviation system with integrated systems, interfaces and interactions.	[1]
1.5	The ASCOS approach should improve the ability to analyse and consider the impact on safety of *all elements of the aviation system* and *the entire system lifecycle* in a complete and integrated way.	[1]
1.6	The ASCOS approach should support certification taking into account *future and emerging risks* so that the certification appropriately takes into account the future developments, changes and scenarios (including the identification and assessment of future and emerging risks).	[1], [16]
1.7	The ASCOS approach should *reduce uncertainties in certification activities*, e.g. uncertainty regarding the feasibility of achieving certification of novel technologies and concepts if no specifications (yet) exist or if the required performance level is not (yet) specified.	[1]
1.8	The ASCOS approach should explicitly consider *human performance* in a consistent and qualitative manner in overall safety assessments.	[1]

1.9	The ASCOS approach should contribute to *safety improvements for the Operational Issues of the European Aviation Safety Plan* (e.g. a reduction of fatal accidents due to: loss of control in flight, aircraft system or component failure or malfunction, aircraft ground handling aircraft damage and Air Traffic Management related incidents/accidents).	[1]

Table 3: Stakeholder expectations – Continuous safety monitoring process and tools.

No	Expectation – Continuous safety monitoring process and tools as part of the proposed ASCOS certification approach	Ref
2	The ASCOS approach towards certification including the developed supporting processes, tools and databases *should offer improvements for continuous safety monitoring* in areas 2.1 to 2.7. Continuous safety monitoring refers to the process for continued airworthiness of aircraft, and maintenance of certificates for air navigation service providers, operators, and manufacturers after they have been certified and while they are being operated / are operating.	[1]
2.1	The ASCOS approach should enhance the process and/or the capability for *providing feedback on assumptions* (e.g. assumptions about the operating environment) made in design and certification safety assessments.	[1], [16]
2.2	The ASCOS approach should enhance the process and/or capability for *identification of new/changed hazards*, and assess associated risks, as part of continued airworthiness.	[1]
2.3	The ASCOS approach should enable the *development and maintenance (updating) of a risk baseline* for continuous safety monitoring (e.g. through a data driven, stable, reproducible EU baseline risk picture from multidisciplinary aviation safety data which can be regularly updated).	[1]
2.4	The ASCOS approach should support the *real time risk monitoring.* The data and the tools used for the real time risk monitoring provide the level of accuracy, reliability, and detail appropriate for the use in certification activities and continued airworthiness.	[1], [20]
2.5	The ASCOS approach for the real time risk monitoring should *facilitate the quantification and semi-continuous updating* of the safety performance of the (total) aviation system at an acceptable level of effort and cost, e.g. of data collection, processing, and analysis.	[1], [19], [20]
2.6	The ASCOS approach should enable the *linking of safety performance indicators to the main Operational Issues of the European Aviation Safety Plan* (e.g. runway excursion, controlled flight into terrain, loss of control in flight).	[1], [16]

Table 4: Stakeholder expectations – Safety risk management and safety based design.

No	Expectation – Safety risk assessment: aviation safety assessment methodology, risk models and tools for risk assessment and safety based design as part of the proposed ASCOS certification approach	Ref
3	The ASCOS approach towards certification including the developed supporting processes, aviation safety assessment methodology, risk models and tools for risk assessment and safety based design risk should *offer improvements* in certification activities.	[1]
3.1	The ASCOS approach *should enable safety based design* of technologies, operations, and systems, which includes:	[1]
3.1.1	An approach for the *setting of safety targets, safety objectives and safety requirements* to be used in design.	[1], [10]
3.1.2	The evaluation of *risk relative to a required safety performance* level.	[1], [10]
3.1.3	The *assessment of the safety impact* of introducing new (safety enhancement) systems, concepts, technologies, and/or operations in the total aviation system in absence of data and deal with the issue of using historical data in that context.	[1], [14], [16]
3.1.4	The *identification of events* that can be considered as new precursors in case the novelty is implemented. Defining the capture process of new precursor and applying it on existing in service events databases to estimate precursor occurrence rate.	[10]
3.2	The ASCOS approach for safety risk assessment, including risk models and tools, should be *adjustable for a new certification question*, while the involved effort and cost are acceptable to the stakeholders.	[10], [15]
3.3	The ASCOS approach for safety risk assessment *should provide a safety picture of the future*, taking into account likely changes, trends as well as the introduction of new products, systems, technologies and operations for which safety regulations may need to be updated.	[1], [10]
3.4	The ASCOS approach for safety risk assessment should enable to *better anticipate on future risks and respond to precursors of future risks and hazards* instead of merely reacting on historic accidents. This aspect supports the continuous safety monitoring.	[10]

Table 5: Stakeholder expectations – Usability and feasibility of proposed ASCOS approach.

No	Expectation - Usability and applicability of the proposed ASCOS certification approach	Ref
4	The ASCOS approach towards certification including the developed supporting processes, tools and guidance material *should receive willingness* of the stakeholders to adopt the new approach and put it into practice.	[1]
4.1	The ASCOS approach should be *user-friendly*, e.g. easy to understand, easy to learn, easy to explain, easy to use.	[1], [13], [14], [15]
4.2	The ASCOS approach should *reduce the required level of expertise and experience*, maintaining an equivalent or better level of safety compared to the current practice.	[13]
4.3	The ASCOS approach should *reduce bureaucracy* both at the applicant and the certifying authority.	[13]
4.4	The ASCOS approach should be *usable for a very wide range of applications* and applicable to the *different certification domains (e.g. aircraft, organisation, ATM, etc.*).	[15]
4.5	The ASCOS approach should enable *involvement of different stakeholders* from early on in the process.	[13]
4.6	The ASCOS approach should *not negatively impact harmonisation* and, preferably, promote harmonisation. It should *contribute to streamlining* processes using industry standards, while keeping differences with current regulations, requirements and practices limited.	[1], [13]
4.7	The ASCOS approach *should be compatible with existing practices, organisation and culture* in aviation industry, for example it should be flexible to accommodate and allow existing practices where appropriate in the ASCOS approach.	[1]

5 Identification of ASCOS proposed solutions and their maturity level

5.1 Introduction

This chapter first summarises the solutions proposed by the ASCOS project to address the problems, challenges and needs identified in the previous chapter. The description of the proposed solutions is at such a level of detail that the benefit mechanisms can be identified for the performance framework (chapter 7). For more details about the proposed solutions the reader is referred to the deliverables of WP1, WP2 and WP3. Secondly, this chapter covers the initial maturity assessment of the ASCOS solutions. The purpose of the maturity assessment is to have a proper understanding of the maturity level of the ASCOS results, which is an indicator of the level of performance, uncertainty, viability, completeness etc. that the validation team could expect when the validation starts. This helps to define appropriate validation objectives and exercises that match the maturity level (see section 5.5).

5.2 The proposed certification approach

5.2.1 Concept description

Today, safety arguments are built in isolation within individual organizations, and integration into a unified safety argument is not considered as essential. Consequently, essential safety critical information such as dependencies, context and other metadata can be lost. This can lead to gaps, overlaps, and unclear definition of responsibilities. The ASCOS proposed concept of certification complements current certification approaches with a standard logical safety argument framework able to encompass the Total Aviation System (TAS). The approach is compatible with existing local approaches in use across different domains. The different stages of the newly proposed certification approach are [4]:

1. Define the change
2. Define the certification argument (architecture)
3. Develop and agree certification plan
4. Specification
5. Design
6. Refinement of argument
7. Implementation
8. Transfer into operation – transition safety assessment
9. Define arrangements for continuous safety monitoring
10. Obtain initial operational certification
11. Ongoing monitoring and maintenance of certification

The ASCOS logical argument framework mandates the development of an integrated safety argument containing the evidence, assumptions, intermediate conclusions and argumentation strategies by which an applicant organization can support the overall top level claim that a proposed change is acceptably safe when considered in the context of the Total Aviation System. Such an argument is supposed to be built during the

initial phases of the system life cycle design and development by the relevant applicant and has to be constantly monitored and upgraded during the ensuing phases of operations and decommissioning.

One distinctive feature of the proposed approach is that the safety impact of the change in question has to be assessed not just with reference to the local domain in which the change occurs, e.g. airport operations, but in the scope of the total aviation system, i.e. airspace planning, aircraft manufacturers, aircraft operators, air navigation service providers, ATM/ANS equipment, and aerodrome. The dependencies and interactions introduced by the specific change will need to be established between the involved organizational actors. To promote the consideration of interdependencies between different domains, the approach is based on a common reference model of the overall TAS, which defines what needs to be done when an individual element is added, replaced or changed. This is intended to clarify not only the potential breakdowns of the system in question but also the impact that the introduction or replacement of the system might have on the rest of the TAS.

As an argument referenced to the TAS can become quite complex, the argument is structured into separate modules so to make it manageable. In particular, modularization clarifies:

- Which module is managed by which organization. In this way, the modularization will reflect the division of responsibility(ies) between the different organizations engaged in the certification process;
- What are the interfaces between modules, and which organization is responsible for managing such interfaces. This will minimize the risk that dependencies between modules will not be considered or tracked.

It should be noted that modularization allows to change specific modules of the overall argument without affecting other modules, as long as the affected module still complies with the interface(s) established with the rest of the argument.

Note that the framework does not intend to replace well established current certification approaches in the different certification domains, but complements them. Each module may take a different certification approach, e.g. performance or compliance based, thus mirroring the approach taken in each domain by the different organizations involved. The ASCOS approach integrates the results of such a local assessment in a way that is shared with and understandable by multiple stakeholders involved in the certification process.

5.2.2 Expected benefits

The expected benefits of the ASCOS approach include:

- Promoting clarity among stakeholders' roles and responsibilities in the certification process. Within ASCOS, the certification of novel concepts will be carried out in a joint goal-oriented way, in which multiple stakeholders will be able to focus on the module they are responsible for without losing sight of the global argument, and of the dependencies established across modules. This is the case because throughout the system life cycle, ASCOS mandates the clear definition of clear areas of responsibilities associated (i) with each module of the safety argument and (ii) with the interfaces existing between

each module. In turn, this is expected to increase the clarity about when and how the various stakeholders will be involved in the approval process throughout system lifecycle, and what their area of responsibility is. As a result, this should reduce the risk of safety gaps or overlaps, conflicting requirements and confused responsibilities.

- Improve the reliability of the top-level argument that the system is acceptably safe. The use of the logical argument framework referenced to the TAS will make sure that assumptions and safety evidence depending on other domains, are appropriately documented, and considered when demonstrating that the change in question is acceptably safe. This represents an important benefit area as today's changes are certified in the context of the single domain the change belongs to, irrespectively of the impact on other domains of the Total Aviation System. Further, the approach should ensure that such dependencies are appropriately tracked throughout the life cycle of the systems involved.
- Flexibility. The logical framework approach is flexible enough to accommodate certification practices existing on different industries.

5.2.3 Roles

The use of ASCOS logical argument framework is expected to rely on the following roles:

- Applicant representative, or team of applicant representatives. These belong to the organization which is seeking approval for a given change;
- Safety Argument Architect. Working for the applicant organization, this role develops and maintains the module of the certification safety arguments he/she is responsible for, and ensures appropriate coordination with the safety architects of other organizations and domains;
- Certification authority representative or team of certification authority representative. This actor will inspect the certification safety argument to assess whether the proposed change is to be approved or rejected.

5.2.4 Enablers

The ASCOS certification adaptation does not depends on a specific enabling technology beyond those required for basic office automation. The ASCOS approach requires knowledge about the safety case development, in particular the concept of developing a safety argument with a claim and evidence based structure. Experience with the use of Goal Structuring Notation (GSN) is beneficial. Although this approach is well documented by Eurocontrol (e.g. in SAME [24], and [25]), there will likely be organisations outside the ATM (certification) domain that are not familiar with this approach.

5.2.5 Limitations

The worldwide acceptability of the logical argument approach depends on the acceptance of the approach by local stakeholders, especially those that are not familiar with safety case development and management practices. Also, the traceability with current recommended practices (e.g. EUROCAE standards and SAE

Aeronautical Recommended Practices) will need specific attention, because ASCOS D1.3 suggests that safety arguments need to be developed until the level of detail on which existing standards can be used.

5.3 Safety performance monitoring process and tools

5.3.1 Concept description

The ASCOS continuous safety monitoring process mandates the monitoring and control of 63 Safety Performance Indicators (SPI) grouped at four levels (Technology, Human, Organisation, System of Organizations) and referring to different stakeholders of the Total Aviation System. Variations of SPIs over time can be monitored by either the applicant or the certification authority following the introduction of a certified change into operation. This would be part of the Safety Assurance pillar in a Safety Management System of an organisation. The process is supported by a tool that allows the calculation of SPIs as a rate per flight, based on queries to an ECCAIRS 5 compatible database containing occurrences and exposure data (e.g. number of flights or flight hours) to normalise the results. The tool supports the monitoring of SPIs through an interface that enables:

- Setting Target Levels of SPIs for the current period;
- Setting thresholds and related alerts, so that appropriate safety activities can be initiated when these threshold values are exceeded;
- Performing comparative analysis: the tool support the juxtaposition of trend lines, so that the safety analyst can for example perform a benchmark with the industry trends or can evaluate how a given SPI evolves after the introduction of a new product compared to the performance assumed during certification. For instance flight data can be used to monitor flight operations and flight crew behaviour for comparison with operational performances assumed during certification.

The SPI framework is described in D2.1 [6], while the continuous safety monitoring process is explained in D2.3 [9]. Since the SPI definitions may be subject to reconsiderations and alterations the tool supports the modification and reconfiguration of SPIs (see D3.1 [7]).

5.3.2 Integration with the proposed ASCOS certification approach

The process and tools for multi-stakeholder Continuous Safety Monitoring, using a baseline risk picture for the Total Aviation System (i.e. including all domains and their interactions), support a posteriori risk assessment by establishing the framework for collecting data. As reference [4] explains “the process and tools initially focus on supporting the stages 8, 9 and 10 of the certification approach, as part of the ‘a posteriori risk assessment’”. As part of this process, Safety Performance Indicators (SPIs) were specified to monitor the safety in service in D2.1 [6].

5.3.3 Expected benefits

The ASCOS continuous safety monitoring concept should enable all stakeholders to monitor continuously the performance of an approved change, and intervene whenever a particular SPI or a set of SPIs deviates from an

expected target level of performance. Note that in this context a change could involve the introduction of a novel technology, system, operation, etc.

The concept may provide feedback to applicant and certifying authorities about the safety performance in practice compared to the performance assumed during certification.

5.3.4 Roles

The intended user of the ASCOS tool for safety monitoring is a safety specialist interested in carrying out trend analysis for one SPI or a set of SPIs. This user can work for different types of organizations, i.e. manufacturers, airline, ANSPs, EASA, etc. Specific to the certification context, this user can generate retrospective trend analysis that can serve for informing the certification safety argument.

5.3.5 Enablers

The ASCOS tool for continuous safety monitoring has both technical and political enablers. The technical enablers include:

- The framework of SPIs and proposed set of ASCOS SPIs require stakeholder acceptation, followed by dedicated occurrence and exposure data collection campaign to continuously quantify and update the set of SPIs. Each proposed safety performance indicator should be unambiguously connected with one or more events of the ECCAIRS taxonomy and a suitable denominator from EASA's warehouse for aviation production data. This requires participation of the stakeholders, using different means to collect data such as voluntary and mandatory reporting schemes, and requires resources to collect and process data.
- The current version of the tool for continuous safety monitoring requires a PC running Windows 2008. The organisation using the tool should have access to occurrence and exposure data in ECCAIRS compatible format (currently ECCARIS 5).

A political enabler is:

- The ASCOS tool for continuous safety monitoring is developed to be compatible with the ECCAIRS database. Consequently, the main enabler to the use of this tool in combination with the database is the existence of political arrangements to ensure that the member states will feed periodically the database with updated and reliable performance data. Today, many data are not shared or not stored in the database due to the lack of a common accepted regulatory framework that makes the reporting of data to ECCAIRS mandatory for members states. The development of such a framework requires political actions that are outside the scope of ASCOS. For the purpose of the validation, it is assumed that such arrangements are in place.

5.3.6 Limitations

The lack of the political enabler described in the previous section implies that the ASCOS tool for continuous safety monitoring lacks at the moment occurrence and exposure data for many of the ASCOS defined SPIs.

Flight data provide an excellent source for monitoring flight operations, system performance and flight crew behaviour. It provides feedback on the assumptions made in certification and helps to identify new/changed hazards and assess associated risks. The most flexible and effective approach to use flight data in support of continuous safety monitoring is to collect raw time trace flight data, however this requires significant resources to manage, see D2.3 [9]. However, the ASCOS Continuous Safety Monitoring methods and tools mainly build on the ECCAIRS software, and the usage of occurrence and incident/accident data. It appears difficult with ECCAIRS – if not impossible – to do any kind of flight data processing on operational data recorded on the aircraft for identification of event exceedances and routine events.

In the context of ASCOS WP5, it is expected that the validation exercises will make use of simulated data.

5.4 Safety risk assessment methodology, risk model and tool

5.4.1 Concept description

The ASCOS risk assessment methodology, risk model and software tool for risk assessment are intended to assist both the applicant and the certification authority to assess how a planned change will impact on existing safety risk levels. The methodology and tool are intended to assist the applicant in the first phases of the certification process, i.e. when the change is being planned and assessed and has not yet affected operations. The methodology enables the identification and assessment of emerging and future risks. The tool supports the development of a safety picture of the future, taking into account likely changes, trends as well as the introduction of new products, systems, technologies and operations. ASCOS provides an integrated approach to risk modelling in which human factors are considered in connection with technical and procedural aspects and with specific emphasis on the representation of emerging and future risks. The development of the risk model is described in D3.2 [8], the functionalities of the software tool are defined in [10], and the user manual of tool is D3.3 [29].

The ASCOS tool for risk assessment consists of a risk model, i.e. a repository of accident and accident avoidance scenarios [8]. Each scenario is formed by events that can be described as hazards that may lead to accidents and/or serious incidents. The scenario also contains events that can be regarded as safety barriers or pivotal events to prevent the accident or serious incident outcome. The ASCOS model uses Event Sequence Diagrams (ESDs) in combination with Fault Trees (FTs) to represent the scenarios, i.e. the occurrence of hazards and failure of safety barriers. An ESD starts with an initiating event, followed by a number of pivotal events that lead to different outcomes or end states. The FTs are used to represent the root causes of both the

initiating and the pivotal events of an ESD. Each fault tree contains events that are stated as faults and are combined by logic gates. In ASCOS, the quantification of the accident scenarios is done by assigning probabilities to the initiating events of each ESD and to the conditional probabilities of the pivotal events. The initiating and pivotal events have associated Fault Trees. The probability of the initiating or pivotal event in the ESD is equal to the probability of the top event of the associated Fault Tree, which in turn is calculated by calculating the probabilities of the FT base events through the logic gates bottom-up. The probability of the base events is determined by using a combination of historical air safety data, by other quantified events (e.g. precursors) and by expert opinion.

The risk model is suitable to support the initial phases of certification, when the specification and design of the product or service is still at a high level. When using the model one should consider that the model, including the quantification, represents a global risk picture (baseline). It is expected that the application of the model in the certification activities requires adaptation of the model structure and data in relevant areas so as to ensure that it represents the subject of certification correctly. The adaptations of the model structure and data will mainly be made in the Fault Trees.

The tool can be used top-down, it is possible to set up high level safety objectives (in relation to the end-states elements); the tool enables safety experts to modify probabilities of elements/events for safety based design purposes (note that the allocation is under the responsibility of the safety practitioner, the tool is just a tool). It supports understanding of the impact of specific stakeholders on certain element/events. This functionality enables the safety practitioner to estimate the impact that a novelty can cause, in terms of improvement, for specific stakeholders. It is possible to quantify the safety impact of a barrier after/before a certain change.

5.4.2 Integration with proposed ASCOS certification approach

As reference [4] explains “the WP3 methods and tools initially focus on supporting the stages 4, 5 and 6 of the certification approach, as part of the ‘a priori risk assessment’ before implementation of the change.” The developed risk model and tool (D3.2 [8], D3.3 [29]) can be applied in particular in step 4 and 5 of the proposed certification approach (D1.3 [4]). These steps include: 4) A safety assessment to identify pre-existing hazards to the system (design) and assesses the consequences of these hazards on the safety of the TAS; and 5) A safety assessment to consider what the elements of the logical design need to do to ensure safety and the degree of assurance required [4].

The risk model can support and enhance safety management in various ways. Report D3.2 [8] describes for instance the use of the risk model to improve the Continuous Oversight function, the Management of Change, and the use to determine the appropriate level of oversight.

5.4.3 Expected benefits

The tool brings two main benefits:

- Assessing and documenting the magnitude of the safety impact of a change on the total aviation system. The tool can be used to assess how a given change would affect the Total Aviation System. In

particular, during the analysis of a change, the analyst can change the failure rate for a selected event or a group of events in the Fault Trees stored in the tool. Based on the adapted values, the tool will update the failure rates of the events and outcomes. In turn this makes the applicant more aware of the areas that will be affected by a change.

- Facilitating the sharing of relevant safety information between the applicant and the certificatory authority. Once the applicant has loaded its data into the model, the results can be easily shared with the certification authority. At this stage the certification authority can even decide to delegate the download and check of the data to a third party.

5.4.4 Roles

During the certification process, the safety assessment methodology, risk model and tool are intended to be used by the safety specialist for conducting the safety risk assessment of the proposed change. The outcome of the exercises consists of identified hazards, risk levels, mitigation actions (i.e. safety barriers) that will be passed to the safety architect for building the certification safety argument.

5.4.5 Enablers

A technical enabler is a computer with the tool and database to feed the probabilities to the events in the accident scenarios. An organisational enabler is the acceptance of the tool, in particular the accident scenarios, the quantification of events and the interdependencies of events, the development and maintenance of the database of probabilities to quantify the model elements.

5.4.6 Limitations

The current version of the ASCOS risk model (described in D3.2) and the associated ASCOS risk tool (described in D3.3) have certain characteristics that limit their application:

- On purpose, the scope of the ASCOS model is broad (all types of accidents in the total aviation system are covered) and the level of detail is such that it will be possible to prioritize safety actions and enable safety based design. Note that differentiation between aircraft types is intentionally not made, as the scope is restricted to commercial air transport with large aircraft (i.e. CS-23 will have to apply).
- The effect of secondary processes on the level of safety of the flight operation, such as maintenance, aircraft servicing, air navigation services, is modelled in less detail than the flight operation. This limitation can be overcome, if user of the risk tool (presumably safety experts) develops this model.
- The model describes the effects of “active” failures on safety and effects of “latent” failures are modelled less explicitly.
- The identification and analysis of common mode failures is difficult. When a single failure impacts several ESDs, it is not possible to analyse these ESDs at the same time. This issue has been partially solved by a “practical approach” enabling safety practitioner to search by the use of keywords,

- The influence of managerial/organisational processes and the effect of safety culture on safety are not directly and explicitly represented in the model. ASCOS D3.2 shows that this is in fact not feasible.
- The influence of human factors is taken into account in a limited extent. Whereas various types of (technical) failures are included in the model, their causal factors are not specified in detail.
- The logic of the Event Sequence Diagrams in combination with Fault Trees is "black or white". In the Fault Tree modelling such a "binary" logic is not always an appropriate representation of reality.
- The quantification is partly based on expert judgement with incomplete validation (e.g. no double-checking). This is an issue that mainly effects the quantification of Fault Trees.

In addition, the developed tool (D3.3 [29]) has characteristics that are partly related to the risk model. On purpose, the ASCOS risk assessment tool does not automatically identify hazardous events (i.e. failures, errors and procedure deviations) that may be included in the current set of fault trees. If hazards are not already included and quantified in the risk model, they have to be included by the safety analyst. These hazards need to be put into the tool based on the outcome of a safety assessment, e.g. from a functional safety assessment or structural safety analysis. In other words, such hazards are "external" to the risk assessment tool. Therefore, the accuracy of the risk levels produced by the tool depends amongst others on the quality of the hazard identification and quantification, the methodologies and data used, and the expert judgment of the involved safety experts.

5.5 Maturity assessment of ASCOS proposed solutions

This section determines the maturity level of the ASCOS results. The purpose of determining the maturity level of the ASCOS results is to ensure that the validation plan is compatible with the ASCOS results' maturity level. The omission to assess the maturity level of a concept is known to result in the planning of inappropriate validation activities, especially in case the maturity level is lower than assumed [22]. The E-OCVM proposes a framework for maturity assessment that determines the maturity level of a concept by comparison with a reference Concept Lifecycle Model. This model consists of six phases, which cover the development of a new concept to implementation. As E-OCVM is intended for the validation of novel concepts only, the reference phases to be considered for the maturity assessment are the V0 to V3 levels (see Table 6).

The ASCOS results are not related to the typical operational concept (e.g. an automated system for air traffic controllers) and the associated staged development or life cycle. The operational concept could be interpreted in the context of the ASCOS project as "the new ASCOS certification approach, including continuous safety monitoring and risk assessment tools". The maturity levels and objectives from the E-OCVM could be applied to the ASCOS results as parallels can be observed between the ASCOS activities, their results and the E-OCVM V0 to V3 objectives.

Table 6: Maturity Level and R&D Phase according to E-OCVM [22].

Maturity Level	Phase of Concept Lifecycle Model	Objective
V0	Identification of Needs	Establish and quantify the need for change.
V1	Scope	Initial operational concept description
V2	Feasibility	Develop and Explore Concept. Demonstrate fitness for purpose of individual concepts.
V3	Pre-Industrial Development and Integration	Refine operational concept. Demonstrate fitness for purpose of concept when working together.

When mapping the ASCOS results against the E-OCVM maturity levels V0-V3 it can be observed that:

- Previous work conducted in the ASCOS project has addressed the need for change in current certification practices based on a description of the shortcomings and bottlenecks of current certification practices, see D1.1 [3]. This material provides an initial understanding of the needs and opportunities for improving current certification practices. However, it must be noted that a performance framework has not been defined in the previous phases of the project. Therefore, this will developed as part of the validation strategy to be able to plan the validation activities.
- Regarding the E-OCVM phase V1 objective, an initial description of the ASCOS products and how they deliver the intended benefit has been provided in various ASCOS deliverables, for example D1.2 [13], D1.3 [4], D2.1 [6], D2.3 [9], D3.1 [7], and D3.2 [8]. However, it must be noted that the link between the expected benefits and the relevant problems and needs identified in V0 is difficult to demonstrate explicitly due the lack of a performance framework.
- Regarding the E-OCVM objective for phase V2, the ASCOS project needs to further specify and refine the description of the proposed approach, process and supporting tools. In particular, the stakeholders and personnel involvement needs to be addressed in more detail, e.g. the roles involved in certification of a new aviation product, responsibilities and tasks, together with any changes of procedures, team structure, communication and coordination between certification domains and organisations. This level of description is usually best covered by diagrams such as a use cases.
- Comparing the ASCOS project against maturity level V3 objectives, it is noted that no evaluation exercise has been initiated yet to collect the evidence that the proposed ASCOS concept will be operationally feasible when integrated into ongoing operations.

In conclusion, the level of maturity of the ASCOS products seems to correspond to the E-OCVM levels V1 and V2. This makes sense since ASCOS is a R&D project that aims to explore preliminary concepts of a novel certification and continued airworthiness approach with an initial evaluation of their feasibility and acceptability. More mature concepts and tools are addressed by development and implementation projects.

The maturity level of the ASCOS solutions has an impact on the validation objectives and exercises, i.e. they should be appropriate to the level of maturity. In principle the objective of the validation is to evaluate whether the ASCOS solutions are fit-for-purpose and bring the expected benefits. One has to consider the

development stage (lifecycle phase) of the solutions that are being validated. The level of maturity of the ASCOS solutions ("prototype", "feasibility") is such that one cannot expect that they will bring at this stage the full benefits and meet all user expectations. It is therefore important to keep in mind that the aim of the validation should be to evaluate the fitness for purpose and the expected benefits in order to collect data, user feedback and recommendations for further concept exploration and refinement. This will support further development of the ASCOS solutions toward higher maturity levels. The current validation will not yet be about demonstrating or proving that all ASCOS solutions work well in practice, fully meet user expectations and bring benefits.

In this context, the maturity level of the ASCOS solutions calls for a qualitative evaluation rather than a formal or quantitative validation that aims to prove that the ASCOS solutions are fit-for-purpose by mean of a quantitative, comparative evaluation. The latter would be typically done at higher maturity levels. The qualitative evaluation will addresses the potential and the feasibility in relevant KPAs of the ASCOS solutions, underlying concepts, methods and prototype tools. The validation exercises will be used not only to collect feedback about the "look and feel" of the solutions, but will also serve as a basis for stimulating respondent thinking about the actual benefits and role that the solution can play in a real-life certification process. Notably, this is normally done by using focus group, heuristic or expert evaluation, in-depth interviewing, and qualitative questionnaires. This approach may include an evaluation of the ASCOS products against a set of criteria that the stakeholders consider as important. Such feedback can be collected in the form of subjective ratings.

6 Validation scope and objectives

6.1 Validation scope

The objective of the ASCOS WP5 "Validation" is to validate the main results or "products" of WP1, 2 and 3. In particular the validation activities will focus on:

- The new certification approach developed in WP1 and defined in D1.3 [4];
- The Continuous Safety Monitoring process described in D2.3 [9] and the supporting tool (D2.4) developed in WP2; and
- The safety risk assessment methodology, risk model (D3.2 [8]) and tool (D3.3 [29]) developed by WP3.

The validation of the new certification approach adaptations (D1.3) can be considered as concept validation. Validation results will provide feedback about the extent to which this new approach is fit for purpose and will be used to refine and consolidate the certification approach. Validation of the process and tools for Continuous Safety Monitoring (from WP2) and the supporting safety based design systems and tools (from WP3) can be considered as "system" validation during which the suitability of the tools will be evaluated.

Applying the definition of "validation" (refer to section 2.1.1) to the ASCOS validation scope and the ASCOS results, the validation strategy aims to answer the three questions:

- Are we building the right certification approach?
- Are we building the right process and tool for safety monitoring?
- Are we building the right methodology, risk model and tool for safety risk management and safety based design?

The definition of what is considered 'right' is presented in the form of the performance framework, i.e. the set of KPAs and KPIs derived from the current challenges and user expectations.

6.2 Validation objectives

The validation objectives describe the main issues to evaluate during the validation exercises. The high level validation objectives should reflect the stakeholder needs, their expectations of the project and project objectives. From the use expectations the following four validation objectives were formulated.

1. Validate that the ASCOS approach towards certification, including the developed supporting processes and tools, offers improvement over the existing certification and approval processes.
2. Validate that the ASCOS approach towards certification including the developed supporting processes, tools and databases offers improvement for continuous safety monitoring.
3. Validate that the ASCOS approach towards certification including the developed supporting processes, aviation safety assessment methodology, risk models and tools for risk assessment and safety based design risk offers improvement in certification activities.

4. Validate that the ASCOS approach towards certification including the developed supporting processes, tools and guidance material is acceptable to the stakeholders to adopt the new approach and put it into practice.

These validation objectives contain the statement “offer improvement”. The performance framework presented in the next chapter will explain the Key Performance Areas (KPA) that will be considered within the scope of the ASCOS validation. The validation of the “offer improvement” relates to the level of improvement that ASCOS will bring in those KPAs. In other words, the validation objectives concern the assessment of the impact of the ASCOS results on the defined KPAs.

7 The performance framework for validating ASCOS results

7.1 Background

The result of the ASCOS project is a set of solutions, including a proposed certification approach, processes and tools for continuous safety monitoring and safety risk management, that will be validated against a performance framework. The performance framework defines the structure of the Key Performance Areas (KPAs) and associated Key Performance Indicators (KPIs). The "fitness" for purpose, performance and benefits of the ASCOS results will be assessed for the relevant KPAs. The challenges in the current certification practice, continuous safety monitoring and safety risk management (chapter 3) and the user expectations (chapter 4) contributed to the identification of KPAs and KPIs. In chapter 3 and Appendix E the relation between on the one hand the challenges and user expectations, and on the other hand the defined KPAs is indicated. Section 7.2 first introduces definitions related to the performance framework, followed by section 7.3 that addresses the considerations in the development of the performance framework. The KPAs are defined in section 7.4, while section 7.5 presents the KPIs and metrics.

7.2 Definitions

7.2.1 Definition of Performance Framework

A performance framework provides the context to assess the performance of an object relevant to some stakeholders against to some desired level of performance. Such an object can be, for instance, a software or a hardware product, a service, a project, an organizational business process. The performance of such an object can be assessed on a one-off basis, such as in the case of the evaluation of a product delivered at the end of a project, or it can be the subject to constant monitoring, such as in the case of internal business processes.

In the ATM domain, a performance framework has been proposed by ICAO and SESAR to monitor and drive the modernization of the overall ATM system. In fact, the specification of a performance framework captures the desired performance results (i.e. what is the outcome that the relevant ATM stakeholders expected to achieve) which are desirable in order to improve current practices. A performance framework is helpful to understand "how a benefit is produced and delivered and for the examination of performance trade off" [22, 23].

In a validation context, it is important that a performance framework is developed during the formulation of the validation strategy, so to make sure that relevant areas of improvement for the system being considered are taken into account during the planning and the conduit of the validation exercises [22, 23].

In the context of the ASCOS validation, the focus is on the definition of a performance framework relevant for the main ASCOS results, i.e. the proposed approach and process of certification and continued safety performance monitoring of new aeronautical products, operations, concepts in different domains and secondly, the supporting (risk) models and delivered software tools. This ASCOS performance framework is needed to evaluate whether or not and to which extent the proposed ASCOS results deliver their intended benefit and to which degree they can contribute to improve existing certification practices.

Basic components of a performance framework include Key Performance Areas (KPAs), Key Performance Indicators (KPIs), and metrics. These terms are explained below in the next sections.

7.2.2 Definition of Key Performance Area (KPA)

Key Performance Areas (KPAs) are broad subjects or areas of performance that reflect high-level ambitions and expectations of stakeholders groups, such a certification authorities, ANSPs, manufacturers, etc. For instance, ICAO has defined the eleven KPAs relevant to monitor the performances of the ATM system: Safety, security, environmental impact, cost effectiveness, capacity, flight efficiency, flexibility, predictability, access and equity, participation and collaboration, interoperability [26]. The KPAs for ASCOS will be defined in section 7.4.

7.2.3 Definition of Key Performance Indicator (KPI)

Key performance indicators (KPI) are indicators of performance. They indicate what aspect of the object under analysis has to be measured. The definition and measurement of KPIs is essential to understand how well the object under analysis performs or works, in particular how much its current behaviour compares with the expected performance or with the performance of an alternative comparable object. This view of what a KPI consists of is reflected in the ICAO definition of KPI: “The performance indicators are a tool for quantitatively measuring past, current and expected future performance (estimated as part of forecasting and performance modelling), as well as the degree to which performance objectives are being and should be met.” [26].

A similar definition can be found in the E-OCVM [22]: “Key performance indicators measure performance in key performance areas and are identified once key performance areas are known. A key performance indicator is a measure of some aspect of a concept or concept element, for example the total number of runway incursions per year”. This definition provides an example of a KPI taken from the ATM system. It should be noted that the definition of the KPI depends on the domain relevant for the activity in question. Within SESAR, for instance, specific efforts have been taken in order to define ATM specific KPIs [22].

In the ASCOS performance framework, the KPIs will be used to measure the “fitness for purpose” of the ASCOS results in a specific performance area. The KPIs and metrics for ASCOS will be defined in section 7.5. Multiple indicators may be related to a single KPA. It must be noted that KPIs specific to certification processes and activities have not been found in the literature. Consequently specific KPIs needs to be developed in the context of ASCOS. To be relevant for the ASCOS validation, the indicators should be developed keeping in mind specific performance objectives. In this way they can correctly “reflect the intention of the associate performance objectives” [26]. The definition of the KPI needs to consider the limitations and constraints in the validation exercises. For instance, during the validation exercise related the evaluation of a novel automated tool, some KPI might be measurable (e.g. cognitive workload by mean of the NASA TLX method) but other KPIs might not be measurable due to for example cost related to installing the required data collection infrastructure.

7.2.4 Definition of metric

According to the E-OCVM definition a metric is an agreed parameter by which a (key performance) indicator is measured [22]. Examples of a metric are “minutes”, “decibels”, “centigrade”. In general different means are available to measure the KPIs, such as objective measurements, observations, interviews, questionnaires, simulation data.

7.3 Considerations in the development of the ASCOS Performance Framework

The following issues have been considered in the development of an ASCOS performance framework.

- The defined performance framework needs to be scoped around ASCOS and focus on the most relevant (possible) improvement areas. The KPAs should reflect those performance areas that ASCOS aims to improve and represent issues that are important to stakeholders. Obviously, ASCOS cannot improve all aspects of certification or continued safety monitoring or remove all current shortcomings or bottlenecks since the scope, resources and time are limited.
- Some aspects which are relevant to stakeholders involved in the certification process are clearly out of the scope of ASCOS. For instance, ASCOS does not deal with the development process of regulations or with the development of standards and requirements. The processes required to deliver these outcomes is very different from the process of certifying a novel concept. However, it might be reasonable to expect that ASCOS could ease the way in which regulations and requirements are considered in the certification process. For instance, it could make clear which regulation, requirement and standard are relevant to which module of the safety case. Alternatively, it could build into the process more objectivity in the way acceptable means of compliance are defined.
- The validation exercise will not be able to make use of a baseline certification process or case for validation of the ASCOS results. Ideally, one would apply the current practice (process and tools) and ASCOS proposed approach, process and tools to the same certification (test) case and compare the end results of both approaches in the different KPAs. Given that such a (historic) baseline certification case is proprietary information of the applicant, and given the resources and time constraints in this project, such a baseline could not be made available or developed in this project. As a result, the validation will depend on the subjective rating and feedback from the participants such as user group members participating in the validation exercises.
- The selection of the final list of KPAs and KPIs needs to consider the project constraints. For practical reasons, the framework should have a limited set of KPAs and KPIs to keep them manageable during the evaluation exercises. The intended users of ASCOS results include certification experts and safety practitioners. Accessing these experts has a cost as they are geographically dispersed and work for different organizations. Consequently, participants’ subjective rating and feedback might be the main type of data that can be collected in the scope of ASCOS and this should be considered in the definition of the KPIs and metrics.

- The metrics (measurements) for KPIs are based mostly on respondents' subjective ratings. In case of the ASCOS KPIs it may be challenging to define metrics because KPIs are in many cases difficult to objectively measure. Therefore, a metric is interpreted in this stage as the way in which the KPIs will be measured. The specific metric or unit of measure for each KPI will be defined when the validation exercises, the questionnaire(s) and rating scale(s) are being developed as part of WP5.2 activities. The rating can be quantitative (e.g. 1 to 5) or qualitative (e.g. a 5-point scale from excellent to poor). A subjective rating on a qualitative or quantitative scale by the participant in the validation exercises should be provided with a rationale explaining the reasoning to come the particular score. In addition, the participant needs to explain what improvements or changes to the ASCOS results are required in his opinion to receive a higher (or top) rating.
- The current set of KPIs may be too abstract or not self-explanatory (enough) for the participant in the validation exercise. Therefore, the background and experience of the participants in the validation needs to be taken into account during the development of the questionnaire and rating scale for each KPA-KPI to make the questionnaire/rating scale understandable and unambiguous.
- It is expected that the performance framework will be adapted during the development of the validation exercises and questionnaire. Although the KPAs are expected to be "stable", the KPIs and metrics may need to be revised later when more information on the actual form and content of the validation exercises will be available. In the ASCOS performance framework, two types of KPIs are expected to be considered: a) Process oriented KPIs: these KPIs relate to the process of certification and continued safety monitoring, and b) Product oriented KPI: these KPIs relate to the outcome of ASCOS certification process. The outcome will be a certified system, product, concept, operation etc., or continued safety during the operational life of the system, product, etc. The safety argument and supporting evidence is an output for instance of the certification process.
- In the KPA and KPI definitions the term "certification process" encompasses the 11 stages of the "Logical Argument Approach to Aviation Certification" (see D1.3 [4]): 1. Define the change; 2. Define the certification argument (architecture); 3. Develop and agree certification plan; 4. Specification; 5. Design; 6. Refinement of argument; 7. Implementation; 8. Transfer into operation – transition safety assessment; 9. Define arrangements for continuous safety monitoring; 10. Obtain initial operational certification; 11. Ongoing monitoring and maintenance of certification. The certification process includes the continuous safety monitoring process or continued airworthiness.
- The term "proposed certification approach" in the following text refers to the "Logical Argument Approach to Aviation Certification" defined in D1.3 [4].
- All KPAs are assumed to have the condition "while still ensuring acceptable level of safety".
- The user expectations (chapter 4) were mapped with the KPAs, see Appendix E. In addition, D1.2 [13] evaluated different options for improvement of the certification practice against a set of 15 evaluation criteria. The criteria represent issues that are considered relevant for a certification approach regarding the potential benefits and drawbacks of the different options. These criteria were also mapped with the KPAs to ensure that the KPAs cover these relevant issues.

7.4 ASCOS Key Performance Areas

Table 7 presents the definition of the seven Key Performance Areas (KPAs) defined for the ASCOS validation. Section 7.5 presents the KPIs and metrics for the validation of the three main ASCOS products.

Table 7: Definition of Key Performance Areas for ASCOS.

No	KPA	KPA Definition and characteristics
1	**Soundness of the Certification Safety Assurance Documentation**	Within ASCOS, soundness can be seen as the extent to which the evidence, assumptions and data contained in the certification safety assurance documentation establish the conclusion that the proposed change is acceptably safe in the context of the Total Aviation System. In other words, soundness refers to the extent to which the top-level certification claim that the change is acceptably safe follows logically from true premises. These premises in ASCOS consist of evidence, data, and assumed contexts of operations derived from safety assessments that consider the total aviation system and not solely the context of the primary domain of certification. These components of the certification safety assurance documentation can be assessed in term of standards such as reliability, accuracy, realism, consistency, consideration of future or emerging risks, completeness and adequacy.
2	**Efficiency of the Certification Process**	The efficiency of the certification process so that it demands minimal effort, appropriate resource utilisation, time, expertise, experience etc. The process starts the moment a change is designed, through to the point at which a decision about the acceptable safety of the product or service to be certified is made by the relevant certification authority, and subsequently continues with the continued airworthiness or continuous safety performance monitoring.
3	**Cross domain integration**	The degree to which coordination, cooperation, and exchange of information between stakeholders and across (certification) domains is promoted. This applies to the entire lifecycle, starting from the early design phase of a change, through implementation, transition into service and the continuous safety monitoring process. The clarity of roles, responsibilities, and accountabilities across stakeholders in different domains are part of this KPA. This KPA includes also the compatibility with local approaches in use in each domain.
4	**Harmonization**	The degree to which the proposed certification processes, methods and tools promote harmonisation and can be harmonised across stakeholders and (certification) domains. It refers to the uniformity in the use of the same processes, methods and tools across stakeholders and domains to demonstrate that a change is acceptably safe and remains so during its entire lifecycle.
5	**Accommodation of Innovation**	The degree to which innovative products and services can be accommodated by the proposed certification processes, methods and tools, leading towards certification and continuous safety monitoring in an effective and timely manner.
6	**Operability of ASCOS processes and tools**	This KPA refers to the degree to which the processes, methods and tools are designed around the limitations and capabilities of the end user (based on the E-OCVM definition of system operability). According to reference [30], operability can be broken down into three sub items: 1) End user acceptability, i.e. the end user's willingness to implement and use the results. The operability is also determined by the compatibility of the ASCOS products with existing practices, culture and organisations. 2) Usability, i.e. ease of use, ease of learning, etc. 3) Usefulness for stakeholder in achieving his goals.

7	**Flexibility**	This KPA concerns three characteristics: 1) Applicability of the processes, methods and tools to a range of products and services varying in "size" and "complexity" (i.e. scalability). 2) Applicability of the processes, methods and tools to the products and services of different (certification) domains, of different stakeholders and to the Total Aviation System. 3) Applicability of the processes, methods and tools to both novel and derivative products and services.

7.5 ASCOS Key Performance Indicators and metrics

The following three tables present the Key Performance Indicators (KPIs) and metrics for the KPAs, specified for the three main ASCOS products that are going to be validated.

7.5.1 KPIs for the proposed certification approach (WP1 result)

Table 8 shows the Key Performance Indicators (KPIs) for the validation of the ASCOS WP1 results: the ASCOS "Logical Argument Approach to Aviation Certification" or "proposed certification approach".

Important notes:

- The KPIs in this table are not the actual items to be asked directly to respondents during the validation exercises. Rather, these KPIs will be translated into a validation questionnaire, which will be designed in WP5.2.
- Related to 1.1: The degree to which the documentation accounts also for the hazards of the TAS domains impacted by the concerned change (other than those hazards from the primary domain of certification). TAS level hazards are important to consider as today each domain carries out its assessment in isolation from other approaches, without a consideration of the TAS.
- Related to 1.4: Often individual elements may have a good individual safety argument, but these are dependent on assumptions the safety case makes about the environment in which the element is used, i.e. about the rest of the TAS (see D1.2 [13]). The more complete the description of the context in which the safety argument is made, the more reliable the argument is considered to be.

Table 8: Definition of KPIs for ASCOS proposed certification approach.

KPA	KPI	Metric
1. Soundness of the Certification Safety Assurance Documentation	1.1 Degree to which the proposed certification approach is able to consider TAS hazards in the certification safety assurance documentation. This includes the capability of proposed certification approach to improve the consideration of cross domain hazards (hazards from other domains than the primary domain of interest), to improve the consideration of the associated evidence and design assumptions.	Respondent subjective rating.

	1.2 Degree to which the proposed certification approach is able to improve the consideration of human factors related hazards in the safety assurance documentation. This includes the capability of the proposed certification approach to address human factors issues in a consistent manner, to establish safety requirements to mitigate human factors related hazards, to improve the consideration of the associated evidence and design assumptions.	Respondent subjective rating.
	1.3 Degree to which the proposed certification approach is able to improve the consideration of hazards from all phases of the lifecycle (including transition into operation) in the safety assurance documentation.	Respondent subjective rating.
	1.4 Degree to which the proposed certification approach enables the continuous consideration and improvement of the feedback mechanism to stakeholders about the context, conditions, in-service performance and assumptions made in the design, safety assessments or the safety assurance documentation (including feedback from domains other than the primary domain of application).	Respondent subjective rating.
2. Efficiency of the Certification Process	2.1 Time needed by the applicant for completing the certification process with the proposed certification approach.	Respondent subjective rating.
	2.2 Time needed by the certifying authority to follow and review proposed certification approach, and to review the result from this approach applied by the applicant.	Respondent subjective rating.
	2.3 Time needed for the training of personnel to familiarise with the proposed certification approach.	Respondent subjective rating.
	2.4 Time needed to develop the certification safety assurance documentation by the applicant.	Respondent subjective rating.
	2.5 Time to complete the review of the certification safety assurance documentation by the certifying authority.	Respondent subjective rating.
3. Cross domain integration	3.1 Degree to which the proposed certification approach promotes and supports coordination, cooperation and exchange of information between stakeholders and across domains during the certification process.	Respondent subjective rating.
	3.2 Degree to which the proposed certification approach provides clarity of roles and responsibilities of the stakeholders involved in the certification process from the start of the process (or through stage 1-11 in the proposed approach).	Respondent subjective rating.
	3.3 Degree to which the proposed certification approach is able to support the involvement of stakeholders from other domains than primary certification domain.	Respondent subjective rating.
	3.4. Degree to which the proposed certification approach is able to integrate the local approaches in use in each domain, regardless of whether they are compliance or performance based.	Respondent subjective rating.
4. Harmonisation	4.1 The extent to which the proposed certification approach promotes harmonisation and can be a standard reference approach in use across different domains and stakeholders.	Respondent subjective rating.
	4.2 The level of compatibility and consistency of the certification approach with existing certification practices, organisation and culture in aviation industry.	Respondent subjective rating.
5. Accommodation of Innovation	5.1 The potential of the proposed certification approach to ease the certification and continuous safety performance monitoring of innovative products and services.	Respondent subjective rating.

6. Operability of ASCOS processes and tools	6.1 Usability of the proposed certification approach in the certification process.	Respondent subjective rating.
	6.2 Usefulness, from an end user perspective, of the proposed certification approach in the certification process.	Respondent subjective rating.
	6.3 Acceptability, from an end user perspective, of the proposed certification approach in the certification process.	Respondent subjective rating.
7. Flexibility	7.1 The applicability of the proposed certification approach to a range of products and services varying in “size” and “complexity”.	Respondent subjective rating.
	7.2 Applicability of the proposed certification approach to the products and services of different domains, of different stakeholders and to the TAS.	Respondent subjective rating.
	7.3 Applicability of the proposed certification approach to both novel and derivative products and services.	Respondent subjective rating.

7.5.2 KPIs for the Safety Performance Monitoring Process and Tools (WP2 results)

Table 9 shows the Key Performance Indicators (KPIs) for the validation of the ASCOS WP2 results: the ASCOS Safety Performance Monitoring Process and Tools including the Safety Performance Indicator (SPI) Framework.

Important notes:

- In the context of the WP2 results, the KPA 1 should be interpreted as the extent to which the ASCOS Safety Performance Monitoring Process and Tools, including the Safety Performance Indicator (SPI) Framework, contribute to the soundness of the certification safety assurance documentation and continued safety performance monitoring (or continued airworthiness).
- The KPIs in this table are not the actual items to be asked directly to respondents during the validation exercises. Rather, these KPIs will be translated into a validation questionnaire, which will be designed in WP5.2.

Table 9: Definition of KPIs for ASCOS Safety Performance Monitoring Process and Tools.

KPA	KPI	Metric
1. Soundness of the Certification Safety Assurance Documentation	1.1 Degree to which the Safety Performance Monitoring Process and Tools contribute to the soundness of the Certification Safety Assurance Documentation.	Respondent subjective rating.
	1.2 Completeness of the SPI framework in relation to the TAS, different domains and stakeholders.	Respondent subjective rating.
	1.3 Degree to which the Safety Monitoring Process and Tools provide and improve feedback to suppliers and service providers on in-service performance and on assumptions regarding the operating environment made in design and certification safety assessments.	Respondent subjective rating.
2. Efficiency of the Certification Process	2.1 Impact on efficiency of stage 8, 9, 10 of the proposed certification approach by the Safety Performance Monitoring Process and Tools as part of the 'a posteriori risk assessment'.	Respondent subjective rating.
	2.2 Time needed to collect data to quantify the relevant SPIs in the context of a certification process and continued safety monitoring.	Respondent subjective rating.
	2.3 Degree of effort for the applicant required to maintain the database and tools and to semi-continuous update the SPIs of the (total) aviation system.	Respondent subjective rating.
	2.4 Time needed by the applicant to train its personnel on the Safety Performance Monitoring Process and Tools.	Respondent subjective rating.
3. Cross domain integration	3.1 Degree to which the Safety Monitoring Process and Tools promote and support coordination, cooperation and exchange of information between stakeholders and across domains during the certification process.	Respondent subjective rating.
	3.2 Degree to which the Safety Monitoring Process and Tools enable the monitoring of the safety performance of systems of organisations.	Respondent subjective rating.
4. Harmonisation	4.1 The extent to which the Safety Monitoring Process and Tools promote harmonisation and can be a standard process and common framework for safety performance monitoring across different domains and stakeholders.	Respondent subjective rating.
	4.2 The level of compatibility and consistency of the Safety Monitoring Process and Tools with existing practices, organisation and culture in aviation industry.	Respondent subjective rating.
5. Accommodation of Innovation	5.1 The potential of the Safety Monitoring Process and Tools to ease the certification and continuous safety performance monitoring of innovative products and services.	Respondent subjective rating.
6. Operability of ASCOS processes and tools	6.1 Usability of the Safety Monitoring Process and Tools in a certification process.	Respondent subjective rating.
	6.2 Usefulness, from an end user perspective, of the Safety Monitoring Process and Tools in a certification process.	Respondent subjective rating.
	6.3 Acceptability, from an end user perspective, of the Safety Monitoring Process and Tools in a certification process.	Respondent subjective rating.
7. Flexibility	7.1 Applicability of the Safety Monitoring Process and Tools to a range of products and services varying in "size" and "complexity".	Respondent subjective rating.
	7.2 Applicability of Safety Monitoring Process and Tools to the products and services of different domains, of different stakeholders and to the TAS.	Respondent subjective rating.
	7.3 Applicability of the Safety Monitoring Process and Tools to both novel as well as derivative products and services.	Respondent subjective rating.

7.5.3 KPIs for ASCOS WP3 Safety Risk Assessment Methodology, Risk Model and Tool

Table 10 shows the Key Performance Indicators (KPIs) for the validation of the ASCOS WP3 results: the ASCOS Safety Risk Assessment Methodology, Risk Model and Tool.

Important notes:

- In the context of the WP3 results, the KPA 1 should be interpreted as the extent to which the ASCOS Safety Risk Assessment Methodology, Risk Model and Tool contribute to the soundness of the certification safety assurance documentation and continued safety performance monitoring (or continued airworthiness).
- The KPIs in this table are not the actual items to be asked directly to respondents during the validation exercises. Rather, these KPIs will be translated into a validation questionnaire, which will be designed in WP5.2.

Table 10: Definition of KPIs for ASCOS Safety Risk Assessment Methodology, Risk Model and Tool.

KPA	KPI	Metric
1. Soundness of the Certification Safety Assurance Documentation	1.1 Degree to which the Safety Risk Assessment Methodology, Risk Model and Tool contribute to the soundness of the Certification Safety Assurance Documentation	Respondent subjective rating.
	1.2 Ability to identify, assess, and provide risk estimates based on the consideration of TAS level failures (i.e. failures from other TAS domains than solely from the primary domain of certification) and consideration of emerging and future risks (future risk picture).	Respondent subjective rating.
	1.3 Accuracy and reliability of output of the Risk Model and Tool.	Respondent subjective rating.
	1.4 Completeness of the Risk Model and Tool (accident scenarios in the model) in reference to international definitions and standards, taxonomies, accident categorisations etc.	Respondent subjective rating.
2. Efficiency of the Certification Process	2.1 Impact on efficiency of stage 4, 5, 6 of the proposed certification approach by the Safety Risk Assessment Methodology, Risk Model and Tool as part of the 'a priori risk assessment'.	Respondent subjective rating.
	2.1 Degree of effort needed by the applicant to develop a future risk picture, inclusive of emerging and future risks, during the certification process.	Respondent subjective rating.
	2.3 Degree of effort needed by the applicant to operate and maintain the Safety Risk Assessment Methodology, Risk Model and Tool.	Respondent subjective rating.
	2.4 Time needed by the applicant to train its personnel on the Safety Risk Assessment Methodology, Risk Model and Tool.	Respondent subjective rating.
3. Cross domain integration	3.1 Degree to which the Safety Risk Assessment Methodology, Risk Model and Tool promote and support coordination, cooperation and exchange of information between stakeholders and across domains during the certification process.	Respondent subjective rating
	3.2 Degree to which interfaces between disciplines, between domains and the entire system life-cycle are part of the Safety Risk	Respondent subjective rating

	Assessment Methodology, Risk Model and Tool to support cross domain integration.	
4. Harmonisation	4.1 The extent to which the Safety Risk Assessment Methodology, Risk Model and Tool promote harmonisation and can become a standard reference model used in the certification process.	Respondent subjective rating.
	4.2 The level of compatibility and consistency of the Safety Risk Assessment Methodology, Risk Model and Tool with existing practices, organisation and culture in aviation industry. Including compatibility and consistency with other risk models and tools used in different (certification) domains.	Respondent subjective rating.
5. Accommodation of Innovation	5.1 The potential of the Safety Risk Assessment Methodology, Risk Model and Tool to ease the certification and continuous safety performance monitoring of innovative products and services.	Respondent subjective rating.
6. Operability of ASCOS processes and tools	6.1 Usability of the Safety Risk Assessment Methodology, Risk Model and Tool in the certification process.	Respondent subjective rating.
	6.2 Usefulness, from an end user perspective, of the Safety Risk Assessment Methodology, Risk Model and Tool in a certification process.	Respondent subjective rating.
	6.3 Acceptability, from an end user perspective, of the Safety Risk Assessment Methodology, Risk Model and Tool in a certification process.	Respondent subjective rating.
7. Flexibility	7.1 Applicability of the Safety Risk Assessment Methodology, Risk Model and Tool to a range of products and services varying in “size” and “complexity”.	Respondent subjective rating.
	7.2 Applicability of the Safety Risk Assessment Methodology, Risk Model and Tool to the products and services of different domains, of different stakeholders and to the TAS.	Respondent subjective rating.
	7.3 Applicability of Safety Risk Assessment Methodology, Risk Model and Tool to both novel and derivative products and services.	Respondent subjective rating.

8 Validation requirements

8.1 General requirements

According to the E-OCVM guidelines the validation requirements are “the requirements to achieve validation” and can be considered “enablers” for the validation activities, e.g. the timely availability of the performance framework. The validation requirements were identified by the authors of this report based on their experience and common sense. In this chapter the identified validation requirements are broken down into general validation requirements (this section) and requirements specific to validation of the three main ASCOS results (next section).

The following general requirements have been identified:

- The ASCOS WP5 partners shall have a good understanding of the expected ASCOS results before the start of the definition of the validation plan.
- The ASCOS products shall be ready and mature at the time that the participants start the preparation and training for the validation exercises. This includes the ASCOS tools (e.g. tool for continuous safety monitoring from WP2 and the risk assessment tool from WP3) and associated e-learning modules.
- The involvement of stakeholders and/or aviation experts with relevant experience in certification and approval processes is essential for a successful validation. For this purpose it is important to timely contact UG members to secure their willingness and availability in the validation exercises. The workshop and meetings with UG members need to be planned adequately in advance.
- To ensure that the validation is complete and representative, i.e. that it covers the full range of users types, the participants involved in the validation should ideally include at least one person representing a service provider (e.g. an airline, airport, or ANSP), a manufacturer (e.g. ATM system or aircraft/aeronautical product), and a certifying authority (e.g. EASA, CAA).
- The participants in the validation exercises shall be properly trained prior to the validation exercises. Training requirements include:
    - The participants shall complete the relevant e-learning modules prior to the validation (familiarisation) workshop.
    - The participants shall be briefed and participate in the training session prior to the validation exercises. The briefing and training session may be part of the validation workshop.
    - The training should include an example application of the ASCOS approach or tool to be validated in the exercises (for example making use of WP4 results).
- It is expected that the ASCOS approach and tools from WP2 and WP3 will also be applied in the test case as part of WP4. Therefore, the validation plan shall take into account the experience and results from the application of these tools in WP4 case studies. It is required that the WP5 participants regularly exchange information with WP4 case studies. E.g. by participating in progress meetings, sharing deliverables, and interim results. Information relates to: fitness for purpose and assessed performance or benefits of ASCOS results, using the performance areas and indicators defined in the validation strategy.

8.2 Requirements for the validation exercises

The following requirements for the validation exercises have been identified:

- The participation of relevant ASCOS partners from WP1, 2, and 3 is required to provide technical and logistical assistance during the preparation of the training material, in relation to the ASCOS software tools needed for the validation exercises and the execution of these tools. The precise mode of involvement of the relevant partners will be defined in the WP5.2.
- The validation data collection activities will be based mainly on interviews, questionnaires and debriefing after the validation exercises. The data collection will be aimed at collecting data about:
  - The fitness for purpose and/or performance of the ASCOS results in relation to the validation objectives.
  - Suggestions for improvement of the ASCOS results.
  - Realism of the validation exercises and scenarios.
  - Possible future developments required.
  - Indications on the difference between the application of the ASCOS results in the validation exercises and the current practice.
- The comparison of the performance and benefits between ASCOS and the current practice relies on (subjective) expert opinion of the participants in the validation. To compare the performance and benefits of ASCOS results with the current practice in the WP4 cases and validation exercises, the participants in the validation need to make a judgement based on their understanding of the ASCOS results, the case or exercise and their experience in certification. Therefore it is required that participants provide not only their opinion or score (rating), but also explain the rationale for this level of rating and what should be done/developed/improved to increase the rate to a more positive level.
- It is important to establish that the tools and platforms to be used in the validation are adequately stable and robust. A sort of “debugging” activity should be completed to limit the risk of losing valuable time during the actual exercises/workshops with troubleshooting.
- In the definition of validation exercises and scenarios the WP5 team should consider examples of shortcomings, bottlenecks and problems in current certification activities provided by UG members during meetings and in questionnaires (WP1.3 and WP5 questionnaire) and described in ASCOS deliverables (e.g. D1.2, D1.3). These examples can be used for developing test case scenarios useful for demonstrating (i) how ASCOS results would deal with the issues embedded in each scenario, (ii) where the benefits of ASCOS can be expected, and (iii) how well ASCOS is able to mitigate the identified (mentioned) issues. Appendix C contains a list of collected examples of shortcomings, bottlenecks and problems.

9 Validation work plan

9.1 Introduction

This chapter describes the high level validation work plan, including validation activities (9.2), planning (9.3) and the outline and template for the validation plan (9.4). The key validation activities and planning will be further defined and refined in the upcoming WP5.2. The validation plan will provide an overview of the validation exercises linked to validation aims, with a draft schedule, resources, interactions (input/output), tools and platforms to be used. A selection of tools, test case, scenarios will be needed to address the validation objectives. It is not expected that one exercise or tool will cover all validation objectives. The validation plan will be defined in the WP5.2 and will be deliverable D5.2.

9.2 Key validation activities

9.2.1 Involvement of stakeholders

The involvement of stakeholders is a critical success factor in the validation. Therefore, the UG members should be timely contacted and invited to participate in the various validation activities. Considering their rank in their respective organization, UG members should be given appropriate advance notice so to maximize the chance of attendance. Alternatively, they may appoint a replacement from their organisation. After confirming their availability to a meeting or a workshop, they have to be briefed and prepared to ensure an adequate level of commitment and an active participation in the concerned activity. For this purpose they will be contacted previously to the first workshop to clarify aspects such as: their expected role and contribution, the required expertise/background, the planning and set-up of the workshop and the required effort. In addition to this, it may be necessary to confirm with the UG members their area of expertise and role in specific parts of the validation (exercises). At this stage the validation exercises are expected to be organized in the context of two events: the User Group Meeting 3 and the familiarization workshop (s). These are described hereafter.

9.2.2 User Group Meeting 3

Although it is primarily designed for the purposes of dissemination in the context of WP6, the UG meeting 3 is an excellent opportunity for the WP5 team to involve the UG members in ASCOS validation activities. For this reason the second day of the UG Meeting 3 (currently planned for the 10th of October 2014) will be dedicated to validation activities, after appropriate coordination with the WP6 team. Depending on the expected attendance, the second day of the UG Meeting 3 will be used to only present the validation strategy and to brief the participants about the ASCOS process and tools that will be subject to validation or to run part of the validation exercises.

9.2.3 Familiarisation workshop(s)

The familiarisation workshop(s) consist(s) of one/maximum two meetings that will be organized at Deep Blue office with selected representatives of the UG members. During this(/these) workshop(s) the participants will be asked to familiarize with the ASCOS process and tools and to test them by taking as reference – to the extent possible - concrete examples of certification.

The workshop(s) will have the following goals:

- Running of validation exercises and scenarios (e.g. apply the approach and tools to test cases).
- Reviewing the application of ASCOS approach and tools in the WP4 use cases and validation exercises to determine the fitness for purpose according to the performance framework.
- Collecting user feedback, data and information with respect to the performance of the ASCOS products. The data on indicators (KPIs) will be collected for the key performance areas (KPAs).
- Defining further actions and validation activities.

The familiarisation workshop(s) will be prepared during ASCOS WP5.2 and WP5.3, and conducted after the UG Meeting 3, in order to take fully advantage of the preparatory work during that meeting.

9.2.4 Interaction with WP4

The certification cases studies performed in ASCOS WP4 are relevant to the WP5 as they exemplify how a typical applicant would use the ASCOS products during the validation process. In other words they provide a real time longitudinal application of the ASCOS products during which the involved WP4 teams will have an opportunity to gain a first-hand in depth understanding of ASCOS products. For this reasons, at the moment the following synergies are expected to occur between the WP4 and WP5:

- WP4 case studies can be useful for demonstrating and assessing the fitness for purpose, performance and benefits of ASCOS results from an applicant perspective. There is an adequate representation of manufacturers in the consortium and User Group; directly (Rockwell Collins, Dassault Aviation) as well as indirectly (through EUROCAE, SAE, SESAR JU). The WP5 is considering the feasibility of involving some WP4 partners and asking other external stakeholders to also play the ‘role of the applicant’.
- WP5 and WP4 evaluations refer to the same performance framework presented in this document (see chapter 7). Although the WP5 validation is more focused on future potential ASCOS users compared to the WP4 evaluation, which is directly involving some of the project members, the aim is to share the same evaluation framework..
- Depending on their realism, depth and completeness, the WP4 cases have the potential to provide material that can be used to train the UG Members on the use of the ASCOS approach and tools. To take full benefit of this synergy, it is agreed that at least a representative from WP5 will attend the relevant WP4 meetings. This will ensure adequate coordination and exposure to feedback on the implementation of the cases by the WP4 partners.

9.2.5 Dry-run Interviews

It is planned that “test interviews” will be carried out by the WP5 validation project team to further refine the validation plan, performance framework, exercises scenarios, questionnaire and interview templates prior the conduct of the actual validation exercises in the familiarisation workshops. In order to take full advantage of the WP5.1 team composition, at present there is a plan to conduct these interviews at the CAA UK site with Certification and Safety Assessment experts among the CAA UK personnel. In case this will be possible, the WP5 team will provide the CAA UK with specific indications of the desired profiles of the interviewees.

9.2.6 Analysis and report

The data collection and analysis will be done in accordance with the performance framework described in this deliverable. The framework will be useful to drive the selection of the data collection methods, and the design of the research materials (i.e. questionnaires and interview templates). During data analysis, it will also provide a useful benchmark against which to compare UG views and perspectives collected during the validation exercise. With this approach it will be possible to determine the achieved level of performance, benefits and issues of the ASCOS products, and to derive conclusions and recommendations for further improvement as described in section 2.2.5.

9.2.7 Feedback to WP1

Feedback related to the continuous safety monitoring process and tool (WP2) and the risk assessment methodology and tool (WP3) that will be collected during the validation will be fed back to WP1 only. WP2 and WP3 will be completed before the end of the validation activities. Improvements to the WP2 and WP3 results (e.g. tools) will not materialise at the end of the project. Instead, feedback on the “fitness for purpose” of these WP2 and WP3 results will be fed back to the WP1 for consideration in the updated version ASCOS certification approach.

9.3 Validation planning

The Table 11 shows the draft planning of the validation activities. The workshops cannot occur too early as the development of the ASCOS products would not be completed. At the same time they cannot occur too late, as the validation also includes data analysis and reporting, which are two time consuming activities.

Table 11: Planning of key validation activities.

Action	Timeframe
Involvement of user group members	June – October 2014
Interaction with WP4	Continuous until December 2014
Dry-run validation workshop	August – September 2014
User Group Meeting 3	9-10 October 2014
Familiarisation workshop 1	To be determined
Familiarisation workshop 2 (Optional)	To be determined
Analysis and report	2015
Feedback to WP1	2015

9.4 Outline and template of the validation work plan

9.4.1 Outline

This section provides general guidelines and a template to define the validation plans to support the development of the experimental plan and scenarios in the WP5.2 “Experimental plan and scenarios development”. The validation plans will describe all aspects necessary to run the exercises, such as exercise objectives, indicators and metrics, scenarios and the roles of the different stakeholders, the activities to be undertaken, resources, schedule, interactions, the method(s), technique(s) and tool(s) to be used (also for the posterior data analysis) and the deliverables that will be prepared. The plan will also include procedures to be used to ensure the quality of the work.

As part of deliverable D5.2 three validation plans will be developed for the main ASCOS results:

- Validation Plan 1: New certification approach;
- Validation Plan 2: The Continuous Safety Monitoring process, methods and tools; and
- Validation Plan 3: The supporting safety based design systems and tools, including risk management methodology and risk models.

9.4.2 Guidelines for the development of the experimental plan and scenarios

This section provides guidelines for the reader to develop the ASCOS Validation Plans. The purpose of this section is to ensure that the development and design of the experimental plan and scenarios will be consistent, will be of quality, and will provide traceability and transparency so that the validation results can be unambiguously related to the validation objectives. This section explains the information that needs to be collected and described in the Validation Plans.

The table of contents of the ASCOS Validation Plan includes:

- Definition of the exercises
- Objectives for the validation exercises
- Validation scenarios specification
- Resources and schedule
- Roles and responsibilities in the exercises
- Validation platform and tools
- Performance indicators for the validation exercises
- Interactions, relationships and dependencies
- Deliverable
- Preparatory activities
- Quality assurance
- Risks and mitigations

These topics will be shortly explained on the following pages.

1. Definition of the exercises

There will be three main ASCOS Validation Plans, consisting of one or more validation exercises. In a validation exercise, one or more scenarios may be executed or tested. Scenarios are the way in which the exercise will be run, testing various cases, conditions, addressing different user questions, etc. The exercises and scenarios will be described In the Validation Plan. The exercises may have the form of simulations, studies, cost-benefit analysis, reviews, “playing with the tool” sessions, etc. In addition, in WP4 “certification case studies” the ASCOS new certification approach and tools will be applied in four use cases. The combination of these case studies and the validation exercises will ensure that ASCOS products are thoroughly evaluated to meet the validation objectives.

One or more exercises may be needed to satisfy a set of validation objectives. For each exercise four main phases are defined:

- Preparation: all activities to prepare the validation exercise and related scenarios.
- Training: the education, training and familiarisation of the users with the approach or tools that will be validated in the exercise. This includes the explanation of the scenario.
- Execution: the actual running of the exercises and scenarios.

- Evaluation: collection of the user feedback, validation results, and outcome of the exercise. The validation results need to be checked against the predefined performance framework to determine the achieved performance. Conclusions and recommendations for further improvement need to be collected and summarised.

Each exercise will be described in the Validation Plan. Table 12 can be used as a reference to support the overview of the exercises and traceability of the validation objectives in relation to exercises.

2. Objectives for the validation exercises

The objectives of the validation exercise and scenarios need to be defined. The objectives of the exercise should relate to one or more validation objectives. It should be explained how and in what form the validation exercises provide the evidence required to satisfy the related validation objectives. In the end, the set of validation objectives need to be satisfied by the set of validation exercises.

3. Validation scenarios specification

The scenarios that will be run during the exercise need to be specified. The scenario provides the "context", i.e. forms the set of assumptions, conditions, test case, sequence of events etc. against which ASCOS results will be tested and evaluated.

4. Resources and schedule

Resources need to be allocated to the three validation activities and the individual validation exercises. In addition, a time schedule needs to be defined for each validation exercise and its four phases. The partners involved in WP5 and the effort available should be distributed over the validation exercises and preferably divided over the four phases in each exercise. In addition, if the validation requires the participation of user group members, other organisations or ASCOS partners (e.g. from WP1, 2, 3 for support in the training), their required effort needs to be allocated.

5. Roles and responsibilities in the exercises

For each exercise, the role and responsibility of each stakeholder (company or user group member) needs to be explained.

6. Validation platform and tools

The validation platform and tools to be used in the validation exercises will be described in this section.

7. Performance indicators for the validation exercises

This section needs to define the performance indicators or metrics that are used in the exercise to determine the performance or "level of fitness" for purpose. The performance framework is defined in chapter 7 of this report.

8. Interactions, relationships and dependencies of the validation exercise

The validation exercises and scenarios may have interactions or dependencies with other exercises or validation activities. This section should define the inputs and outputs for each validation exercise. Inputs can be for example a set of scenarios, data, tools.

9. Deliverable

For each validation activity this task will produce a report, containing a detailed description of the executed exercises and the corresponding results. At the end of the WP5.3 there will be one deliverable D5.3 Validation exercises report. In the subsequent WP5.4, the validation results will be analysed and overall conclusions will be provided about the validation of the ASCOS products and recommendations for further improvement.

10. Preparatory activities

Preparing the validation exercises well is important since the resources and time available are limited within the project and also the availability of the involved user group members will be limited. The Validation Plan should describe the preparatory activities, especially preparation of the exercises and involved platforms/tools and the training of the involved user group members.

- Exercise preparation: Before the ASCOS products are validated with the user group members, the tools need to be tested with for example test data or a baseline scenario. It is important to establish that the tools and platforms to be used in the validation are stable and robust. This is a sort of "debugging" activity to make sure that everything works as planned and that no time is lost during the actual exercises/workshops with troubleshooting. Secondly, the validation platforms, tools, questionnaires, etc. used in the validation exercise need to be checked to ensure that they are correct, consistent, and unambiguous, which is a sort of calibration to ensure we are measuring the right thing during the validation exercise. It is expected that the ASCOS tools from WP2 and WP3 will also be applied in the test case as part of WP4. Therefore, the Validation Plan shall take into account the experience and results from the application of these tools in WP4 case studies.
- Training/familiarisation: The Validation Plan needs to specify the level of training, the form of training, for whom and when to be delivered. It is expected that user group members will participate in various validation exercises, for example in the form of a workshop, "off-line" experiments or review. They need some level of training and familiarisation so that they will understand the concept of ASCOS, the new certification approach and the ASCOS tools that will be validated. Training material and presentations need to be prepared by the WPs (including WP4). Also, the user group members need to be briefed on the relevant exercises and scenarios, and their roles and responsibilities.

11. Quality assurance

This section describes the plan and actions taken to ensure quality assurance, such as standards used, review procedure etc.

12. Risks and mitigations

This section of the Validation Plan should define the identified risks for the validation exercises and the proposed mitigation actions. The mitigation actions should clear define the entity responsible for implementation and deadline for implementation. If risks cannot be fully mitigated, the impact on the validation exercises needs to be specified, including the expected effect on the final outcome of the validation.

9.4.3 Example template validation plan

Table 12 shows an example of the overview table of the key characteristics of each validation exercise which is recommended to be included in the Validation Plan. The overview will help the reader to track and trace the set of validation exercises and validation objectives.

Table 12: Validation Plan: overview table.

Validation Exercise Reference	Validation objective	Schedule	Resources	Interactions	Tools and platforms
Ref number for the exercise ASCOS VE-1	List the validation objectives that will be tested in the exercise	Start date End date Of … Preparation, Training, Execution, and Evaluation	List the distribution of resources per company over the four stages; Preparation Training Execution Evaluation Company A, B, C (MM)	Define inputs and outputs related to this exercise. Needs input from: … Will be output for: ….	List tools and platforms to be used in the exercise
Etc.	Etc.	Etc.	Etc.	Etc.	Etc.

10 Conclusions and recommendations

The validation of the ASCOS results is intended to collect feedback from users on the fitness for purpose and expected benefits of the ASCOS results. The feedback will be used to revise and update ASCOS results, where possible, and make recommendations for further improvements and refinements of the ASCOS solutions.

The scope of the ASCOS validation activities will be 1) the newly proposed certification approach, as developed in WP1 and defined in D1.3 [4]; 2) the Continuous Safety Monitoring process described in D2.3 [9] and the supporting tool (D2.4) developed in WP2; and 3) the safety risk assessment methodology, risk model (D3.2 [8]) and tool (D3.3 [29]) developed by WP3. However, note that - in addition to these results - ASCOS also delivers:

- A method for assessing the overall safety impact of bringing safety enhancements into operational use. This method combines results obtained with the tool ATM-NEMMO (emerging NEtwork-Wide effects of inventive Operational approaches in ATM) with results obtained with the tool CATS (Causal model for Air Transport Safety) in order to assess the safety impact on the total aviation system.
- A proposal for application of a common safety standard framework to all the TAS stakeholders.
- A method to detect and code automatically aircraft system malfunctions, in order to be able to improve the in-service safety assurance guidelines and processes provided by e.g. EUROCAE and SAE.

These additional results are not in scope of the ASCOS validation activities. However, some ASCOS consortium members (notably APSYS) intend to bring these results into use within EUROCAE and SAE working groups.

The tools for Continuous Safety Monitoring (developed in WP2) and Safety Based Design (developed in WP3) both depend on the CATS, which was originally developed for CAA the Netherlands. It is recommended to dedicate additional effort to the validation of the original CATS tool, which was developed in 2008 [36].

ANSPs, airlines, ground handlers and airport operators are only indirectly involved in the User Group through membership of e.g. ESSI, SESAR JU, IATA, and FAST. These four stakeholder groups could also benefit from (parts of) the ASCOS solutions. Furthermore, they may be involved in the application of ASCOS solutions or affected by these solutions in the context of the cross domain integration and the total aviation system approach envisaged in ASCOS. It is therefore recommended to seek more direct involvement, if possible, of a representative of each of these four stakeholders in the validation. Their participation in the validation will be beneficial to collect feedback and to identify potential improvements that will enable to improve the ASCOS solutions so that they will add value to as many stakeholder groups in the total aviation system as possible.

The validation strategy was developed based on the guidelines documented in the E-OCVM. Although the ASCOS results are not an operational concept or system, it is believed that the guidelines and good practice of E-OCVM can be applied to the ASCOS project. The application of the E-OCVM principles with adaptations to the ASCOS project proved useful for developing the validation strategy and performance framework.

The assessment of the maturity level of the ASCOS proposed solutions conducted in section 5.5 has concluded that current maturity level calls for a validation focus on concept refinement and exploration, rather than on proving fit-for-purpose as if it were the final “end product”.

A performance framework was developed to be able to assess the performance of the ASCOS results in the validation exercises. This framework consists of a set of Key Performance Areas (KPAs), Key Performance Indicators (KPIs) and metrics. The KPAs are areas of performance that reflect high-level ambitions and expectations of the stakeholders. Seven KPAs are defined:

1. Soundness of the certification safety assurance documentation,
2. Efficiency of the certification process,
3. Cross domain integration,
4. Harmonization,
5. Accommodation of innovation,
6. Operability of ASCOS processes and tools, and
7. Flexibility.

In the ASCOS performance framework, KPIs will be used to measure the “fitness for purpose” of the ASCOS results in a specific area. The metrics are the way in which the KPIs are measured or expressed. The KPIs and metrics have been identified for the KPAs for each of the three ASCOS “products”. During the validation exercises feedback will be collected from the involved users by means of a questionnaire, which will be designed in follow-up activities (WP5.2). These KPIs will be addressed in validation questionnaires. Validation requirements were established, i.e. items that need to be satisfied to prepare for and achieve validation.

In conclusion, the present document provides the basis for conducting the validation activities in WP5. While it is providing directions for the work ahead in the form of validation objectives and validation requirements, this document has also developed a comprehensive performance framework for evaluating the ASCOS proposed solutions. The next phase of the work (WP5.2 Validation Plan and Scenarios) will build upon this basis in order to specify all the aspects needed for conducting the validation exercises, i.e. exercise objectives, scenarios, tasks, roles, data collection and data analysis methods, and evaluation schedule.

References

#	Authors(s), Title, Year
1	ASCOS Website, http://www.ascos-project.eu, 2014.
2	FAA, Commercial Airplane Certification Process Study, March 2002.
3	B. Pauly, T. Longhurst, A. Iwaniuk, M. Idzikowski, B. Dziugiel. Analysis of existing regulations and certification processes. ASCOS D1.1, version 1.3, 20-08-2013.
4	A. Simpson, S. Bull, T. Longhurst. Outline Proposed Certification Approach. ASCOS D1.3, version 1.2, 18-12-2013.
5	European Commission; Setting up an aviation Safety Management System for Europe, Brussels, COM(2011) 670 final, 25-10-2011.
6	A.L.C. Roelen, J. Verstraeten, L. Save, N. Aghdassi. Framework Safety Performance Indicators. ASCOS D2.1, version 1.5, 14-01-2014.
7	J.P. Magny, A.L.C. Roelen, J.J. Scholte, T. Longhurst, A. Iwaniuk. Total aviation system safety assessment methodology. ASCOS D3.1, version 1.6, 30-12-2013.
8	A.L.C. Roelen, J.G. Verstraeten, V. Bonvino, J.-F. Delaigue, J.-P. Heckmann, T. Longhurst, L. Save. Risk models and accident scenarios. ASCOS D3.2, version 1.3, 21-08-2013.
9	Andrzej Iwaniuk, Piotr Michalak, Gerard van Es, Bartosz Dziugieł, Wojciech Miksa, Maciej Mączka, Nuno Aghdassi, Reinhard Menzel, Luca Save. Process for Safety Performance Monitoring. ASCOS D2.3, version 1.0, 21-3-2014.
10	L.J.P. Speijker, A.L.C. Roelen. Required functionalities of risk assessment tool. An initial view on how to ensure that customer and user expectations are met. Version 1.2, 31-10-2013.
11	SESAR Definition Phase; Study of safety regulatory framework, WP1.6.1/D1, DLT-0507-161-00-03.
12	EASA; Opinion no 02/2010 of the European Aviation Safety Agency, “for a Commission Regulation XXX/2010 on common requirements for the provision of air navigation services, as regards working methods and operating procedures AND for a Commission Regulation XXX/2010 on safety oversight in air traffic management and air navigation services”, of 28 May 2010.
13	U. Dees, P. van der Geest, A. Simpson, S. Bull, P. Blagden, T. Longhurst, A. Eaton, G. Temme, B. Pauly. Definition and evaluation of innovative certification approaches. ASCOS D1.2, version 1.3, 20-08-2013.
14	L. Wamiti, G. Temme. Minutes of ASCOS User Group Workshop 1, 30 October 2012, Amsterdam, the Netherlands.
15	M. Heiligers. Minutes of ASCOS User Group Workshop 2, 19-20 September 2013, Arona, Italy.
16	M. Heiligers. Minutes of ASCOS – SESAR Meeting, 30 July 2013, Brussels, Belgium.
17	L.J.P. Speijker. Minutes of ASCOS – EASA Technical Information Meeting, 4 September 2013, Cologne, Germany.
18	L.J.P. Speijker. Minutes of ASCOS-EASA Technical Information Meeting, 26 November 2013, Cologne, Germany. Part 1.
19	L.J.P. Speijker. Minutes of ASCOS-EASA Technical Information Meeting, 26 November 2013, Cologne, Germany. Part 2.
20	M. Heiligers, G. Temme. Minutes of ASCOS EASA Workshop, 19 April 2013, Cologne, Germany.
21	C. Haddon-Cave, C; An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, HMSO UK, 2009.
22	E-OCVM Version 3.0, Volume I, Eurocontrol, February 2010.
23	E-OCVM Version 3.0, Volume II Annexes, Eurocontrol, February 2010.
24	Eurocontrol, Safety Assessment Made Easier (SAME), Part 1 Safety Principles and an Introduction to Safety Assessment, January 2010.
25	Eurocontrol, Safety Case Development Manual, Version 2.2, November 2006.
26	Manual on Air Navigation Services Economics. ICAO Doc 9161. Fifth edition, 2013.
27	SESAR Project ID 16.06.06 D06-05 - ATM CBA for Beginners
28	EPISODE 3, Performance Framework. D2.4.1-04. Version 3.06, 9-11-2009.
29	H. Udluft, P.C. Roling, R. Curran. Tool for risk assessment - User Manual. D3.3, version 1.0, 24-3-2014.

30	K. Harwood. Defining human-centered system issues for verifying and validating air traffic control systems. Verification and Validation of Complex Systems: Human Factors Issues. Springer NATO ASI Series Volume 110, 1993, pp 115-129.
31	Bishop and Bloomfield. A methodology for safety case development. Proceedings of the Sixth Safety-critical Systems Symposium, February 1998.
32	ASCOS D2.4; Tools for continuous safety monitoring
33	ASCOS D2.5; Continuous Safety Monitoring, WP2 Final Report
34	ASCOS D3.5; Total aviation system standards improvements
35	ASCOS D3.6; Safety Risk Management, WP3 Final Report
36	B. Ale et al; Causal model for Air Transport Safety (CATS), Final report, 2008

Appendix A Definitions

Benefit Mechanism. It consists of a cause-effect description of the improvement proposed by a project. It shows how the change proposed by a project leads the intended benefit. It can be presented in both textual and diagrammatic form [27].

Certification. The process and set of activities aiming at the satisfaction of an authority that a "deliverable" (e.g. aircraft, aviation product, service, or organisation) complies with a set of regulations in order to ensure its proper operation and to ensure continued performance of these items during their operational life.

Certification Safety Argument. A documented body of evidence that provides a convincing and valid argument that a system is acceptably safe for a given application in a given environment [31]. A safety case is composed by a set of explicit claims about the system, a body of supporting evidence, by a set of inference rules that link the claims to the evidence, an explicit set of fundamental assumptions and judgments in which the argument is valid. While this definition applies to safety arguments in general, we refer here to certification safety argument as the safety argument to be used in a certification context.

Certification Safety Assurance Documentation. The documentation produced by the applicant to demonstrate to the certifying authority that the change in question is acceptably safe. This documentation contains the evidence, the data, and the assumption that support the overall claim that the change is acceptably safe. After being produced by the applicant(s), this documentation is then reviewed by the certificatory body which will have to approve or reject such documentation. In countries like the UK the Certification Safety Assurance Documentation corresponds to the certification safety argument. However, while this latter is perhaps the most sophisticated methodology to demonstrate the acceptable safety of a given change, safety arguments are not adopted uniformly across all states and stakeholders, and some states might use other approaches.

Change. In this context, the replacement or the introduction of a new procedure, operation, hardware or software system.

Cross acceptance. A situation where equipment in service accepted by a particular authority is accepted for use by a different authority.

Key Performance Area (KPA). "Key performance areas are broad categories that describe different areas of performance of an ATM system." [22]. "Key Performance areas are a way of categorising performance subjects related to high-level ambitions and expectations. ICAO has defined 11 KPAs: Safety, security, environmental impact, cost effectiveness, capacity, flight efficiency, flexibility, predictability, access and equity, participation and collaboration, interoperability." [28].

Key Performance Indicator (KPI). Key performance indicators "measure performance in key performance areas and are identified once key performance areas are known. A key performance indicator is a measure of some aspect of a concept or concept element, for example 'the total number of runway incursions per year', the 'mean arrival delay per week at airport X'." [22]. "Current/past performance, expected future performance

(estimated as part of forecasting and performance modelling), as well as actual progress in achieving performance objectives is quantitatively expressed by means of indicators (sometimes called Key Performance Indicators, or KPIs). To be relevant, indicators need to correctly express the intention of the associated performance objective. Since indicators support objectives, they should not be defined without having a specific performance objective in mind. KPIs are not often directly measured. They are calculated from supporting metrics according to clearly defined formulas, e.g. cost-per-flight-indicator = Sum (cost) / Sum(flights). Performance measurement is therefore done through the collection of data for the supporting metrics." [28].

Metrics. "Supporting metrics are used to calculate the values of performance indicators. For example cost-per-flight indicator = Sum(cost) / Sum(flights). Performance measurement is done through the collection of data for the supporting metrics (e.g. this leads to a requirements for cost data collection)" [28].

Modularization. It is the process of breaking up complex or large arguments into manageable modules.

Performance Framework. A performance framework is "used to document and establish the framework for performance assessment. It typically consists of Key Performance Areas (KPAs), key performance indicators (KPIs), performance targets, metrics and measurement-related assumptions which are used to validate a concept. The performance framework may be enhanced to support the understanding of how benefit is produced and delivered and for the examination of performance trade off" [22]. A performance framework needs "to be in place at the very early stage to ensure that it is taken into account in the planning of the validation programme and exercises" [22].

Performance Target (PT). "Performance targets are closely associated with [key] performance indicators: they represent the values of performance indicators that need to be reached or exceeded to consider a performance objective as being fully achieved." [28].

Validation. The process by which the fitness-for-purpose of a new system or operational concept being developed is established". The objective of the validation of the ASCOS results is to demonstrate that they are suitable for their intended purpose or use and brings the expected benefits for the user

Verification. Verification is the set of activities aimed at testing or demonstrating that the product (e.g. a tool) meets the technical specifications. The verification aims to assess the technical quality and performance of the products.

Appendix B Identification of bottlenecks and shortcomings

This Appendix presents a summary of the identification of bottlenecks and shortcomings in the current certification and continued safety monitoring practise. These bottlenecks and shortcomings have been collected from previous work done and deliverables in the ASCOS project. The next Appendix includes examples provided by ASCOS user group members related to issues in current certification.

As part of WP1 the existing regulations and certification processes were analysed to identify shortcomings and bottlenecks in these regulations and processes. In other words, to identify areas for improvement. In the context of validation, these identified shortcomings and bottlenecks are relevant since it provides a reference and "test cases" to evaluate whether ASCOS brings benefits to the current certification practice, amongst others by reducing shortcomings and bottlenecks. The list of identified shortcomings and bottlenecks is a helpful addition to the list of user expectations with regards to the ASCOS results. The shortcomings and bottlenecks can be translated into user expectations, but obviously ASCOS will not be able to address all shortcomings and bottlenecks as our project is a research project within limited time, resources and scope.

In ASCOS D1.3 [4] a shortcoming is defined as a situation where the existing regulations are either inadequate or simply do not provide the necessary control. A bottleneck is defined as situation where the existing regulations, although adequate on paper, are not adequately implemented, throughout Europe; this may include situations where implementation is not uniform in the member states.

The list below is based on information collected from ASCOS D1.1 [3], D1.2 [13], and D1.3 [4]. In ASCOS WP1.3 a questionnaire was distributed amongst the user group members on certification regulation, processes, current practices, issues etc. The responses were analysed in the appendix of D1.3.

In D1.1 the following bottlenecks and shortcomings were identified:

- The contribution of human error is not adequately recognised during the certification process
- Insufficient attention is paid to human contributions to past accidents in the design of new processes, products and systems.
- Insufficient attention is paid to how flight crew will react to equipment failure when designing equipment.
- Insufficient attention is paid to ensuring that maintenance activities are not error prone.
- There is a lack of staff who sufficiently understand the regulatory requirements.
- There is a lack of staff who sufficiently understand the certification process.
- Existing regulations and specifications do not provide flexibility to allow innovation.
- Certification of COTS is unnecessarily difficult.
- Accountability for safety is unclear.
- Safety requirements are incompatible with requirements in other domains.
- Requirements do not allow hazardous failures to be balanced against the benefits of successful implementation.

- Inappropriate weight given to the service history of a product.
- SWALs and SILs do not have any evidence linking risk to process requirements.
- Insufficient attention is paid to safety assessment (including review of initial design safety assessments) when considering aircraft alterations.
- Lack of consistent format of take-off and landing data for all runway conditions.
- Inadequate regulation for provision of correct, up-to-date and timely runway condition reports.
- Safety features of procedures or equipment are not sufficiently explained to ensure that they are not compromised by subsequent alteration, maintenance and repair.
- There are insufficient controls to ensure that the manufacturer's operational or maintenance recommendations are fully implemented.
- Argument-based approaches not applied with the necessary rigour, with insufficient focus on safety risks or with insufficient attention paid to the context in which the argument is made.

The FAA's Commercial Airplane Certification Process Study [2] identifies a number of shortcomings and bottlenecks in certification, of which many are also applicable to Europe and are still applicable to the situation of today. Here we list the five focus areas, and for each an example [from [4]):

- The airplane certification process. For example regulations do not yet adequately address the subject of human error in design, operations and maintenance.
- Aviation safety data management. For example, multiple data collection and analysis programs exist in Europe without adequate coordination or executive oversight.
- The interfaces between maintenance, operations, and certification. For example, improvement is still possible in capturing the lessons learned from specific experiences in manufacturing, maintenance, and flight operations, and in making these available for the aviation industry.
- Major repairs and modifications. For example, inconsistencies exist between the safety assessments conducted for the initial type certificate (TC) and some of those conducted for subsequent alterations to the aircraft as there is no established and detailed enough safety assessment methodology commonly used by all interested parties.
- Safety oversight process. For example, there are inconsistent processes to detect and correct errors made by individuals in for example design or certification.

From both SESAR WP1.6.1/D1 [11] and EASA Opinion 02/2010 [12] it is known that there are many issues associated to the current ATM safety regulation framework, for example:

- Solving the fragmentation and variability in regulations over different domains of air transport, and in the interpretation of regulations over European countries.
- Improving safety accountability: The complex safety regulatory framework and the often detailed and prescriptive nature of safety regulations easily result in confusion over safety accountability.
- Reducing duplication of regulations, as overlap and contradictions lead to confusion and difficulty.
- Reducing complexity of regulation, which otherwise leads to ambiguity regarding compliance.

- Improving cost effectiveness: it should be clear how ATM safety regulation contributes to cost effective management of safety.

Additionally, D1.2 provides a collection of shortcomings and bottlenecks in the domain of air operator certification, aircraft/product certification, ATM, and airport certification. In summary the following bottlenecks are mentioned:

Air operator certification

In D1.2, section 2.2.3, a few bottlenecks in the current certification practice are mentioned:

1. Time consuming and therefore expensive certification process.
2. Applicants often do not have an adequate level of knowledge of the applicable regulatory requirements, especially they lack understanding of the regulations and their purpose to enhance safety.

Aircraft/product certification

In D1.2, section 2.3.3, a list of problems in the current certification practice were identified:

- Lack of regulations/rules to certify new technology; the process in place to address such a shortcomings (e.g. through special conditions) is time consuming and causes delay in certification.
- Lack of coordination between domains, such as between the product certification and operational certification, causing delay.
- New technologies could not be certified in time due to lack of requirements from the authority.
- Due to lack of requirements systems were introduced because of a perceived safety enhancement by fast introduction without due appreciation of the required reliability and availability.
- Human factors evaluations were not applied to “grandfather” developments from existing designs, negating the fact that this standard did not prevent several accidents.
- The EASA safety plan does not mention a streamlined certification process as a means to enhance safety.
- Human factors evaluations and certification is still not integrated with System Safety Assessments. Integration could give an incentive for good Human Factor design.
- Transmission of assumptions during a certification process are not properly transmitted to the next domain (e.g. auto throttle, Flight Management Systems at early stage).
- Retroactive applicability is not always considered due to the cost for the industry, despite the possibility to do so via CS26.
- Different certification approaches between different domains, which are sometimes in plain conflict, e.g. product certification, Operational certification, Maintenance certification and ATM requirements.

ATM certification

Report D1.2, section 2.1.4, describes the current process, challenges and potential solutions from the perspective of an ATM certifying authority, a developer of ATM systems and procedures, and an ATM ground systems manufacturing company. The following list is a collection of identified challenges, bottlenecks, or shortcomings in the "ATM certification" domain.

Many ATM projects are complex, especially regarding the number of interfaces and interactions, both within the domain and in its external interfaces. Addressing adequately the safety or risks of these interfaces and interactions is a challenge.

Previous studies have identified a number of weaknesses in the safety regulatory framework for ATM. The ASCOS project should take these weaknesses into account when developing a new approach and supporting tools. Examples of weaknesses mentioned in D1.2 include:

- Fragmentation of the regulatory framework across the states of Europe, inevitably leading to diversity of approaches and variation in the level and rigour with which the requirements are enforced.
- Confusion over accountability for safety.
- Complexity and duplication of regulations.
- Lack of transparency, especially where regulations are based on specific technology, making it difficult to introduce innovative solutions and difficult to demonstrate safety improvement.
- Lack of harmonisation between ATM and the other parts of the air transport industry in respect of safety targets and assessment approaches.

In the ATM domain the safety argument approach to obtain approval is common practice. As part of a safety case development, a safety argument is formulated and supporting evidence is collected to validate the claims in the argumentation, in other words to assure safety. D1.2 mentions a few challenges with this approach, such as:

- There may not be an (obvious) indication as to how the evidence should be obtained or how rigorous or trustworthy that evidence needs to be.
- There is the issue of addressing interfaces/integration and the broader aviation system. Aviation is an integrated, complex system. Stand-alone safety assessments may not represent risk from the interactions/integration completely or appropriately. The safety argument of a change or system element may be dependent on assumptions on interactions or performance of other parts of the system. Individual changes or elements of the system may be considered safe, but the challenge is to maintain a view on the overall system risk. The effect of a change on the safety of the total aviation system, across different organisations is difficult and impractical to assess.
- It is also mentioned in D1.2 that is may be (too) easy to create arguments that are false or invalid (or both), or biased towards proving it is safe that its leading the identification and analysis of risks. This has been highlighted as well by the Nimrod accident report [21] in which the safety case regime was thoroughly evaluated.

- It may be difficult or impossible to provide the evidence that safety targets are met, especially when it concerns software and human performance.
- In the (ATM) operational concept design or development phase limitations, dependencies, assumptions are defined which relate to organisations or actors outside ATM domain or outside the direct responsibility of the stakeholder.
- There can be unintended consequences on other systems if those systems are only considered in the context of the system or service under consideration for approval. The physical implementation of specifications can have unintended outcomes as a result of the implementation technology or equipment chosen. E.g. the equipment may provide more functionality, which was not considered during the design phase. It is then necessary to demonstrate that these unintended outcomes (e.g. extra functionality) cannot adversely affect the safety of the system. This is a common issue with Commercial-Off-The-Shelf products.
- The design specifications need to be realistic or realisable, i.e. the functionality, performance or integrity required are implementable by people, equipment or procedures.

Airport

D1.2 mentions that the airport certification domain is based on licencing airport operators, which is a relatively mature approach. At this stage in the ASCOS project, no bottlenecks or shortcomings have been identified in the domain of airport certification.

Appendix C Examples of identified bottlenecks and shortcomings

The ASCOS User Group members were asked to provide examples of bottlenecks, shortcomings, or problems in the current certification practices, processes and activities. Report D1.3 [4] and the questionnaires distributed as part of WP1 and WP5 contain examples, which are copied here.

Example 1: About coordination, integration, interfaces, cross-domain issues

Accidents resulting from air frame icing (of Fokker aircraft) while on the ground led to an overhaul of Fokker's operational rules with the target of ensuring that aircraft are clean before take-off. The manufacturer had to design a solution which met the differing requirements of three different authorities (in USA, Canada and Netherlands). The solution was driven by the manufacturer (perhaps because it is their name which will be discredited wherever any accident occurs), although the responsibility for implementation depends on interaction between airline, manufacturer and aerodrome procedures. This example illustrates how issues can cross boundaries both between domains and organisations, and how important it is to ensure that communication across these boundaries is effective. The modular argument approach described in this document (meaning D1.3 [4]) captures these cross boundary issues and supports effective management of them. A logical argument approach (supported by all stakeholders), if taken from the outset, could also have identified a different ideal solution, by changing the responsibility for the ground de-icing task.

Example 2: About coordination, integration, interfaces, cross-domain issues

Non-voice systems for controller-pilot communications (obviously) involve changes in (and affect) multiple domains (aircraft manufacturer, aircraft operator, ANSP). The European ATN system was developed largely from the ATM perspective with insufficient consideration of the aircraft (cockpit) end of the system. Development did not adequately consider: the need for certification of the airborne system, the human factors issues in the cockpit, the integration with the existing Future Air Navigation System (FANS) system (providing similar service, used in Pacific and North Atlantic), the need for training of operators in use of the system. Furthermore, the system was novel with no existing Acceptable Means of Compliance (AMC), which delayed the certification of the system on the aircraft side. Later on AMC material was developed which was difficult to comply with and also delayed the introduction by approximately two years. Furthermore, most implementations were substandard needing Airplane Flight Manual (AFM) limitations on its use to cover poor Human Machine Interface (HMI) designs. An ongoing concern is that there may be pressure to increase the use of the data communications system (currently limited to cruise phase, non-time critical messaging): the safety implications of this change of use would need careful consideration. The management of these issues could have been improved by earlier and better coordination between the domains and earlier publication of the requirements. The logical argument approach provides a framework to consider the total impact of introduction of this system. It also allows a performance based approach (where the specifications required for

a compliance based approach are not available), while allowing a compliance-based approach where the existing AMC material remains sufficient. The approach would also identify and define the interfaces between domains and stakeholders, allowing more efficient management of them. However, success of the approach does rely on co-operation between each domain (and geographic area?) within the TAS, and on identification of an "argument architect" to own and maintain the certification argument throughout the lifetime of the system.

Example 3: About safety assurance, validity of assumptions, future/emerging risks, future scenarios

A study in the mid-1990s identified that in 70% of accidents involving airplane systems, the original design assumptions were inadequate for the situation existing at the time of the accident due to changes in: the aviation system, airplane operational usage, personnel demographics, evolving infrastructure or other considerations. The continuing complexity and diversity of changes, including the changes in underlying technology can only serve to exacerbate the situation. This shows the criticality of documenting context and assumptions within a certification argument, and how it is critical to continually monitor these items through the lifetime of the system.

Example 4: About a change between performance-based and compliance-based or vice versa

Technology advances have made it possible to design an engine control system that automatically increases the thrust on the remaining engine(s) in case of engine failure. However, existing requirements require manual selection and back-up for this automatic feature, as previous automated systems were not reliable enough. Modern systems are so reliable that this manual back-up is no longer necessary, making it possible to remove unneeded components, thus removing failure modes and also increasing reliability. However, the authorities have not yet been able to develop an alternative requirement due to lack of resource. Adoption of a logical argument approach would open a way to implement this change without the need to first develop the alternative requirement and would ensure that all the possible impacts of such a change are adequately considered.

Example 5: About a proof of concept approach

The complexity of Flight Management Systems (FMS) makes it infeasible to test them exhaustively prior to introduction into service. Fokker F100 VNAV (Vertical Navigation) was improved following service entry using feedback from revenue flights; the improved version was then tested, as a proof of concept exercise, before introduction as a final version. Future FMS system development and introduction would benefit from wider application of this proof of concept approach, supported by logical argument to (a) identify where proof of concept would be most effective and (b) justify safety of execution of the proof of concept. (In this case, the

testing could be undertaken in revenue service, because the Fokker FMS 100 is not used as a primary navigation tool; however the proof of concept approach can also be applied without needing to undertake testing in revenue service.)

Example 6: About cross-domain fertilisation

Existing requirements for certification [meaning here the entire process of bringing operations into service and monitoring the operation] of flight operators are specified in detail and are effective in ensuring safety of flight operations. The existing approach follows the 5 phase ICAO process (although this is only advisory). The logical argument approach allows these requirements to be retained, while also allowing the flexibility of using a different approach where the applicant has specific needs which are not covered in the requirements. It may also be beneficial to adopt this approach when certifying other organisations involved within the TAS.

Appendix D ASCOS from a regulator's perspective

First and foremost the role of the National Supervisory Authority (NSA) is to act in loco parentis for the public in the context of air transport safety. The NSA, as a regulatory body, is established on the basis of legal mandate and consequently has to apply the State and European law. The underpinning principles of recent changes in European law are;

- The organisation that creates the risk is responsible for it;
- The organisation that creates the risk should manage it via the application of a Safety management System (SMS);
- Those organisations who are capable of creating significant risk are to be supervised which takes the form of:
  - Certificating their SMS,
  - Supervising the operation of the SMS, and
  - Approval of change in cases where it is believed there are significant risks.

A significant expectation of ASCOS is that it will assist in the "Approval of change in cases where it is believed there are significant risks".

In broad terms service providers are required to prepare a change safety case (or equivalent, please see the definition below) for any safety related change and to notify the NSA of that change. The risk used to determine whether a change safety case will be reviewed by the NSA is a combination of the safety risk associated with the change and the likelihood that the change safety case contains errors. Where this risk is low, the change safety case is unlikely to be selected for review by the NSA and the change can be implemented after the service provider has followed its approved change procedures, which must lead to the production of a valid safety case prior to the change being implemented. However, when the risk associated with the change exceeds given risk criteria, the NSA is required to review the safety case for change and the service provider must not implement the change until it has been approved by the NSA.

In reviewing any safety case the following principles, assertions and definitions are applied;

No part of a current operational system may be changed until a valid safety case exists that shows that the safety risk will be acceptable according to valid risk criteria for the change.

A safety case is: "a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment".

The purpose of the safety case is to convince the service provider that the proposed change will be safe and to communicate the reasons for that belief to an interested stakeholder e.g. regulator, judicial review or court.

A change safety case demonstrates that the proposed change (in all modes of operation, including fall-back), and the transitional stage(s) to implement it, will be acceptably safe.

A change safety case is notionally an amendment to the safety case that demonstrates all of the service provider's operations are acceptably safe.

The service provider has a responsibility to perform a risk assessment, demonstrate that excessive risks will be mitigated and amend the current unit safety case (or create a change safety case) before modifying the existing system. This responsibility is not affected by whether the NSA selects the change for review.

The change safety case contains safety criteria, which will be used during transition and in operation to determine whether the safety performance of the changed system is as predicted by the change safety case. The safety criteria explicitly define measureable parameters with acceptable limits, which demonstrate acceptable safety during transition and in operation, and the continuing validity of the change safety case.

The reason for the NSA reviewing a change safety case is to reduce the probability of an unsafe change entering service, by confirming that the change safety case is valid and accepting that the claimed level of safety is acceptable.

The role of the regulator is to only approve a change if it has been adequately justified by the delivered change safety case. It is not for the regulator to augment the safety case or to provide an alternative safety case in order to approve the change. Approval can only be based upon the contents of the delivered change safety case, together with any documented clarifications or further information supplied in response to the Regulator's enquiries. However, the Regulator may reject the safety case on the basis of expert knowledge or independently acquired information.

Comparing these principles and assertions it is clear that the stakeholder expectations (as expressed in Table 2 - Table 4) accord well with the expectations a regulator may have of the ASCOS approach.

What remains unresolved is the distinction between being 'better' and 'good enough'. The observation being that whilst one might know what to assess there is no clear determination of the degree to which one should assess. This is work in progress for the regulator.

It should be noted that provision has been made within the ASCOS programme for a regulator (i.e. CAAi) to review the safety cases that will be produced as part of the proof of concept. This is viewed very positively by the regulator as an opportunity to test the emerging thinking on setting the 'stop criteria' for assessment i.e. answering the question of how much assessment is enough.

Appendix E Relation between KPAs and user expectations

This appendix shows the user expectations and the 15 criteria used to evaluate proposed certification approached (in D1.2 [13]) with the related Key Performance Areas defined in chapter 7. This demonstrates the way in which the user expectations and previously used evaluation criteria are covered by the ASCOS performance framework.

Table 13: Stakeholder expectations (proposed ASCOS certification approach) and related KPAs.

No	Expectation – Proposed ASCOS certification approach	Related KPA
1	The ASCOS approach towards certification, including the developed supporting processes and tools, *should offer improvements over the existing certification and approval processes* in the areas 1.1 to 1.9 (below), whilst ensuring that at least a similar, and preferably an improved, level of safety assurance is provided as with the current certification approaches.	All KPAs
1.1	The ASCOS approach should *lower costs* of all involved processes and activities, both to the applicant and certifying authority.	KPA 2 Efficiency of the Certification Process
1.2	The ASCOS approach should *reduce throughput time* of certification processes. E.g. it will accelerate the certification and introduction into service of novel systems, technologies, and operations for which detailed prescriptive requirements are not available.	KPA 2 Efficiency of the Certification Process
1.3	The ASCOS approach should *ease the introduction* of safety enhancement systems and operations with special characteristics that are not yet or not fully covered in existing Certification Specifications;	KPA 5 Accommodation of innovation
1.3.1	It should *improve the ability to analyse and demonstrate acceptable safety for new concepts and technologies*.	KPA 5 Accommodation of innovation
1.3.2	It should *improve flexibility* in demonstrating compliance to (compliance or performance based) regulations in case of new or changed systems, technologies and/or operations.	KPA 7 Flexibility; KPA 5 Accommodation of innovation
1.4	The ASCOS approach should contribute to and support certification of *integrated systems* and *integration of different domains* in a certification approach, which includes:	KPA 3 Cross domain integration
1.4.1	Improve the ability *to analyse and consider the entire aviation system* rather than sub-elements in isolation.	KPA 3 Cross domain integration ; KPA 1 Soundness of the Safety Assurance Documentation
1.4.2	Enable *better addressing interfaces* between various domains in certification, e.g. ATM functions integrated in aeronautical products, and	KPA 3 Cross domain integration ; KPA 1

	aeronautical products and flight operations.	Soundness of the Safety Assurance Documentation
1.4.3	*Reduction of uncertainty* regarding safety accountability, roles and responsibilities, in the complex aviation system with integrated systems, interfaces and interactions.	KPA 3 Cross domain integration
1.5	The ASCOS approach should improve the ability to analyse and consider the impact on safety of *all elements of the aviation system* and *the entire system lifecycle* in a complete and integrated way.	KPA 1 Soundness of the Safety Assurance Documentation; KPA 3 Cross domain integration
1.6	The ASCOS approach should support certification taking into account *future and emerging risks* so that the certification appropriately takes into account the future developments, changes and scenarios (including the identification and assessment of future and emerging risks).	KPA 1 Soundness of the Safety Assurance Documentation
1.7	The ASCOS approach should *reduce uncertainties in certification activities*, e.g. uncertainty regarding the feasibility of achieving certification of novel technologies and concepts if no specifications (yet) exist or if the required performance level is not (yet) specified.	KPA 1 Soundness of the Safety Assurance Documentation
1.8	The ASCOS approach should explicitly consider *human performance* in a consistent and qualitative manner in overall safety assessments.	KPA 1 Soundness of the Safety Assurance Documentation
1.9	The ASCOS approach should contribute to *safety improvements for the Operational Issues of the European Aviation Safety Plan* (e.g. a reduction of fatal accidents due to: loss of control in flight, aircraft system or component failure or malfunction, aircraft ground handling aircraft damage and Air Traffic Management related incidents/accidents).	KPA 1 Soundness of the Safety Assurance Documentation

Table 14: Stakeholder expectations (continuous safety monitoring process and tools) and related KPAs.

No	Expectation – Continuous safety monitoring process and tools as part of the proposed ASCOS certification approach	Related KPA
2	The ASCOS approach towards certification including the developed supporting processes, tools and databases *should offer improvements for continuous safety monitoring* in areas 2.1 to 2.7. Continuous safety monitoring refers to the process for continued airworthiness of aircraft, and maintenance of certificates for air navigation service providers, operators, and manufacturers after they have been certified and while they are being operated / are operating.	All KPAs
2.1	The ASCOS approach should enhance the process and/or the capability for *providing feedback on assumptions* (e.g. assumptions about the operating environment) made in design and certification safety assessments.	KPA 1 Soundness of the Safety Assurance Documentation
2.2	The ASCOS approach should enhance the process and/or capability for *identification of new/changed hazards*, and assess associated risks, as part of continued airworthiness.	KPA 1 Soundness of the Safety Assurance Documentation
2.3	The ASCOS approach should enable the *development and maintenance (updating) of a risk baseline* for continuous safety monitoring (e.g. through a data driven, stable, reproducible EU baseline risk picture from multidisciplinary aviation safety data which can be regularly updated).	KPA 1 Soundness of the Safety Assurance Documentation
2.4	The ASCOS approach should support the *real time risk monitoring.* The data and the tools used for the real time risk monitoring provide the level of accuracy, reliability, and detail appropriate for the use in certification activities and continued airworthiness.	KPA 1 Soundness of the Safety Assurance Documentation
2.5	The ASCOS approach for the real time risk monitoring should *facilitate the quantification and semi-continuous updating* of the safety performance of the (total) aviation system at an acceptable level of effort and cost, e.g. of data collection, processing, and analysis.	KPA 1 Soundness of the Safety Assurance Documentation; KPA 2 Efficiency of the Certification Process
2.6	The ASCOS approach should enable the *linking of safety performance indicators to the main Operational Issues of the European Aviation Safety Plan* (e.g. runway excursion, controlled flight into terrain, loss of control in flight).	KPA 1 Soundness of the Safety Assurance Documentation

Table 15: Stakeholder expectations (safety risk management and safety based design) and related KPAs.

No	Expectation – Safety risk assessment: aviation safety assessment methodology, risk models and tools for risk assessment and safety based design as part of the proposed ASCOS certification approach	Related KPA
3	The ASCOS approach towards certification including the developed supporting processes, aviation safety assessment methodology, risk models and tools for risk assessment and safety based design risk should *offer improvements* in certification activities.	All KPAs
3.1	The ASCOS approach *should enable safety based design* of technologies, operations, and systems, which includes:	KPA 1 Soundness of the Safety Assurance Documentation
3.1.1	An approach for the *setting of safety targets, safety objectives and safety requirements* to be used in design.	KPA 1 Soundness of the Safety Assurance Documentation
3.1.2	The evaluation of *risk relative to a required safety performance* level.	KPA 1 Soundness of the Safety Assurance Documentation
3.1.3	The *assessment of the safety impact* of introducing new (safety enhancement) systems, concepts, technologies, and/or operations in the total aviation system in absence of data and deal with the issue of using historical data in that context.	KPA 1 Soundness of the Safety Assurance Documentation; KPA 5 Accommodation of innovation
3.1.4	The *identification of events* that can be considered as new precursors in case the novelty is implemented. Defining the capture process of new precursor and applying it on existing in service events databases to estimate precursor occurrence rate.	KPA 1 Soundness of the Safety Assurance Documentation; KPA 5 Accommodation of innovation
3.2	The ASCOS approach for safety risk assessment, including risk models and tools, should be *adjustable for a new certification question*, while the involved effort and cost are acceptable to the stakeholders.	KPA 7 Flexibility
3.3	The ASCOS approach for safety risk assessment *should provide a safety picture of the future*, taking into account likely changes, trends as well as the introduction of new products, systems, technologies and operations for which safety regulations may need to be updated.	KPA 1 Soundness of the Safety Assurance Documentation; KPA 5 Accommodation of innovation
3.4	The ASCOS approach for safety risk assessment should enable to *better anticipate on future risks and respond to precursors of future risks and hazards* instead of merely reacting on historic accidents. This aspect supports the continuous safety monitoring.	KPA 1 Soundness of the Safety Assurance Documentation

Table 16: Stakeholder expectations (usability and feasibility of proposed ASCOS approach) and related KPAs.

No	Expectation - Usability and applicability of the proposed ASCOS certification approach	Related KPA
4	The ASCOS approach towards certification including the developed supporting processes, tools and guidance material *should receive willingness* of the stakeholders to adopt the new approach and put it into practice.	All KPAs
4.1	The ASCOS approach should be *user-friendly*, e.g. easy to understand, easy to learn, easy to explain, easy to use.	KPA 6 Operability
4.2	The ASCOS approach should *reduce the required level of expertise and experience*, maintaining an equivalent or better level of safety compared to the current practice.	KPA 2 Efficiency of the Certification Process
4.3	The ASCOS approach should *reduce bureaucracy* both at the applicant and the certifying authority.	KPA 2 Efficiency of the Certification Process
4.4	The ASCOS approach should be *usable for a very wide range of applications* and applicable to the *different certification domains (e.g. aircraft, organisation, ATM, etc.*).	KPA 7 Flexibility
4.5	The ASCOS approach should enable *involvement of different stakeholders* from early on in the process.	KPA 3 Cross domain integration
4.6	The ASCOS approach should *not negatively impact harmonisation* and, preferably, promote harmonisation. It should *contribute to streamlining* processes using industry standards, while keeping differences with current regulations, requirements and practices limited.	KPA 4 Harmonisation
4.7	The ASCOS approach *should be compatible with existing practices, organisation and culture* in aviation industry, for example it should be flexible to accommodate and allow existing practices where appropriate in the ASCOS approach.	KPA 6 Operability

Table 17: Evaluation criteria from D1.2 and matching KPAs.

No	15 evaluation criteria for certification approach (from D1.2 [13])	Related KPA
1	Safety benefits	KPA 1 Soundness of the Safety Assurance Documentation
2	Costs benefits	KPA 2 Efficiency of the Certification Process
3	Reducing throughput time	KPA 2 Efficiency of the Certification Process
4	Stimulation of innovation	KPA 5 Accommodation of innovation
5	Reducing required expertise	KPA 2 Efficiency of the Certification Process
6	Bureaucracy	KPA 2 Efficiency of the Certification Process
7	Interoperability between domains	KPA 3 Cross domain integration
8	Early stakeholder involvement	KPA 3 Cross domain integration
9	Harmonisation and standardisation	KPA 4 Harmonisation
10	Acceptable means of compliance definition	KPA 4 Harmonisation; KPA 6 Operability
11	Level of difference with current requirement	KPA 4 Harmonisation
12	Ability to use retroactively	KPA 7 Flexibility
13	Promote human factor involvement	KPA 1 Soundness of the Safety Assurance Documentation
14	Possibility to delegate responsibilities to the applicant	KPA 3 Cross domain integration
15	Feasibility	Not applicable (referred to the outcome of the evaluation of all criteria in D1.2).

Appendix F WP5 Stakeholder's expectations questionnaire

This questionnaire aims to collect your feedback on the list of user expectations regarding the ASCOS project results.

In preparation for the validation activities in WP5, the project team needs to establish a complete overview of user expectations or needs with respect to the ASCOS results and benefits. This list of expectations will form the basis for the validation. The aim of the validation is to evaluate whether the ASCOS results are fit for purpose and bring the expected benefits. ASCOS delivers three "products" that need to be validated: a new certification approach (developed in WP1), the methods and tools for Continuous Safety Monitoring (developed in WP2), and the tools for safety based design and risk management (developed in WP3).

A list of user expectations was collected from the ASCOS Public material, the user group meetings, technical meetings with user group members and earlier ASCOS questionnaires. This questionnaire summarises these user expectations into four topics. For each topic there is a table with the corresponding expectations:

1. New certification approach (table 1);
2. Continuous safety monitoring (table 2);
3. Safety based design and risk assessment (table 3); and
4. Usability and applicability of the proposed ASCOS "products" (table 4).

We kindly ask you to complete the following three actions. You may provide your input only about those areas where you have experience or interest.

1. Please review and comment on the correctness and the completeness of the definition of the user expectations. Please provide suggestions for improvements if needed. If you miss expectations with respect to the ASCOS products in the current list, then you can provide your input per topic in the last row of the table, i.e. rows 1.10, 2.7, 3.5 and 4.8.
2. Please rate your top 5 of all expectations (from 1 = most important to 5 = least important) in the right-hand column of the tables.
3. Please provide examples from your professional experience that illustrate current certification problems, shortcomings and bottlenecks in relation to the topics or specific expectations.

Your input to this questionnaire will help us 1) to establish a correct and complete list of user expectations, 2) to focus on the most relevant expectations, and 3) to develop validation exercises using your examples as input.

We thank you in advance for filling in the questionnaire. If you have questions, please do not hesitate to contact us. You are kindly requested to return the questionnaire to:

Rombout Wever (NLR); Rombout.Wever@nlr-atsi.nl; Tel: +31 88 511 3124

Table 1

1	**New certification approach**	**1. Review and comment on the completeness and correctness of expectations listed in the column to the left. 3. Provide examples from your professional experience that illustrate current certification problems, shortcomings and bottlenecks in relation to the topic or specific expectations.**	**2. Your top 5 expectations.**
1	The ASCOS approach towards certification, including the developed supporting processes and tools, *should offer improvements over the existing certification and approval processes* in the areas 1.1 to 1.9 (below), whilst ensuring that at least a similar, and preferably an improved, level of safety assurance is provided as with the current certification approaches.	[please provide your review comments here] [please provide your examples here]	
1.1	The ASCOS approach should *lower costs* of all involved processes and activities, both to the applicant and certifying authority.	[please provide your review comments here] [please provide your examples here]	
1.2	The ASCOS approach should *reduce throughput time* of certification processes. E.g. it will accelerate the certification and introduction into service of novel systems, technologies, and operations for which detailed prescriptive requirements are not available.	[please provide your review comments here] [please provide your examples here]	
1.3	The ASCOS approach should *ease the introduction* of safety enhancement systems and operations with special characteristics that are not yet or not fully covered in existing Certification Specifications;	Etc.	
	• It should *improve the ability to analyse and demonstrate acceptable safety for new concepts and technologies*.		
	• It should *improve flexibility* in demonstrating compliance to (compliance or performance based) regulations in case of new or changed systems, technologies and/or operations.		
1.4	The ASCOS approach should contribute to and support certification of *integrated systems* and *integration of different domains* in a certification approach, which includes:		
	• Improve the ability *to analyse and consider the entire aviation system* rather than sub-elements in isolation.		
	• Enable *better addressing interfaces* between various domains in certification, e.g. ATM functions integrated in aeronautical products, and aeronautical products and flight operations.		
	• *Reduction of uncertainty* regarding safety accountability, roles and responsibilities, in the complex aviation system with integrated systems, interfaces and interactions.		
1.5	The ASCOS approach should improve the ability to analyse and consider the impact on safety of *all elements of the aviation system* and *the entire system lifecycle* in a complete and integrated way.		
1.6	The ASCOS approach should support certification		

	taking into account *future and emerging risks* so that the certification appropriately takes into account the future developments, changes and scenarios (including the identification and assessment of future and emerging risks).		
1.7	The ASCOS approach should *reduce uncertainties in certification activities*, e.g. uncertainty regarding the feasibility of achieving certification of novel technologies and concepts if no specifications (yet) exist or if the required performance level is not (yet) specified.		
1.8	The ASCOS approach should explicitly consider *human performance* in a consistent and qualitative manner in overall safety assessments.		
1.9	The ASCOS approach should contribute to *safety improvements for the Operational Issues of the European Aviation Safety Plan* (e.g. a reduction of fatal accidents due to: loss of control in flight, aircraft system or component failure or malfunction, aircraft ground handling aircraft damage and Air Traffic Management related incidents/accidents).		
1.10	***1.*** **Please mention any additional needs, requirements or expectations regarding the new certification approach here: …**		

Table 2

2	**Continuous safety monitoring process and tools as part of the proposed ASCOS certification approach**	**1. Review and comment on the *completeness* and *correctness* of expectations listed in the column to the left.** **3. Provide examples from your professional experience that illustrate current certification problems, shortcomings and bottlenecks in relation to the topic or specific expectations.**	**2. "Top-5 column"**
2	The ASCOS approach towards certification, including the developed supporting processes, tools and databases, *should offer improvements for continuous safety monitoring* in areas 2.1 to 2.6. Continuous safety monitoring refers to the process for continued airworthiness of aircraft, and maintenance of certificates for air navigation service providers, operators, and manufacturers after they have been certified and while they are operating.	[please provide your review comments here] [please provide your examples here]	
2.1	The ASCOS approach should enhance the process and/or the capability for *providing feedback on assumptions* (e.g. assumptions about the operating environment) made in design and certification safety assessments.	[please provide your review comments here] [please provide your examples here]	
2.2	The ASCOS approach should enhance the process and/or capability for *identification of new/changed hazards*, and assess associated risks, as part of continued airworthiness.	[please provide your review comments here] [please provide your examples here]	
2.3	The ASCOS approach should enable the *development and maintenance (updating) of a risk baseline* for	Etc.	

	continuous safety monitoring (e.g. through a data driven, stable, reproducible EU baseline risk picture from multidisciplinary aviation safety data which can be regularly updated).		
2.4	The ASCOS approach should support the *real time risk monitoring.* The data and the tools used for the real time risk monitoring provide the level of accuracy, reliability, and detail appropriate for the use in certification activities and continued airworthiness.		
2.5	The ASCOS approach for the real time risk monitoring should *facilitate the quantification and semi-continuous updating* of the safety performance of the (total) aviation system at an acceptable level of effort and cost, e.g. of data collection, processing, and analysis.		
2.6	The ASCOS approach should enable the *linking of safety performance indicators to the main Operational Issues of the European Aviation Safety Plan* (e.g. runway excursion, controlled flight into terrain, loss of control in flight).		
2.7	***1. Please mention any additional needs, requirements or expectations regarding the Continuous Safety Monitoring process and tools as part of the proposed ASCOS certification approach here: …***		

Table 3

3	**Safety based design and risk assessment process and tools as part of the proposed ASCOS certification approach**	**1. Review and comment on the *completeness* and *correctness* of expectations listed in the column to the left.** **3. Provide examples from your professional experience that illustrate current certification problems, shortcomings and bottlenecks in relation to the topic or specific expectations.**	**2. "Top-5 column"**
3	The ASCOS approach towards certification, including the developed supporting processes, safety assessment methodology, risk models and tools for risk assessment and safety based design risk, should *offer improvements for certification activities* in areas 3.1 to 3.4.	[please provide your review comments here] [please provide your examples here]	
3.1	The ASCOS approach *should enable safety based design* of technologies, operations, and systems, which includes:	[please provide your review comments here] [please provide your examples here]	
	• An approach for the *setting of safety targets, safety objectives and safety requirements* to be used in design.	[please provide your review comments here] [please provide your examples here]	
	• The evaluation of *risk relative to a required safety performance* level.	Etc.	
	• The *assessment of the safety impact* of introducing new (safety enhancement) systems, concepts, technologies, and/or operations in the total aviation system in absence of data and deal with the issue of using historical data in that context.		
	• The *identification of events* that can be		

	considered as new precursors in case the novelty is implemented. Defining the capture process of new precursor and applying it on existing in service events databases to estimate precursor occurrence rate.		
3.2	The ASCOS approach for safety risk assessment, including risk models and tools, should be *adjustable for a new certification question*, while the involved effort and cost are acceptable to the stakeholders.		
3.3	The ASCOS approach for safety risk assessment *should provide a safety picture of the future*, taking into account likely changes, trends as well as the introduction of new products, systems, technologies and operations for which safety regulations may need to be updated.		
3.4	The ASCOS approach for safety risk assessment should enable to *better anticipate on future risks and respond to precursors of future risks and hazards* instead of merely reacting on historic accidents. This aspect supports the continuous safety monitoring.		
3.5	***1. Please mention any additional needs, requirements or expectations regarding the aviation safety assessment methodology, risk models and tools for risk assessment and safety based design as part of the proposed ASCOS certification approach here: …***		

Table 4

4	**Usability and applicability of the proposed ASCOS certification approach**	**1. Review and comment on the *completeness* and *correctness* of expectations listed in the column to the left.** **3. Provide examples from your professional experience that illustrate current certification problems, shortcomings and bottlenecks in relation to the topic or specific expectations.**	**2. "Top-5 column"**
4	The ASCOS approach towards certification, including the developed supporting processes, tools and guidance material, *should receive willingness* of the stakeholders to adopt the new approach and to put it into practice considering items 4.1 to 4.7.	[please provide your review comments here] [please provide your examples here]	
4.1	The ASCOS approach should be *user-friendly*, e.g. easy to understand, easy to learn, easy to explain, easy to use.	[please provide your review comments here] [please provide your examples here]	
4.2	The ASCOS approach should *reduce the required level of expertise and experience*, maintaining an equivalent or better level of safety compared to the current practise.	[please provide your review comments here] [please provide your examples here]	
4.3	The ASCOS approach should *reduce bureaucracy* both at the applicant and the certifying authority.	Etc.	
4.4	The ASCOS approach should be *usable for a very wide range of applications* and applicable to the *different certification domains (e.g. aircraft, organisation, ATM, etc.)*.		
4.5	The ASCOS approach should enable *involvement of different stakeholders* from early on in the process.		
4.6	The ASCOS approach should *not negatively impact*		

	harmonisation and, preferably, promote harmonisation. It should *contribute to streamlining* processes using industry standards, while keeping differences with current regulations, requirements and practises limited.		
4.7	The ASCOS approach *should be compatible with existing practises, organisation and culture* in aviation industry, for example it should be flexible to accommodate and allow existing practises where appropriate in the ASCOS approach.		
4.8	***1. Please mention any additional needs, requirements or expectations regarding usability and applicability of the proposed ASCOS certification approach here: …***		

Appendix G WP5 Questionnaire response

This appendix presents a summary of comments and examples provided in the responses to the WP5 stakeholder's expectations questionnaire (see Appendix F). Responses were received from members of the following organisations (the corresponding stakeholder group, refer to Table 1, is reported in brackets):

- R1: Netherlands Aircraft Company (Manufacturer)
- R2: CAA UK (Regulators, regulatory bodies, authorities)
- R3: ESASI (Aviation safety and certification advisory bodies)
- R4: Dutch Ministry of Transport (Regulators, regulatory bodies, authorities)
- R5: Rockwell Collins (Manufacturer)

The observations and examples provided by the respondents are quoted below, grouped by the related user expectations (refer to Table 2 to Table 5 in section 4.3). This information may be useful when defining validation exercises and for the design of the data collection methods (e.g. interview template or questionnaires) that will be used to collect user feedback during the validation exercises. The authors reviewed the prioritisation of the user expectations by the respondents. Due to the limited number of responses it was decided not to provide a finale aggregated top-5 ranking.

User expectation 1.2 "The ASCOS approach should reduce throughput time of certification processes".

- R3: "Novel systems regarding new flight data recorder systems have been delayed and the difficulties in searching for Malaysian MH370 may have been avoided had new systems received timely certification."

User expectation 1.3 "The ASCOS approach should ease the introduction of safety enhancement systems and operations with special characteristics that are not yet or not fully covered in existing Certification Specifications".

- R4: "One of the main issues [in development of regulations for unmanned aircraft (RPAS)] is that the current approach to certification as we know from manned aviation does not fit for most of the unmanned aircraft and their operations. From this perspective there is no need for just some (major) steps in improving and optimising the current certification approach, but there is a strong need for a thorough rethinking of certification, its meaning as part of aviation safety and the economy of scales when considering the vast amount of unmanned aircraft that will be operating in the European skies in the not so distant future. Of course, improvements, reduction of cost and the ability to quickly adapt to new developments are important for manned aviation too […], but the real challenge is how we are going to deal with the 'new kid on the block' that does not fit very well into our current system."

User expectation 1.4 "The ASCOS approach should contribute to and support certification of integrated systems and integration of different domains in a certification approach".

- R2: "Safety assessment of integrated systems is essential to deal with current technology which relies on integrated functions and activity across traditional aviation sectors."
- R5: "A "systems of systems" approach, incorporating system engineering practice, is recommended in overall airspace system design and –ultimately- certification. First, the overall objective of the certification case should be well defined, including what is meant with "safety". Secondly, we need to define the top level argument and define the safety target or safety objective for the "system of systems". Subsequently the applicable regulations, certification specifications, standards, requirements, AMCs or other required guidance material needs to be defined and established. Thirdly, the breakdown of the top level safety target into more detailed requirements should be applied across the entire aviation system, across all (functional) domains, such as aircraft manufacturing, ATC, airports. It must be noted that this practice is in place and is highly developed specifically in the aircraft design, construction and certification practice, including systems, sub-systems design down to component level. This practice includes all the various standards and respective working groups, committees, relation to ICAO SARPS, internal industrial scrutiny, requirements conformance and compliance methods aimed at airworthiness and operations certification.

  The "system of systems" approach also requires coordination and feedback between each of the various stakeholders ("owning" their part of the system domain) to evaluate whether the requirements allocated to these domains will be feasible in order to ultimately meet the top-level safety target. If a requirement cannot be met, stakeholders need to discuss solutions by re-balancing their assigned requirements, for example by a re-distribution of the top level safety target across the (functional) domains.

  There is a need for a process that ensures the development and continuous improvement of safety standards, requirements, MOPS etc. in the total of aviation system domains. The current process in the aircraft manufacturing industry with standardisation bodies such as Eurocae/RTCA committees is mature compared to other domains. If ASCOS could somehow support this issue and bring improvement in performance and safety standard development in other domains, it would be seen as a major step forward in overall system performance and certification practice."

User expectation 1.6 "The ASCOS approach should support certification taking into account future and emerging risks so that the certification appropriately takes into account the future developments, changes and scenarios (including the identification and assessment of future and emerging risks)". Note that the comment also relates to *user expectation 2.2 "The ASCOS approach should enhance the process and/or capability for identification of new/changed hazards, and assess associated risks, as part of continued airworthiness"* and *expectation 3.3 "The ASCOS approach for safety risk assessment should provide a safety picture of the future, taking into account likely changes, trends as well as the introduction of new products, systems, technologies and operations for which safety regulations may need to be updated".*

- R3: "New lithium (and other) battery technology may have been identified as an increased risk under ASCOS proposals. The B787 [battery] incidents have shown the limitation of current certification regimes. [...] It is important that manufacturers do not shy away from pushing the technological boundaries therefore they must have confidence that any associated hazards are recognised at an early stage. […] Safety regulators need to be kept aware of the future and not just rely on what has worked well in the past. ASCOS needs to assist them by making assessments for currently unknown risks easier to incorporate into existing systems."
- R4: "The identification of new hazards is a very important aspect of a successfully implemented Safety Management System, requiring an administrative system for occurrence reporting as well as just culture within the organisation."

User expectation 1.8 "The ASCOS approach should explicitly consider human performance in a consistent and qualitative manner in overall safety assessments".

- R2: "The traditional approach seems to make significant assumptions about human performance and operation of the system. As such we are faced with sub optimal design of human interfaces and inadequate systems and processes for the human to deal with failures in automation."
- R5: "Notwithstanding this good objective, it must be noted that the present (aircraft) airworthiness and operational requirements contain specific Human Factors oriented paragraphs (e.g. CS25.1301, 1302, 1309, 1523). It should also be noted that "intended function" is a design consideration involving the option for distributing sub-functions between automation and human operators (.1301, .1523). In achieving the required performance (even separate from the requirements emanating from Airworthiness consideration, such as the recent .1302), it means that the human factor will be explicitly acknowledged and addressed in order to meet the overall performance expectation".

User expectation 2 "The ASCOS approach towards certification, including the developed supporting processes, tools and databases, should offer improvements for continuous safety monitoring […]."

- R2: "The process needs to ensure the ability for in service monitoring to validate safety case assumptions and predictions, such that the risks can be updated and addressed appropriately. The safety case needs to be a living document."

User expectation 3 "The ASCOS approach towards certification, including the developed supporting processes, safety assessment methodology, risk models and tools for risk assessment and safety based design risk, should offer improvement for certification activities".

- R4: In the context of the need for RPAS regulations "currently, the international thinking is that a safety assessment, both for operations and for airworthiness, are vital tools to ensure safe operations. So any develop or improvement in this area is greatly supported. Furthermore, the methodology should be applicable to the total aviation system, not just the airworthiness certification."

User expectation 3.1 "The ASCOS approach should enable safety based design of technologies, operations, and systems, which includes: a) An approach for the setting of safety targets, safety objectives and safety requirements to be used in design; b) The evaluation of risk relative to a required safety performance level; c) […]; d) […]."

- R5: "An approach that helps in setting safety targets, objectives and requirements to different domains of the aviation systems for design and certification would be helpful. ASCOS needs to assist in developing the "system of systems" safety argument, including the breakdown and allocation of the safety target/requirement to the different (functional) domains or stakeholders. ASCOS proposed solutions should encourage to start with a decomposition of functions, identification of hazards and consequences from a "system of systems" perspective."

User expectation 4 "The ASCOS approach towards certification, including the developed supporting processes, tools and guidance material, should receive willingness of the stakeholders to adopt the new approach and to put it into practice".

- R2: "If the ASCOS approach cannot be self-evident as a better way of doing things then there is no hope of success. It is essential that the methodology and demonstrable outputs make sense to both safety experts in the traditional certification approach, as well as aviation generalists. It will fail if it is only understood by PHD graduates!"

User expectation 4.2 "The ASCOS approach should reduce the required level of expertise and experience, maintaining an equivalent or better level of safety compared to the current practise."

- R3: "May have to be careful this doesn't lead to downgrading roles which may have implications elsewhere."
- R4: "Strongly oppose against wording of 'reduce the required level of expertise and experience'. This would indicate a worse level of safety to me. It would be better to mention that expertise and experience are required in a different area of knowledge than the currently required knowledge."