Evaluation of certification case studies

A.L.C. Roelen, R. Wever, (NLR), S. Rozzi, L. Save (Deep Blue), S. Bull (Ebeni)

This document describes the evaluation of the four certification case studies conducted in ASCOS WP4. The evaluation focussed on the proposed ASCOS certification approach, the continuous safety monitoring process and tool, the tool for safety risk assessment, and the Area of Change (AoC) list from the Future Aviation Safety Team (FAST). This evaluation considered an outline of the ASCOS certification approach. ASCOS will subsequently deliver a consolidated, final version of the certification approach taking into account, amongst others, recommendations from this evaluation.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	A.L.C. Roelen (NLR)

Grant Agreement No.	314299
Document Identification	D4.5
Status	Approved
Version	1.1
Date of Issue	29-06-2015
Classification	Public

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	Roelen et al	12-05-2015	All	Version for approval by PMT
1.1	Roelen et al	29-06-2015		Comments PMT processed

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	P.J. van der Geest	04-06-2015
APSYS	S. Bravo Munoz	04-06-2015
CAAi	A. Eaton	04-06-2015
Ebeni	A. Simpson	04-06-2015
TR6	B. Pauly	29-06-2015
Avanssa	N. Aghdassi	29-06-2015
CertiFlyer	G. Temme, M. Heiligers	29-06-2015
Organisation Responsible for Approval	Name of person approving the document	Date
NLR	A.L.C. Roelen	04-06-2015
NLR	L.J.P. Speijker	30-06-2015

Document Distribution

Organisation	Names
European Commission	M. Kyriakopoulos
NLR	L. Speijker, A. Rutten, M.A. Piers, P. van der Geest, A. Roelen, 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, S. Rozzi
JRC	W. Post
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
AARS	Automatic Aircraft Recovery System
AFMS	Automated Failure Management System
AIM	Accident Incident Model
AMC	Acceptable Means of Compliance
AoC	Areas of Change
ARP	Aerospace Recommended Practice
ASCOS	Aviation Safety and Certification of new Operations and Systems
ATC	Air Traffic Control
ATM	Air Traffic Management
CAA	Civil Aviation Authority
CBR	Compliance based regulations
CS	Certification Specification
CSM	Continuous Safety Monitoring
D	Deliverable
DAL	Development Assurance Level
EASA	European Aviation Safety Agency
EC	European Commission
ECCAIRS	European Coordination Centre for Accident and Incident Reporting
ED	Eurocae Document
E-OCVM	European Operational Concept Validation Methodology
ESD	Event Sequence Diagram
FAST	Future Aviation Safety Team
FHA	Functional Hazard Assessment
FRAM	Functional Resonance Accident Model
FT	Fault tree
ICAO	International Civil Aviation Organisation
IRP	Integrated Risk Picture
ISS	Integrated Surveillance System
KPA	Key Performance Area

OEM	Original Equipment Manufacturer
PBR	Performance based regulations
PSSA	Preliminary System Safety Assessment
R&D	Research and Development
RPAS	Remotely Piloted Aircraft System
SESAR	Single European Sky ATM Research
SMS	Safety Management System
SPI	Safety Performance Indicator
STAMP	Systems-Theoretic Accident Model and Processes
SWAL	Software assurance level
TAS	Total Aviation System
WP	Work Package

This page is intentionally left blank

Executive Summary

This document describes the evaluation of the four case studies that were conducted in ASCOS WP4. The evaluation focussed on the initial proposed ASCOS certification approach (as described in ASCOS D1.3), the continuous safety monitoring process and tool, the tool for safety risk assessment, and the Area of Change (AoC) list from the Future Aviation Safety Team (FAST). This evaluation considered an outline of the ASCOS certification approach, while ASCOS WP 1.5 will deliver subsequently a consolidated, final version of the certification approach taking into account, amongst others, the recommendations from this evaluation.

The case studies involve the following topics:

- D4.1: Automated Failure Management System (AFMS) installed on a Remotely Piloted Aircraft System (RPAS). The AFMS function is to detect and react to failures of the RPAS and to respond autonomously to these failures as best as possible (e.g. using reconfiguration of the systems on the aircraft where appropriate), with the intention to remain on the original intended flight path. In case of a failure, the AFMS replaces the pilot in the management of failures, reconfiguration of system(s), and the continuous monitoring, decision making and surveillance tasks normally performed by a pilot. [6]

- D4.2: The (initial) development of an Automatic Aircraft Recovery System (AARS) intended to reduce the number of Loss of Control accidents. The function of such system is to restore automatically the aircraft from any potential upset or any other deviation from a normal control regime, after an unexpected system failure or any other flight disturbing event, to a stable flight condition, within the normal flight envelope of the aircraft, and maintain this situation for a sufficient period of time to diagnose the potential problem and to restore situational awareness. Currently, such a system does not exist for civil aircraft and no specific certification requirements have been specified, as yet. [7]

- D4.3: The certification of a de-icing/anti-icing service provider. Currently, such service providers operate under the Air Operator's Certificate of the air operator they are part of, and/ or the air operators to which they provide their services. This case study assumes a situation in which this is no longer the case, and in which the de-icing/anti-icing service provider is responsible and accountable for their safe operations in compliance with assumed novel regulations. [8]

- D4.4: The certification of an Integrated Surveillance System (ISS) consisting of cooperative surveillance and independent non-cooperative surveillance systems. The ISS provides the ATC surveillance function as a primary means of surveillance, replacing (by attrition) the current primary and secondary radar systems. The ISS consist of two components: a cooperative surveillance system with a distributed, independent Wide Area Multilateration and aircraft dependent ADS-B. The second component is an independent non-cooperative Surveillance system of a network of “small” Multi-Static Primary Surveillance Radar to mitigate failures of the cooperative surveillance system. [9]

The evaluation of the case studies is based on an analysis from three angles. Firstly, the application of the certification approach and tools, the experienced benefits, lessons learned, conclusions and recommendations from the four case studies were analysed at an aggregate level to formulate conclusions and recommendations regarding the ASCOS certification approach and supporting tools. Secondly, the four case studies were reviewed against the performance framework that defines Key Performance Areas (KPAs) for the ASCOS approach to evaluate the 'fitness for purpose' of the certification approach. Thirdly, the case studies were reviewed from a 'verification perspective' against a set of 'design' principles that was considered in the development of the certification approach. The aim was to evaluate the efficacy of the ASCOS approach and how it could be improved, rather than as a scoring mechanism for the quality of the case studies. The recommendations in this report are addressed to the ASCOS project on the one hand, and EASA and the European Commission (EC) on the other hand. The recommendations to "ASCOS" will be taken up by the ASCOS WP1.5 as feedback for development of the final version of the ASCOS certification approach.

The ASCOS certification approach

The ASCOS certification approach is applicable and beneficial in the light of a performance based approach to certification. The aviation industry is moving towards the introduction of performance based regulations, which can only be successful if the certification approaches are adapted to this new environment. The ASCOS certification approach provides added value because it considers the Total Aviation System (TAS) from the start of design/certification activities and covers the entire lifecycle. Additionally, the coordination and sharing of safety requirements between stakeholders and across domains is one of the key characteristics and main benefits of the ASCOS approach. Safety benefits may be anticipated by using an approach that takes into account the TAS. However, these benefits will require early involvement of all stakeholders and authorities from all aviation domains. This will add complexity to the initial phase of the design and certification process, and involves increased management and communication as compared to the current way of working.

The ASCOS certification approach is a suitable approach if there is a clearly defined change in the operation, e.g. in the ATM, airport or airline operation, in the context of performance based regulations. The application of the ASCOS certification approach in the current, mainly compliance-based certification framework introduces additional complexity as a result of the logical argument framework, and provides consequently – for compliance based certification – little to no benefits.

The set-up of the logical argument structure can provide the certification basis in a performance based regulatory framework. However, the set-up of the argument structure itself can be a complex and laborious task, especially for novices. Application of a logical argument framework requires appropriate guidance material, which is not yet sufficiently available. In a performance based regulatory framework the argument structure may be worth the effort. However, it is questionable if this benefit will materialize for a practical case and if it is worth the additional effort, especially in the context of a compliance based regulatory framework and/or in a domain such as aircraft system certification which applies well developed certification practices.

Sixteen recommendations are made to ASCOS concerning mainly the improvement of guidance material on the application of the certification approach. Two recommendations are made to the EC and EASA about

safety target setting for the TAS and its distribution across domains, and the acceptability of the TAS level risk and net safety effect of the introduction of a change in the TAS.

The tool for continuous safety monitoring

The tool for continuous safety monitoring was not applied by the case studies, because these focused on the definition, design and specification of proposed changes in the TAS while the tool is initially developed for *monitoring*, i.e. use after proposed change(s) are approved, implemented and transferred into operation). Hence, from ASCOS WP4 there is no hands-on experience and feedback available about the application and benefit of the tool. Nevertheless, two recommendations to ASCOS are provided. One is about developing guidance material that explains the added value and differences of this tool compared to the tool for risk assessment. The second recommendation concerns the development guidance material and suggestions for use of the tool in stages of the ASCOS approach.

The tool for safety risk assessment

The ASCOS tool for safety risk assessment can support safety assessment activities in the context of certification. The tool was applied by two case studies for a safety effect assessment and a safety target allocation. The tool supports the TAS approach and a safety effect assessment of a change or subject of certification. It also helps to define relevant accident scenarios for the subject of certification. The tool can be applied during the hazard identification process as means to perform a cross-check whether all relevant types of accident scenarios and hazards have been covered. In the context of performance based regulations, the tool and risk model can support safety objective or safety requirement allocation to domains and stakeholders provided that the format of the safety performance target is in the form of an accident, incident or failure probability target. Two recommendations to ASCOS are made about further risk model and tool development, and two recommendations concern the development of guidance material by ASCOS to explain the use of the tool in the stages of the approach, and how the tool can be used to identify and allocate safety requirements.

The FAST AoC list

Three case studies applied the FAST Areas of Change (AoC) list as part of the certification approach stages. It is concluded that the FAST AoC list is helpful in defining the future environment as part of the description of the certification case in the context of the TAS. Furthermore, the FAST AoC list can be used as a source for hazard identification. However, it takes significant effort to assess all possible AoCs for the certification of a certain change. Another issue is that the FAST AoC list includes generally high-level, TAS related changes which may be difficult to “translate” to a specific, low-level change in a domain. One recommendation to ASCOS and three recommendations to FAST are made to improve the application of the FAST AoC list as part of the ASCOS certification approach stages.

The evaluation of the ASCOS certification approach against Key Performance Areas (KPAs)

The evaluation of the case studies against the seven KPAs concluded that the ASCOS certification approach has clear potential in the areas Soundness (KPA 2), Cross-domain integration (KPA 3) and Harmonization (KPA 4), in

a compliance and performance based regulatory environment. The contribution of the ASCOS certification approach to the KPA Efficiency (KPA 1), Accommodation of innovation (KPA 5) and Flexibility (KPA 7) is rated as high in a performance based regulatory context. In the context of a compliance based regulatory environment the ASCOS contribution to KPAs Efficiency and Flexibility is rated low, and for KPA Accommodation of innovation it scores neutral. The KPA Acceptability (KPA 6) was not rated because it was not possible to form an informative judgement about the potential contribution of the ASCOS approach to this KPA based on the case studies alone. Three recommendations to ASCOS are made regarding further development of guidance material to improve the ASCOS performance in areas Cross-domain integration, Acceptability, and Flexibility.

'Verification' of the ASCOS certification approach against 'design requirements'

A set of 'design requirements', considered by ASCOS WP1 in the development of the initial proposed certification approach, was used to formulate 'verification' questions. The questions were used to explore the efficacy of the ASCOS approach, and how it could be improved, rather than as a "scoring mechanism" for the (quality of) case studies. The case studies demonstrated that the ASCOS approach is capable of considering impacts on the TAS and that safety issues at the interfaces between the domains can be identified, but the extent to which they are fully captured and managed is unclear from the case studies. Addressing the TAS early in the design cycle may result in lower cost in the end, but this hypothesis could not be tested during the case studies. These benefits will be achieved at the cost of added complexity to the initial design and certification process and increased management and communication, as compared to the current process, in the early stages of the certification process. In a performance based regulatory approach, the ASCOS approach may have other benefits but this could not be verified in the case studies. The review also identified some issues related to safety target setting, safety requirement allocation and risk acceptability across the TAS that need to be resolved by the regulator(s). One recommendation is made to EASA and national CAAs on consistent application of safety across TAS domains. Three recommendations are made to ASCOS on clarification and consistency of terminology.

This page is intentionally left blank

Table of Contents

List of Tables

This page is intentionally left blank

1 Introduction

1.1 Background

The ASCOS project aims to outline a newly proposed approach to certification that is more flexible and more efficient than the current certification processes, and that considers the impact on safety of all elements of the Total Aviation System (TAS) and the entire system lifecycle in a complete and integrated way. ASCOS D1.3 [1] proposed an outline certification approach, while a number of other ASCOS documents describe associated supporting safety methodologies and tools for this certification approach [2, 3, 4, 5, 13]. Note that the ASCOS WP1.5 will update the ASCOS certification approach defined in D1.3, taking into account feedback from the evaluation and validation activities.

The objective of WP4 in the ASCOS project is to apply the proposed certification approach and supporting tools to four certification case studies in order to evaluate the feasibility of the practical application, and to collect feedback of the experience with the application and benefits of the certification methodology in the case studies. The case studies involve the following topics:

- D4.1: Automated Failure Management System (AFMS) installed on a Remotely Piloted Aircraft System (RPAS). The AFMS function is to detect and react to failures of the RPAS and to respond autonomously to these failures as best as possible (e.g. using reconfiguration of the systems on the aircraft where appropriate), with the intention to remain on the original intended flight path. In case of a failure, the AFMS replaces the pilot in the management of failures, reconfiguration of system(s), and the continuous monitoring, decision making and surveillance tasks normally performed by a pilot. [6]
- D4.2: The (initial) development of an Automatic Aircraft Recovery System (AARS) intended to reduce the number of Loss of Control accidents. The function of such system is to restore automatically the aircraft from any potential upset or any other deviation from a normal control regime, after an unexpected system failure or any other flight disturbing event, to a stable flight condition, within the normal flight envelope of the aircraft, and maintain this situation for a sufficient period of time to diagnose the potential problem and to restore situational awareness. Currently, such a system does not exist for civil aircraft and no specific certification requirements have been specified, as yet. [7]
- D4.3: The certification of a de-icing/anti-icing service provider. Currently, such service providers operate under the Air Operator's Certificate of the air operator they are part of, and/ or the air operators to which they provide their services. This case study assumes a situation in which this is no longer the case, and in which the de-icing/anti-icing service provider is responsible and accountable for their safe operations in compliance with assumed novel regulations. [8]
- D4.4: The certification of an Integrated Surveillance System (ISS) consisting of cooperative surveillance and independent non-cooperative surveillance systems. The ISS provides the ATC surveillance function as a primary means of surveillance, replacing (by attrition) the current primary and secondary radar systems. The ISS consist of two components: a cooperative surveillance system with a distributed, independent Wide Area Multilateration and aircraft dependent ADS-B. The second

component is an independent non-cooperative Surveillance system of a network of "small" Multi-Static Primary Surveillance Radar to mitigate failures of the cooperative surveillance system. [9]

The proposed outline of the ASCOS certification approach in D1.3 consists of the following stages:

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 approach and stages are further explained in Appendix A.

1.2 Objective and scope

This ASCOS D4.5 document describes the evaluation of the four certification case studies. The evaluation will focus on the ASCOS approach described in D1.3 [1] and the supporting tools:

- the continuous safety monitoring process and tool from WP2 [3, 13], see Appendix B;
- the tool for safety risk assessment from WP3 [4, 10], see Appendix C; and
- the Area of Change list from FAST [5].

The evaluation aims to assess the application of the certification approach and tools, the experienced benefits, lessons learned, conclusions and recommendations from the four case studies. The evaluation considers similarities and differences between the experienced issues, lessons learned and recommendations in the case studies. As a result of the evaluation recommendations for the application and improvement of the ASCOS certification approach and supporting tools are provided. The recommendations are addressed to the ASCOS project on the one hand, and EASA and the EC on the other hand. Note that the ASCOS WP 1.5 will be considering the recommendations to "ASCOS" in this report as input for the consolidation of the revised, final version of the ASCOS certification approach.

Recommendations about the proposed certification approach and supporting tools is described in boxes.

The evaluation of the certification case studies is complementary to the WP5 validation activities. While WP4.5 collects feedback from the actual application of the ASCOS approach in the case studies, WP5 collects feedback from validation exercises that were dedicated to validate ASCOS results against stakeholders' expectations and needs, and not in the context of a particular case study.

1.3 Approach

The evaluation of the proposed ASCOS certification approach and supporting tools is based on a review and analysis from three angles:

1. from the experience and feedback while applying them in the case studies;
2. from the review of the case studies against the performance framework; and
3. from a 'verification' perspective (i.e. does the approach meet the design requirements?).

Experience and feedback from the case studies

The collection of observations, conclusions, and recommendations from the four case studies is analysed at an aggregate level to formulate conclusions and recommendations regarding the ASCOS certification approach and supporting tools. In the review and the analysis of the case studies three aspects are covered:

- The application of the certification approach and supporting tools in the case studies. In case (parts of) the certification approach and supporting tools were not applied in a case study, the reason for doing so is analysed.
- Benefits from the application of the certification approach and supporting tools in case studies. In case (parts of) the certification approach and supporting tools did not deliver benefits, the reasons for that are analysed.
- Recommendations and potential areas for improvement.

Review of the case studies against the performance framework

The four case studies are reviewed against the performance framework that defines key performance areas (KPAs) and key performance indicators (KPIs) for the validation of the ASCOS certification approach (see D5.1 [12] and D5.3 [24]). These KPAs and KPIs are based on user needs and expectations. The application of and experience with the ASCOS certification approach in the four case studies is analysed against the KPAs to evaluate the "fitness for purpose" of the certification approach. The evaluation based on the case studies is complementary to the results obtained in the validation exercises that were conducted as part of WP5. In the validation exercises the ASCOS approach is evaluated "stand-alone" by ASCOS User Group members, whereas in WP4.5 the specific case studies provide additional insight in how well the ASCOS certification approach performs in the defined KPAs.

Review of the case studies from a verification perspective

Verification in this case is a two-step approach. Due to the absence of design requirements these have to be developed first. The second step is to evaluate (verify) to what extent the ASCOS certification approach meets these requirements. The deliverable D1.2 [23] proposed a set of principles to be considered in the development of the certification approach. Taking these principles as 'design requirements', the case studies are reviewed against these principles to evaluate the efficacy of the ASCOS approach and how it could be improved, rather than as a "scoring mechanism" for the quality of the case studies.

1.4 Document structure

The document is organised as follows. Chapter 2 describes the results of the evaluation of the ASCOS certification approach applied by the case studies, covering the application, benefits, conclusions and recommendations. The subsequent three chapters address the evaluation of respectively the tool for continuous safety monitoring (Chapter 3), the tool for safety risk management (Chapter 4), and the FAST AoC list (Chapter 5). Chapter 6 describes the results of the evaluation of the ASCOS certification approach as applied in the case studies against the KPAs framework. Chapter 7 describes the 'verification' of the ASCOS certification approach against 'design requirements'.

2 Evaluation of the ASCOS certification approach

2.1 Application

2.1.1 Scope of application in case studies

The ASCOS certification approach consists of an eleven stages process (see section 1.1 and Appendix A). The stages 1 to 4 were applied in all case studies, while case study D4.2 and D4.3 applied stage 5 as well, and D4.1 applied stages 1 to 6. Initial ASCOS briefing material on stage 4 and 5 was used by D4.2 [15] and D4.3 [14, 15]. The stages 6 to 11 are out of scope of the ASCOS research activities and would require follow-up activities in order to bring the proposed products and services into operational use.

2.1.2 Application of Stages 1 to 3

Stage 1 (Definition of the change)

All case studies found it difficult to define the change at the appropriate functional level. In particular, case study D4.3 (certification of a de-icing/anti-icing service provider) experienced trouble in defining the scope and approach for stage 1, which may be due to the type of change (procedural as opposed to an introduction of a system) and lack of guidance material. The definition of the change and its scope, the definition of the (assumed) regulations to be used as certification basis, and the definition of the applicable safety target were difficult to perform in D4.3. Especially when the subject of certification and certification argument include multiple stakeholders with different roles and responsibilities, it is not straightforward to conduct stage 1.

Stage 2 (Definition of the safety argument)

Stage 2 was a complex and laborious task for all case studies. For the (top-level) logical argument structure all case studies made use of the template provided in the D1.3. All case studies developed a logical argument structure for Claim 1 (Change X is specified such that is will achieve an acceptable level of safety) with sub-claims. The case study D4.4 developed an argument structure for Claim 1 divided into sub-claims by flight phase, which was not done by the other case studies.

Only case study D4.1 decomposed Claim 2 (Logical design of the change satisfies the specification and is realistic) into sub claims. Cases D4.2 and D4.4 described how the evidence would be delivered to demonstrate Claim 2. In particular case study D4.3 struggled with a meaningful decomposition of the Claim 2 due to the nature of the case. Note that Claims 3, 4, and 5 were considered outside the scope of the case studies.

The application of the logical argument approach, especially the definition and breakdown of claims, was considered difficult to understand and perform. The case studies struggled in the scoping and development of the argument structure for many reasons including the character of case studies, the limited experience of

team members in the D1.3 approach and logical argument structure approach, and the limited guidance material. The D1.3 guidance material and vocabulary were not easy to understand, especially for non-experts. Also, presenting the logical argument approach to non-experts revealed that it was not intuitive to understand.

It was found difficult to develop high level claims in meaningful sub-level claims. The argument structure has a high-level character, whereas the cases are dealing with specific, lower-level certification activities which were difficult to match with the high level structure. The case study teams are familiar with the current practice in their domains and are generally working at a detailed level, e.g. conducting FHA and PSSA, developing performance specifications, assigning SWALs, etc.

The definition of the applicable safety targets, or safety objectives, and the definition of the top level claim (Claim 0, “change X is acceptably safe”) caused some discussion in the case studies. The allocation of a target level of safety for the TAS and handling different safety targets in different domains emerged from the case studies as two issues that need to be addressed (see section 2.3). Case study D4.2 provides an example where the definition of safety objectives in different domains (aircraft system certification and ATM) may lead to different probability requirements for similar hazard categories. Agreement by stakeholders on the process for defining and allocating TAS level safety objectives is a prerequisite for the application of the ASCOS approach (see recommendations in section 2.3).

For case studies D4.1 and D4.2 existing regulations and standards provided qualitative and/or quantitative safety targets (safety objectives). The D4.3 case applied the tool for risk assessment to define a quantitative safety objective, as there was no safety objective available in current regulations/standards. The tool for safety risk assessment or continuous safety monitoring was not applied by the other case studies to assess the current risk level as a basis for a target level of safety. The D4.4 case referred to safety criteria from a previous study.

Stage 3 (Develop and agree safety plan)

All case studies conducted stage 3 and delivered an initial certification plan without noteworthy issues. However, these plans cannot be regarded as representative plans of an actual certification as the case studies did not fully address issues like (a) how collaboration between different stakeholders (applicants and authorities) would be achieved, (b) which parts of the argument would be delivered by each applicant, and (c) which parts of the argument would be accepted by each authority. In addition, some case studies identified that multiple plans would be needed either at different stages or different levels.

2.1.3 Application of Stage 4 (Specification) and Stage 5 (Design)

Conducting these stages appeared relatively straightforward for the three case studies related to the introduction of a system (D4.1, D4.2, D4.4), using different, existing approaches and safety assessment techniques to build the evidence for Claim 2. Case D4.3 experienced more issues in the execution of stages 4 and 5, mainly due to the nature of the change and a lack of existing standards. The scope, depth and rigor of the safety assessments performed in each case study in stages 4 and 5 are diverse which is partly due to the topic of the case studies, the team's experience in the approach, resources, and availability of suitable guidance material from current regulations/standards or from the ASCOS project.

The case study D4.1 identified hazards in different domains, assigned severity levels and derived qualitative and quantitative safety requirements using existing regulatory guidance material (e.g. JARUS [21], ARP4754/ED78A [16]) for severity levels and safety objectives. The specified safety objectives include a reference to Development Assurance Levels, and safety requirements were derived from normal, abnormal and failure scenarios. The case study had a problem with allocating quantitative requirements to human related hazards as regulations do not address this issue today. The study suggested the use of Human Development Assurance Levels as a potential way to address this.

In D4.2 a common Functional Hazards Assessment (FHA) was conducted as part of stage 4, followed by a 5-step assessment in stage 5 in accordance with an ASCOS briefing guide [17]. The case study used CS25.1309 [22] for the definition of severity categories and safety objectives in this FHA.

While D4.1 and D4.2 could make use of existing guidance material such as ARP4754 [16], CS25 [22], and the common FHA process, the case study D4.3 did not have such reference material. The D4.3 case used ASCOS guidance material (briefing guide [14], [15]) that defines safety assessment steps for stages 4 and 5. The briefing guide [14] was specifically developed for D4.3 and not applied by other case studies. The D4.3 case study was able to apply stage 4 with suggestions for improvement in the briefing guide. The execution of stage 5 revealed a few issues that are the result of the fact that guidance material describes a system design oriented approach, which is less appropriate for application to operations or organisational changes.

D4.4 applied stage 4 in an exploratory nature only, using results from a previous safety assessment instead of executing stage 4 for the particular case study from scratch. The application of stage 4 did not identify any noteworthy issues. Stage 5 was not applied due to the fact that a logical design for the Integrated Surveillance System was not available and could not be developed within the scope of the ASCOS project. Given that stage 4 is of an exploratory nature and stage 5 is lacking in this case study, there is limited information to assess the application and benefits of stages 4 and 5.

2.2 Benefits

2.2.1 Benefits of Stages 1 to 3

The main advantage of the ASCOS certification approach is that it addresses the Total Aviation System (TAS) from the start. The ASCOS approach was considered helpful for all case studies to identify domains and stakeholders that should be involved in the case. Early identification of stakeholders and having a process for properly sharing safety requirements across domains are added value compared to the current practice. The application of a logical argument structure, as an alternative for a traditional certification basis, seems attractive from a theoretical viewpoint and provides a logic structure for the certification process.

The development of a complete and consistent logical argument structure that logically builds up a collection of claims and sub-claims to an appropriate level for demonstrating that the top level claim is satisfied, is a laborious and complex task. It is expected that a proper argument structure might be – in theory – beneficial from a safety viewpoint, as it explicitly addresses the required safety level, as opposed to current certification approaches that are more implicit. In a performance based regulatory framework the argument structure may be worth the effort to structure the certification argument and to establish the certification basis. However, it is questionable if this benefit will materialize for a practical case and if it is worth the additional effort, especially in the context of a compliance based regulatory framework and/or in a domain such as aircraft system certification which applies well developed certification practices. For example, the added value of the logical argument structure was not clear in case studies D4.2 and D4.3. In both case studies the lower claims are not very different from the higher claims after the decomposition of the claims, while for example stages 4 and 5 of the certification approach were conducted without being clearly driven by the developed argument.

2.2.2 Benefits of Stage 4 (Specification) and Stage 5 (Design)

Safety benefits may be anticipated by using an approach that takes into account the Total Aviation System. It leads to early identification of potential negative safety consequences in other domains which can thus be mitigated as part of the basic design. However, these benefits will be achieved at some costs, namely early involvement of all stakeholders and authorities from all aviation domains. This will add complexity to the initial design and certification process and requires an increased management and communication burden. Most likely also organisational adaptations are required to ensure that responsibilities and safety objectives or requirements are properly distributed.

One of the consequences of the TAS approach is that safety benefits may be identified in one domain while there are safety reductions in another domain. It is unclear whether the top-level argument is indeed satisfied if the net effect is positive, or whether it is only satisfied under the condition that local safety reductions are not allowed. The current guidance material does not specify how to deal with such a situation. In fact, the EC and EASA need to provide guidance as it is not within the scope of ASCOS to resolve this issue.

From D4.3 it is concluded that the D1.3 approach appears to deliver limited added value in support of certification of a service provider, especially when the main complexities of certifying such a provider are of an organizational nature, with for example shifted responsibilities. The approach appeared to be rather 'heavy' when compared to the technical complexity of the subject of certification and was not scalable or flexible in that sense.

The current certification methodologies for aircraft systems are well established. Sufficient experience and guidance exist to efficiently certify novel systems such as the AARS in D4.2. Moreover, essential stages 4 and 5 of the new approach broadly align with existing FHA and PSSA methods, and therefore are not expected to provide substantial improvement to the current practice.

2.3 Conclusions and recommendations

This section provides conclusions and recommendations divided into the following topics:

- overall conclusions and recommendations (2.3.1);
- alignment of the ASCOS approach stages with the current certification process (2.3.2);
- stages 1 to 3 (0), including coordination across stakeholders and domains, defining an acceptable level of safety or a target level of safety across the TAS, and balancing safety effects across domains;
- stages 4 and 5 (2.3.4), including scope of stage 4 and 5 versus FHA and PSSA, hazard definition and identification, defining high level safety requirements and allocation and distribution of safety objectives /safety requirements.

2.3.1 Overall conclusions and recommendations

The ASCOS certification approach is applicable and beneficial in the light of a performance based approach to certification. The aviation industry is moving towards the introduction of performance based regulations, which can only be successful if the certification approaches are adapted to this new environment.

The ASCOS certification approach provides added value because it considers the Total Aviation System from the start of the design and certification activities, and covers the entire lifecycle. Additionally, the approach supports involvement of stakeholders, avoiding working in isolation, and supports sharing safety requirements between stakeholders across domains. The innovation of the ASCOS approach is that an overall top level claim of an acceptably safe change to the TAS is decomposed into supporting claims that are aligned with individual aviation domains, such that the approach dovetails with the individual certification approaches existing within those domains.

The ASCOS approach will be applicable in a performance based context to certification cases that relate to the execution of operations. The concept of 'performance' only makes sense in the context of some sort of

execution of operations. A performance level can be expected from operations, such as safety, environmental, financial, or efficiency performance. The top level claim represents a certain performance level that must be achieved. The applicant supports the top level claim with the sublevel claims. Note that if claims are qualitatively defined, meeting sub-claims will not guarantee a safe performance: If one satisfies lower level claims qualitatively, it does not guarantee that one meets the top level claim.

The application of the ASCOS certification approach in the current, mainly compliance-based certification framework introduces additional complexity as a result of the logical argument framework, and provides consequently – in compliance based framework – little to no benefits. The approach has limited value for aircraft system certification in a compliance based certification framework. The current process and approach in aircraft system development and certification is well developed and mature, with well-defined existing acceptable means of compliance. However in case the aircraft system certification would take place in the setting of performance based regulations, the ASCOS approach could be useful.

The ASCOS certification approach is a suitable approach if there is a clearly defined change in the operation, e.g. in the ATM, airport or airline operation, in the context of performance based regulations. The approach is not suitable if the certification case involves organisational responsibilities, organisations or for example the certification or approval of an organisation, Air Operator Certificate, certification of a maintenance or training organisation, flight crew licencing etc. Using a logical argument approach in these 'compliance based environments' is overly complex and may be impractical. The ASCOS approach seems more favourable for certification of aircraft systems, ATC systems and procedures than for the certification of organisations or management systems such as SMS.

Recommendation 01: It is recommended to ASCOS to develop guidance material explaining criteria for determining whether the ASCOS certification approach is suitable and efficient to apply to a particular certification case.

2.3.2 Alignment of the ASCOS approach stages with the current certification process

This section explains how the stages of the ASCOS certification approach can be related to the existing, established certification process for aircraft system certification. A compliance based certification process (basically) follows these four steps:

1. In the first step the applicant and authority reach agreement on the subject of certification, i.e. the function that is to be certified.
2. Next, the applicant and authority agree on the certification baseline, i.e. the certification requirements and standards with respect to the subject of certification.
3. The third step is to determine the acceptable means of compliance, i.e. the means the applicant is allowed to use to demonstrate that the subject of certification complies with the certification requirements and standards.

4. Finally, the applicant and authority need to agree that the evidence delivered by the applicant sufficiently and acceptably demonstrates that the subject of certification meets the certification requirements and standards. In fact, the authority needs to be convinced by the evidence delivered by the applicant.

The proposed ASCOS certification approach stages can be mapped upon these steps of the current certification practice as follows:

- Stage 1 in the ASCOS approach is similar to step 1 in the current certification process.
- Stage 2 in the ASCOS approach develops the (initial) certification argument structure, which needs to be submitted to the authority as a first version that will be updated during the following stages. This aligns with step 2 in the current practice. The logical argument structure forms the certification basis in the context of performance based certification. In theory, the applicant should receive the certificate once the top level claim in that logical argument structure is demonstrated in an acceptable manner. In stage 6 the final logical argument structure should be delivered by the applicant and agreed upon with the authority.
- Stage 3 considers the certification plan. This would be in practice a first version of a certification plan. As the specification and design stages follow subsequently, there will be a need to update the certification plan in stage 6 when more details on the actual functions and design solution of the end product or service will be known. It could be part of step 3 in the current certification process.
- Stage 4 should derive the safety performance level on a functional level. The focus should be on the functional analysis of the product of service, defining the functions without considering how they will be implemented. This relates to functions of systems, procedures, operations, and so on.
- Stage 5 should focus on hazard identification, risk assessment and mitigation. It includes the implementation of the functions in 'design'. It involves developing concepts for implementation of the function that will be evaluated before a final concept or design is selected. This stage defines requirements and preconditions. It concerns the identification of hazards and the mitigation of their risks, and for instance could include a Preliminary System Safety Assessment type of analysis.
- Stage 6 will refine the certification basis and update the certification plan. It mirrors step 3 in the current certification practice.
- Stage 7 in the ASCOS approach is similar to step 5 in the current certification process. Stage 7 will deliver a "system safety assessment" of the product or service that is to be certified, which needs to generate the evidence to convince the authority that the product or service meets the safety requirements.

Recommendation 02: It is recommended to ASCOS to include this section in guidance material to explain how the ASCOS approach stages align with the current (aircraft system) certification practice.

2.3.3 Conclusions and recommendations for Stages 1 to 3

Stage 1 (Definition of the change)

Recommendation 03: It is recommended to ASCOS to develop guidance material that helps the user to define the "change X" (i.e. Claim 0, in D1.3) and its scope or "boundaries". The definition of the change should cover technical, organizational, operational, procedure, environmental aspects. It should also identify all involved stakeholders, including those outside the TAS that may interact with the subject of certification. In this stage the applicant should collect information from all stakeholders how the change will impact them, and include this information in the definition of the change.

Stage 2 (Definition of the safety argument)

The set-up of the logical argument structure provides the certification basis in a performance based regulatory framework. However, the set-up of the argument structure itself can be a complex and laborious task, especially for novices. The approach is suitable for performance based certification domains such as the ATM domain, but less suitable for a compliance based regulatory environment such as in aircraft system certification with well-established certification practices and AMC.

Argument architects need to be specifically trained for the development of arguments. It is unclear how much of the (initial) effort to complete a case study would be reduced in future studies when the team builds up experience and develops a "learning curve" in the ASCOS approach.

Recommendation 04: It is recommended to ASCOS to provide an extensive explanation about the following topics with examples of logical argument structures in guidance material:

- The level of detail of the claims and sub-claims;
- The process that can be followed for decomposing the claims;
- How to address safety management requirements, and in which claim;
- How to reduce the effort or complexity of the logical argument structure;
- How to take into account whether associated regulations already exist, and how to do this;

Recommendation 05: It is recommended to ASCOS to change the nomenclature in the logical argument structure and to adapt the argument template(s) to make it generally applicable, including to the certification of organisations and operations. The D1.3 report on the ASCOS approach seems rather focused certification of a (system) change, whereas it should be broadly applicable. The case study D4.3 shows that it is more appropriate to focus on the 'subject of certification' or the 'scope of the certificate' rather than 'a change X' as D4.3 focuses on the certification of an organisation. It is recommended to change the definitions and explanation such that the approach focusses on the certification of the performance of a function (which can be fulfilled by an operation, procedure, system, etc.).

Recommendation 06: It is recommended to ASCOS to adapt the terminology used in the guidance material on the ASCOS certification approach so that it is understandable for a wide range of users and all domains.

Recommendation 07: It is recommended to ASCOS to provide guidance to stage 2 about the development of the argument decomposition, and on how to link the common, detailed certification activities to the high-level logical argument approach. Guidance material needs to explain what kind of decomposition of the claims could be followed for a change that is of an organisational nature rather than of a technical nature and what process can be followed to satisfy these Claims in such cases.

Coordination across stakeholders and domains

The coordination across stakeholders and domains is one of the key characteristics and main benefit of the ASCOS approach. The case studies all recommend to improve guidance on the process and organisation of this coordination and interaction between stakeholders as part of the D1.3 approach. It is currently not clear where, when and how coordination between stakeholders and domains needs to take place in stages 1 to 3. Especially if the subject of certification involves a significant number of stakeholders and domains (like in D4.2 and D4.3), it is unclear how the argument structure tackles such organisational complexity.

Recommendation 08: It is recommended to ASCOS to explain in guidance material how domains and stakeholders should work together and coordinate in the ASCOS certification approach and logical argument structure development. Guidelines should address:

- How to define all aspects of a change (e.g. operational, organisational, functional, and system description) in a way that takes all stakeholders into account;
- How to organise traceability of involvement of stakeholders in the different elements of the argument structure (e.g. in claims);
- How to develop and agree upon safety targets and risk criteria (e.g. severity levels, safety objectives definitions, risk matrices);
- How to develop and agree upon a process to allocate safety objectives or design requirements across stakeholders and domains.
- Where and when coordination between stakeholders and domains needs to take place. It should explain at which stage in the process the safety targets are to be defined, and who is responsible for the overall TAS safety target.
- How the logical argument structure should include the roles and responsibilities of different certifying authorities and stakeholders.

Recommendation 09: It is recommended to the EC to define which authority is responsible for safety across the TAS.

Defining an acceptable level of safety or a target level of safety across the TAS.

The ASCOS certification approach does not aim to replace or adapt the existing certification regimes in the individual aviation domains, but provides a structure to the certification of the change in the TAS. As such, the risk acceptance criteria or safety targets applied currently in safety assessments in the individual domains remain applicable. It is not a-priori evident that failure conditions with a given severity level are equally acceptable (in terms of frequency) within the various domains. The top-level claim of the argument structure is by definition that the "*the operation of … system achieves acceptable safety across the TAS*". By definition the specification of the acceptable level of safety is the responsibility of the certifying authority, and defining the acceptable level of safety across the TAS for Europe should be done by EASA.

Recommendation 10: It is recommended to ASCOS that guidance material explains how the argument structure should cover the issue of which authorities or regulators are involved and how to deal with a case where multiple regulators are involved. The guidelines should explain:

- How to identify applicable safety targets across stakeholders and domains;
- How to agree on a single safety target for the TAS that is acceptable to all domains and stakeholders, or how to handle different safety targets for different domains in a single argument structure;
- How to determine the contribution of each stakeholder to the safety objective, and how to properly allocate (share) safety requirements (e.g. what sort of "formula" can be used to distribute safety requirements);
- How the tool for safety risk assessment and tool for continuous monitoring can be used to determine the current risk level for the TAS and/or domains, which may be used as a basis to demonstrate an equivalent level of safety in case the regulations do not provide a specific safety target.

Balancing safety effects across domains

Within the ASCOS approach the situation may occur that a change brings positive safety effects in one domain and negative safety effects in another domain. It is unclear whether the top-level argument is indeed satisfied if the net effect is positive, or whether it is only satisfied under the condition that local safety reductions are not allowed. The current guidance material does not specify how to deal with such a situation. It is unclear whether the top-level argument is indeed satisfied if the net effect is positive, or whether it is only satisfied under the condition that local safety reductions are not allowed. The process, method and responsibility for assessing the acceptability of TAS-level risk and the net safety effect of a certification case on a TAS level needs to be defined as well.

Recommendation 11: It is recommended to ASCOS to explain in guidance material how the net safety effect can be determined and how the aforementioned situation can be addressed.

Recommendation 12: It is recommended to EC and EASA to develop a process and method to 1) allocate an overall TAS level safety target to domains and stakeholders in a performance based certification approach and 2) determine the acceptability of the net safety effect of the introduction of a certification subject or change in the TAS.

2.3.4 Conclusions and recommendations for Stage 4 and Stage 5

Scope of stage 4 and 5 versus FHA and PSSA

In the description of the ASCOS certification approach in D1.3 it is stated that stage 4 focuses on the behaviour of the changed system in the absence of failure. This statement appears to be incompatible with a statement in D1.3 that stage 4 broadly aligns with a FHA, and stage 5 with a PSSA. It is unclear how a functional hazard assessment process can be conducted without addressing functional failures of the system. The core of an FHA is to define the functions of the system (independent of implementation) and to derive the consequences of failure of these functions, in order to determine the criticality of the functions. The established function criticality drives the system safety requirements (in terms of integrity, reliability, accuracy, continuity of service, etc.). Only if these requirements are known a logical system design can be made (stage 5). Therefore the description in D1.3 seems to be lacking by restricting itself to focus on system behaviour in the absence of failures.

Recommendation 13: It is recommended to ASCOS that the description in D1.3 is updated to reflect the characteristics of the FHA. The added value of stages 4 and 5 would be increased if the approach is not focussed on mitigation of failure conditions or hazards, but also on achieving a certain performance level by the intended function and its design.

Hazard definition and identification

Speaking a common language is essential when the ASCOS approach aims to promote coordination and interaction between different stakeholders. The use of a common taxonomy for hazards, safety objective, severity levels, safety requirement etc. is recommended. The hazard definition and scope of hazards in stage 4 mentioned in D1.3 and briefing note [14] are ambiguous and need clarification.

Recommendation 14: It is recommended to ASCOS to define ‘hazard’ in guidance material using the wide definition of hazard, i.e. “any condition, event, or circumstance, which could introduce an accident” (refer to the ICAO Safety Management Manual).

Recommendation 15: It is recommended to ASCOS to explain in guidance material that in stage 4 sub-claims are specifically directed to hazards in the various domains across the TAS (e.g. flight technical, flight

operational and ATM) such that responsibilities for mitigating these hazards can be clearly assigned to specific stakeholders. The scope of the hazards that are dealt with in stage 4 should be clarified. It concerns:

- hazards which the subject of certification aims to mitigate,
- hazards that exist in in other domains while the subject of certification performs it normal functions.

Defining high level safety requirements

The FHA and PSSA are standard elements of existing design and certification processes and it is unclear how these processes can be consistently incorporated into the argument structure. The argument structure (at lower levels) may formulate sub-claims that are inherently addressed by FHA and PSSA processes. Interfacing the FHA and PSSA with the argument structure may be cumbersome. This also relates to the earlier comments that detailed certification activities need to be matched with the high-level claims structure through some "interface".

Recommendation 16: It is recommended to ASCOS to explain connecting common FHA and PSSA approaches to the logical argument structure. Furthermore, guidance material should define that the high level safety requirements need to be developed for all claims in the argument, and covers functions, operations, organisations, SMS etc.

Allocation and distribution of safety objectives/safety requirements

The 'governance' of the argument structure and the safety objectives amongst domains and stakeholders is an issue that arises in the case studies. In a performance based approach, where safety performance for a particular topic is delivered by different stakeholders together, it is essential to have a uniform, consistent process to allocate and share safety objectives and safety requirements.

Recommendation 17: It is recommended to ASCOS to provide guidance concerning the consistent application of safety objectives over the various domains of the Total Aviation System.

Recommendation 18: It is recommended to ASCOS that guidelines are developed to explain how a safety objective that is supported or "delivered" by different stakeholders can be allocated or "shared" across stakeholders. It is remarked that two case studies mentioned that besides safety requirements, requirements related to quality, integrity, availability, continuity, performance etc. for all types of functions could be shared between stakeholders (in and outside the TAS).

3 Evaluation of the tool for continuous safety monitoring

3.1 Application

The ASCOS tool for continuous safety monitoring has been developed to facilitate the continuous monitoring of safety performance. The tool provides statistics and trend information (e.g. tables and charts) based on reported occurrence data extracted from an ECCAIRS compatible data repository and exposure data. The safety performance is monitored using predefined or user-defined safety performance indicators.

The tool for continuous safety monitoring, described in D2.4 [3] and Appendix B, may be useful in a priori and a posteriori risk assessment according to the guidance in D1.3 [1]. The D1.3 report mentions: "The data generated by the Continuous Safety Monitoring (CSM) support a priori risk assessments by providing (predictive) quantifications of the probability and/or frequency of occurrence of events within the system, supporting the overall estimation of risk required to demonstrate that the system is capable of meeting the safety requirements derived during development of the safety argument. This includes using the data to support any quantified assumptions about how the system will behave. […] The CSM process supports a posteriori risk assessments by establishing the framework for collecting data. As part of Cl 5 for a specific change, specific metrics (SPIs) will be identified to monitor the safety in service of the change. Some of the required metrics will already be defined within the overall CSM scheme defined in WP2. It is necessary for the CSM process to be sufficiently flexible to allow additional metrics to be added where necessary to support the safety monitoring required to fulfil Cl 5 for a specific change."

The scope of the case studies was limited to stages 1 to 4/5/6 of the ASCOS certification approach and does not include stage 9 that deals with arrangements for continuous safety monitoring, or stage 11 about ongoing monitoring and maintenance of certification. Consequently, the continuous safety monitoring tool was not applied by the case studies. Although the D1.3 report explains that the tool can be used as part of the a priori risk assessment, the case studies did not apply the tool as they believed it was to be used in later stages of the certification approach.

3.2 Benefit

Since the case studies did not apply the tool, there is no hands-on experience and feedback available about the benefit of the tool. The WP leaders of the case studies were interviewed to collect their recommendations about the potential use of the tool and expected benefits for their case studies if they would have applied the tool. This information in included in the next sections.

3.3 Conclusions and recommendations

This section provides conclusions and recommendations on the possible applications of the tool for continuous safety monitoring, divided into the following topics: naming of the tool (3.3.1), use in the stages of the ASCOS certification approach (3.3.2), and the relation between the tool for continuous safety monitoring and the tool for safety risk assessment (3.3.3).

3.3.1 Naming of the tool

The naming of the tool "for continuous safety monitoring" suggests that is can be used for continuous safety monitoring only, i.e. stage 9 or 11 of the D1.3 approach. It may be confusing that the tool for continuous safety monitoring may also be applied in support of a risk assessment, besides the tool for safety risk assessment.

Recommendation 19: It is recommended to ASCOS to explain in guidance material the "power" of the current tools for continuous safety monitoring and safety risk assessment, their differences and similarities.

3.3.2 Use of the tool in the stages of the ASCOS certification approach

Recommendation 20: It is recommended to ASCOS to address in guidance material the following potential applications of the continuous safety monitoring tool within the 11 stages of the certification approach.

- Stage 1 (Definition of the change)
  The tool can be used to derive the current safety performance in areas that are relevant for the change. As a result the applicant is made aware of the actual safety performance in the TAS in the domain(s) of interest. These data may be used to define the current risk level as a basis for safety target setting as part of the argument structure that defines the applicable safety criteria in stage 2. It may also be used to assess the potential safety impact of the change in the TAS.

- Stage 2 (Define the certification argument) and stage 3 (Development of certification plan)
  In the development of Claim 5, "The service(s) introduced by change X will continue to be demonstrated as acceptably safe in operational service", the tool and supporting SPI framework can be used to define the SPIs that need to be monitored to ensure continuous monitoring and feedback on the safety performance of the approved "change" or certification case.

- Stage 4 (Specification) and stage 5 (Design)
  The tool for continuous safety monitoring can provide accident/incident statistics, complementary to the data from the tool for safety risk assessment. These data may for example provide input to the Fault Tree analysis of an applicant. However, it remains to be seen whether the current maturity level, completeness, reliability of the ECCAIRS dataset is sufficient to use these data to adapt the quantification of the ESDs and FTs in the ASCOS risk model in the tool for risk assessment. Note that

the OEMs get operational data directly from the end-users, and not through ECCAIRS. ECCAIRS may be just one of the many data sources that needs to be considered to collect operational (safety) feedback for stage 4 and 5.

- Stage 9 (Define arrangements for continuous safety monitoring)
  The tool can be used to identify existing SPIs, to assess the feasibility of new SPIs specific for the certification case, and to implement those new SPIs.

- Stage 11 (Ongoing monitoring and maintenance of certification)
  It is useful for the applicant and authority to collect feedback on the operational performance of the implemented change. The applicant may use these data for instance in the context of product support, design improvements, reliability improvements, safety enhancements etc. For the authority the operational (safety) performance feedback loop will provide input to a continuous operational safety process. For instance, based on safety performance feedback (e.g. occurrence data) in combination with a risk assessment, an authority can decide to issue an airworthiness directive in case of a detected safety deficiency in the design, or it may decide to develop new regulations or specifications to reduce certain risks and improve aviation safety. The tool can support this stage by performing the actual monitoring of the safety performance of the TAS and the certification case.
  The tool also enables the monitoring of assumptions made in the certification case, which requires that appropriate SPIs are defined in stage 9 to do so. This type of monitoring provides feedback to the applicant and certifying authority about the safety performance in service compared to the performance assumed during certification. This information can be used to update the certification argument (safety case).

3.3.3 Relation between the tool for continuous safety monitoring and the tool for safety risk assessment

The tool for continuous safety monitoring and the tool for safety risk assessments may provide complementary data on similar events, and they may provide a risk picture on different events, for example in case the SPIs in the tool for continuous safety monitoring are not covered by the risk model or vice versa.

The tool for continuous safety monitoring can provide a more up to date picture of a particular SPI than the current risk picture in tool for safety risk assessment. The data source of the tool for continuous safety monitoring is a repository of reported occurrences in ECCAIRS format, which can be updated continuously. The data used in the quantification of the risk model in the tool for safety risk assessment come from a variety of data sources over a long time period, which is regularly (but not continuously) updated.

The tool for safety risk assessment contains a risk model that relates events based on cause-effect relationships to risk, whereas the tool for continuous monitoring provides just a frequency of occurrence of a single SPI without relationships to other events or a risk level. The tool for continuous safety monitoring has no risk assessment capability, although it has some capabilities to conduct statistical analyses.

4 Evaluation of the tool for safety risk assessment

4.1 Application

The ASCOS tool for safety risk assessment embodies the ASCOS risk model and allows the user to access, explore, and modify the risk model. The tool allows the user to run a quantitative analysis of the safety impact of a change on the Total Aviation System and to review the current risk picture by means of the tool. The risk model is based on accident scenarios which are represented in the form of Event Sequence Diagrams (ESDs) and Fault Trees (FTs). The events in the risk model were quantified with safety data. The risk model and the tool for safety risk assessment are described in D3.2 [2], D3.3 [4] and Appendix C. The D1.3 report [1] explains that the tool for safety risk assessment "supports analysis required to support the argument for the functional specification (Claim 1), the logical design (Claim 2) and for the implementation (Claim 3). This includes both the safety of the system when functioning as designed and the analysis of failures and failure modes.".

From D1.3 and supporting guidance material it is understood that the tool may provide support in stage 4 to identifying:

- Safety objectives for the system. The safety practitioner can impose a safety objective to the end state of the ESDs. The safety objective that is allocated to the end state can be cascaded to the Fault Trees and allocated to the stakeholders corresponding to the risk model structure and elements.
- Safety requirements which specify what the system is required to do (not how it does it) in order to achieve the safety objectives. The cascading process will provide a safety requirements breakdown over the different domains and stakeholders associated with the different risk model elements in the ESDs and related Fault Trees.
- The degree of assurance required that the system will meet its requirements.
- Any additional functionality requirements or assumptions to capture any external means of mitigating the consequences of the hazards caused by failure of the system.

In Stage 5, the tool may provide support to setting requirements without necessarily prejudging how that design should be physically implemented. This assessment also needs to consider the achievability of any requirements and therefore must consider whether the requirements can be met (at least in principle) by the preliminary design.

Two case studies, D4.2 and D4.3, applied the safety risk assessment tool, while case studies D4.1 and D4.4 did not apply the tool. The D4.2 case applied the risk assessment tool as part of stage 1 to estimate the potential risk reduction as a result of the AARS system. The tool provided the set of accident scenarios that are related to a loss of control in flight. With the quantitative data on accident probabilities in those scenarios the D4.2 team was able to estimate the potential overall risk reduction of loss of control that could be achieved with the AARS. The D4.2 case study did not use the tool for a risk assessment or allocation of safety objectives as part of stage 4 and 5. The case study made use of an existing certification basis (CS25.1309) to obtain safety objectives/requirements for different severity levels of (functional) failure conditions. Hence, there was no need to use the tool to support the safety objective allocation.

The tool for safety risk assessment was applied in the case study D4.3 in an exploratory way. The case study first formulated a qualitative high level safety requirement, and then used the risk assessment tool to define the quantitative safety requirement. One of the quantified accident scenarios in the tool provided a reference accident probability that could be taken as a safety objective assuming an equivalent level of safety has to be demonstrated. Note that the case study D4.3, in contrast to D4.2, did not have a certification baseline for their subject of certification and therefore used the tool to derive a safety objective.

The case study D4.3 also envisioned a straightforward way to identify Design Safety Requirements at a lower level. The risk assessment tool could provide the probabilities for the events in the ESDs and supporting Fault Trees as maximum allowable frequencies. This activity was, however, not conducted in the case study due to the lack of maturity of the tool and risk model. The risk model's events were not yet fully quantified at the time of application. Secondly, the events in the ESDs and the underlying Fault Trees are generally not at the level of the logical elements developed in the case study.

The main reason that the tool was not used in D4.1 is that the specific case study did not match well with the level of detail and maturity of the existing risk model. For the case study D4.1 the risk model is more useful at a TAS level than at a detailed system level. For instance, the case study would have needed to develop its own ESD and FTs to connect to the existing risk model.

Case study D4.4 did not apply the risk assessment tool since it was believed that the scope of stage 4 was the assessment of the behaviour of the changed system in the absence of failure, whereas the tool mainly represents hazards resulting from system failures. Moreover, there was no need to use the tool for safety objective allocation as D4.4 used safety objectives from another sources for their case. Since the case study could not conduct stage 5 due to a lack of a logical design, the application of the tool to support Fault Tree development and risk assessment was not considered.

4.2 Benefits

The two case studies that applied the tool experienced benefits in the following areas:

- Definition of relevant accident scenarios for the subject of certification. In case study D4.2 these scenarios were subsequently used to assess the potential safety benefit of the AARS system, while in D4.3 the identified scenarios helped to determine a safety objective.
- Use of the tool to assess the potential safety benefit of the change, which can support stage 1. In the case study D4.2 the tool was used to estimate the potential effectiveness of the AARS system to reduce loss of control risk.
- Definition of safety objectives or safety requirements. Case study D4.3 made use of the baseline risk picture included in the tool to define a reference safety objective. However, the case study also found that lower severity events were not (yet) included in the accident risk model, so safety objectives could not be derived for those events in a similar manner as for the catastrophic event. The

application of the tool to the lower level of detail or less severe events was therefore not beneficial. Although D4.3 did not use the tool for the activities in stages 4 and 5 because of the explanatory nature of these stages in the case study, it notes that a few accident scenarios in the safety risk assessment tool may be useful in the risk assessment.

4.3 Conclusions and recommendations

Conclusions and recommendations are divided into the following topics: safety risks assessment (4.3.1), hazard identification (4.3.2), safety objective/requirement allocation (4.3.3), and the use of the tool in the stages of the ASCOS certification approach (4.3.4).

4.3.1 Safety risk assessment

The ASCOS tool for safety risk assessment can support safety assessment activities in the context of certification. The tool supports the TAS approach and a safety effect assessment of a change or subject of certification. The ASCOS risk model could be a sort of “super bowtie” serving as an “umbrella” model for the TAS. If the applicant is making use of accident scenarios and/or modelling techniques like ESDs and FTs as part of the safety assessment, then the ASCOS tool for safety risk assessment can be used to integrate these “local” or domain specific models into a Total Aviation System model. For example, airports which see a lot of interaction between stakeholders may benefit from such a risk model and tool that covers or integrates multiple domains.

The ASCOS risk model and tool for safety risk assessment can be used by some service provides as part of the risk assessment in their Safety Management System (SMS). The tool can be a means or the fundament of a means, which is flexible so that the user can adapt the risk model such that it will be fit for purpose of the user, i.e. for the particular application and certification subject.

It is imaginable that the tool may be used as part of stage 4 or 5 to determine and allocate safety objectives in other domains, or in cases where a certification baseline or risk criteria are absent. For the actual execution of a FHA or PSSA in the context of aircraft system certification, this tool is not directly helpful. The reason is that in this domain well established AMC, guidance material and a certification baseline, including safety objectives such as in CS25.1309, are available.

The tool for safety risk assessment can be further applied to:

- Support the assessment of safety effects when the certification case or change is implemented. The tool allows the user not only to assess the effect on the domain level but also on the level of the Total Aviation System.

- To identify interfaces between domains or stakeholders affected by the certification case or change. Each risk model element or event in the tool can be allocated to a domain or stakeholder responsible for that event. If a change impacts a particular risk model element, then the tool shows what other risk model elements are affected, i.e. showing the domains or stakeholders affected.

Recommendation 21: It is recommended to ASCOS that domain(s) and stakeholder(s) are allocated to the risk model elements.

Recommendation 22: It is recommended to ASCOS to further develop the airport and ATM related parts of the ASCOS risk model. Eurocontrol has developed a similar risk assessment tool, called IRP or AIM, that can be used to analyse risks and assess the impact of changes to the ATM system. It is proposed to consider using IRP/AIM (sub)model elements in the ASCOS risk model.

4.3.2 Hazard identification

The tool can be applied during the hazard identification process as means to perform a cross-check whether all relevant types of accident scenarios and hazards have been covered. The structure of the risk model provides a reminder of which main accident types can be considered in the hazard identification. The events in the Fault Trees can provide suggestions for the types of hazards to consider. The risk model events also provide a link or a 'hook' to relate brainstormed hazards to accident scenarios. If one is able to directly relate or to associate a particular hazard with a risk model element, then the tool will provide the relation between that hazard and accident risk.

It is remarked that the current risk model and tool includes mainly 'technical' hazards. The applicability of the tool to changes or to subjects of certification with an organisational or strong socio-technical character requires further risk model and tool development. Hazards related to the functioning of the Safety Management System (SMS) that the service provider has to establish cannot be addressed explicitly by the current version of the risk model and tool.

4.3.3 Safety objective/requirement allocation

In the context of performance based certification, the tool and risk model can support safety objective or safety requirement allocation to domains and stakeholders, but this depends on the format of the safety performance target. If the safety performance target is defined by the regulator in terms of an accident, incident or failure probability target, then the tool and model could be used to apportion these high level target probabilities to risk model elements using the model's logic and structure. Since risk model elements can be associated with domains and stakeholders, the model's logic/structure can help to distribute TAS level

safety targets to domains. If safety performance targets are defined in other terms than event probabilities, then the tool is most likely not applicable for safety objective/requirement allocation.

Identification of design safety requirements by using the risk model in the tool can be done up to a level that is determined by the risk model's scope and level of detail. Safety objectives or design safety requirements can be derived only for those accident scenarios and hazards covered in the risk model. The lower level severity events (less severe outcomes of scenarios) may not be sufficiently represented in the current risk model to support the definition of safety objectives for those lower severity classes.

Recommendation 23: It is recommended to ASCOS that guidance material will describe how to solve the following issues:

- How exactly can the safety risk assessment tool assist in identifying Design Safety Requirements, specifically considering that the events and faults in the risk model are generally at a different level than the logical elements at which the Design Safety Requirements need to be identified?
- It is unclear to what level the ESDs and Fault Trees need to be decomposed to assess how the various stakeholders work together to satisfy the high level safety requirements.

4.3.4 Use of the tool in the stages of the ASCOS certification approach

The tool for safety risk assessment can be used to in support of stages 1, 4, and 5, but further tool and risk model development and guidance material are recommended to increase the benefits of this tool in support of certification activities.

Recommendation 24: It is recommended to ASCOS that guidance material explains the potential use of the tool in the following stages.

- Stage 1 (Definition of the change)
  The tool can be used to derive the current risk picture for the TAS, including different domains and stakeholders. As a result the applicant is made aware of the actual risks or safety performance in the TAS in the domain(s) of interest. These data can be used to assess the potential safety impact of the change in the TAS and to define the current risk level as a basis for safety target setting as part of the argument structure that defines the applicable safety criteria in stage 2. The ASCOS guidance material should explain how the tool for safety risk assessment can be used as part of stage 1 and explain its value and difference compared with the tool for continuous safety monitoring (see also section 3.3.3).

- Stage 2 (Define the certification argument)
  The tool can be used to derive and allocate safety objective/requirements as explained in section 4.3.3. The ASCOS guidance material should include a process to ensure that the tool reflects correctly the operational environment and scenarios if it is to be used by multiple stakeholders for safety objective allocation. In addition, guidance material should explain what process to follow for the allocation of safety requirements to human factors (events related to human performance).

- Stage 4 (Specification)
  When the topic of certification is a technical system, stage 4 includes a FHA where the hazards are 'driven by' the functional design. In these cases the tool cannot properly provide a functional hazard identification and assessment.

- Stage 5 (Design)
  The tool can support stage 5 when a PSSA is conducted. The ASCOS risk model and tool can be used as an overall safety assessment model/tool for the TAS, integrating 'local', case specific risk models from different domains or stakeholders (provided that these models use similar modelling techniques). Although the Fault Trees are not yet developed to the level of detail that is immediately useful for application in a certification case, the tool is flexible so that the safety practitioner can update, modify and expand the risk model (ESDs and Fault Trees) as required.

5 Evaluation of the FAST AoC list

5.1 Application

The Future Aviation Safety Team (FAST) has developed a list of Areas of Change (AoC). This list describes generically major changes to the aviation systems that are ongoing or that may occur in the near or long term. The FAST Area of Change list provides for each Area of Change a description of the change, associated potential hazards, and a source and comments [5]. These AoCs can be used in safety assessments of future systems, services and operations, and can contribute to the definition of possible future environments in which the system, service or operation will be functioning. The assessment of the FAST AoC list is an inherent part of the ASCOS certification approach. According to the outline of the ASCOS certification approach the definition of the subject of certification or change in Stage 1 has to consider the FAST AoC list to identify what AoCs are expected in the TAS within the defined time frame, and to assess their effect, e.g. whether they may introduce additional hazards.

Three of the four case studies applied the FAST AoC list as part of Stage 1 (i.e., D4.1, D4.2, D4.3). The application of the FAST AoC list to identify potential future hazards was only done by case study D4.2 in stage 1 and stage 5. The set of applicable AoCs obtained in Stage 1 in the case studies is long and diverse, and many AoCs are only loosely related to the subject of the case study. Due to the fact that the FAST AoC list is not very well structured, it is cumbersome to identify all applicable AoCs and associated hazards.

In case study D4.1 the FAST AoC list was reviewed and the impact of AoCs on RPAS were defined and classified as direct, indirect or no/not applicable impact.

In case study D4.2 the FAST AoC list was reviewed to identify which AoCs could materialise within the time frame of the case study. Those AoCs expected to be (partly) realized within the defined time frame were reviewed to determine which AoC could affect the subject of certification in the case study. From these AoCs a list of potential hazards was derived that were considered relevant for the case study. The hazards that were available in the FAST AoC list could not be used as part of stage 4, which concerns a functional hazard analysis that deals by definition with hazards associated with functions of the system to be developed. One hazard from the FAST AoC list was taken into account in stage 5.

The case study D4.3 considered the FAST AoC list to determine which AoCs may be relevant for the subject of the case study. This analysis resulted in a quite large subset of potentially relevant AoCs, which were not further used in the case study. This was due to the exploratory character of the stages 4 and 5 in this study, and due to a lack of clarity on how these AoCs should be used.

In the case study D4.4 the concept of Areas of Change was defined as any (future) phenomenon that will affect the safety of the aviation system either from within or from important domains external to aviation. This case study defined the AoCs from the reference SESAR P15 04 01-D10 Final Report Part 2 (Ed 00.01.00) and did not use the FAST AoC list as they found it difficult to assess the impact of the FAST AoCs in the context of the topic of the case study.

5.2 Benefit

The benefit of the use of the FAST AoC list lies primarily in the fact that it helps to describe the future context of a change. The use of the FAST AoC list in the change definition is useful as it may direct attention to areas otherwise overlooked, particularly in view of the TAS approach. It helps to ensure that the certification considers not only the context of today but also the future, and that attention is given in the specification and design to relevant AoCs and hazards as identified by FAST. This should prevent that a new change is required after the change is implemented or that additional risk mitigation measures are required once the significant AoC materialises in the near term. In the hazard identification process the FAST list of hazards may be useful as a means to perform a cross-check whether all relevant types of scenarios and hazards have been covered. As an example, D4.2 considered the following hazard from the FAST AoC list, “controllers may be overwhelmed by a proliferation of caution and waning systems and alerts in periods of high workload”, as an issue that needs to be addressed in the discussion about the design of the system.

5.3 Conclusions and recommendations

The FAST AoC list is helpful in defining the future environment as part of the description of the certification case in the context of the Total Aviation System. Furthermore, the FAST AoC list can be used as a source for hazard identification. It can be regarded as a brainstormed list of possible future changes and hazards which the applicant may use to identify additional hazards for his certification case. However, it takes significant effort to assess all possible AoCs for the certification of a certain change, given the uncertainty about the timeframe of the AoC, the exact manifestation of the AoC and their effect on the particular certification subject. The FAST AoC list includes generally high-level, TAS related changes which may be difficult to “translate” to a specific, low-level change in a domain.

Recommendation 25: It is recommended to FAST to provide an assessment of the timeframe within which the change and future hazards are expected to develop. This would prevent applicants to do such an assessment based on their own perception without knowing the precise background of the AoC. In addition, it is suggested to better structure and classify the FAST AoC list and to enable search according to the main topic, domain, time frame and geographic function to improve the usability.

Recommendation 26: It is recommended to ASCOS to provide guidance on the use of the FAST AoC list in stages 1, 4 and 5 to ensure that the FAST AoCs are consistently interpreted, understood and applied in the definition of the change (stage 1), in the hazard identification, in the specification (stage 4) and design (stage 5).

In stage 1 the first step would be to identify all relevant AoCs and to determine which AoCs should be considered for the subject of certification in the short term and which AoCs may become relevant for the subject of certification in the long term. During the specification and design, and possibly in the safety assessment prior to a change, only the AoCs of significant importance could be considered. ‘Significant

importance' could be determined for example by the degree of the effect of the AoC on the certification case or the time horizon in which the AoC may impact the certification case. An AoC that will occur in the short term needs to be addressed more urgently in the specification and design stages than a long term AoC. Addressing long term AoCs can be undertaken by Safety Management Systems (SMS) and continuous safety monitoring processes in due course.

Recommendation 27: It is recommended to ASCOS to link the FAST AoCs and related hazards to the risk model elements in the tool for safety risk assessment. If the link between the AoC and the main accident categories, the accident scenarios, Event Sequence Diagrams and/or Fault Tree elements can be established, then the user of the FAST AoC list may be able to identify how the AoC affects the safety of the TAS. The applicant can use this information to determine which accident scenarios are relevant to consider during certification.

Recommendation 28: It is recommended to ASCOS that guidance material for the application of the FAST AoCs and hazards in the ASCOS certification approach stages includes the following activities:

- Identify relevant FAST AoCs and hazards in stage 1 for the certification subject.
- Determine for each FAST AoC if there is a short-term significant relevance, or whether the AoC could be addressed in the future as part of the safety management systems or continuous safety monitoring process. This step aims to identify which AoCs and hazards should be addressed in the current certification case compared to those that can be addressed in the future. If the AoC is to be addressed in due course as part of the SMS or continuous safety monitoring process, then the arrangements for this activity should be developed in stage 2.
- After identifying the relevant FAST AoCs and hazards for the certification subject, the tool for risk assessment can be used to identify relevant accident categories, accident scenarios and risk model elements for further consideration in stages 1, 4 and 5.
- Assess the potential impact of the FAST AoCs and their related hazards on the subject of certification, i.e. consider these hazards as part of the stage 4 and 5 complementary to the "FHA" or "PSSA" type of analysis. Especially in stage 5, when the concept or system design is developed, the applicant could take into account the expected FAST AoCs and hazards. Three situations may occur:
    - There is no impact foreseen of the AoC, so no further assessment is needed.
    - The FAST AoCs and their hazards are a cause for (new) hazards in the context of the subject of certification or they are relevant for the safety of the change. This may require for example further risk assessment or design considerations.
    - The subject of certification will have an impact on the FAST AoC or its hazards, and this would require an assessment of the safety effect of the subject of certification on the FAST AoC and hazards (this could also be input to stage 1).

6 Evaluation of ASCOS certification approach against Key Performance Areas

6.1 Approach

This chapter describes the evaluation of the case studies against the performance framework that defines Key Performance Areas (KPAs) for the ASCOS approach. The application of and experience with the ASCOS certification approach in the four case studies is analysed against the KPAs to evaluate the "fitness for purpose" of the certification approach in the context of a compliance and performance based regulatory framework. The objective of the evaluation is to assess the quality of the ASCOS certification approach that guided the execution of each case study, without making a judgment on the engineering and technical quality of the case studies. It is assumed that each case study reflects mainly the potential of the underlying approach, rather than the ability, skill or experience of the developers of the cases. This assumption is based on the fact that the development of the case studies benefitted from the assistance of the partner responsible for the development of the approach and the partner with expertise in certification. Since the case studies applied the ASCOS certification approach up to stages 4/5/6, they provide evidence about the quality of the underlying ASCOS approach for those stages. The current evaluation can be regarded as an initial one since not all stages of the approach were conducted in the case studies.

The evaluation exercise took the form of an expert evaluation. The ASCOS approach, as implemented in the case studies and documented by the case studies reports, has been rated according to a set of seven predefined Key Performances Areas, which were defined in the context of WP 5. These KPAs are important for two reasons. Firstly, they reflect areas of performance in the certification domain in which the proposed ASCOS approach may deliver improvements, and secondly, they allow the comparison and integration of the results of this report with the results of other evaluations activities carried out in the context of the project. Initially the KPA framework was defined in the D5.1 [12] and the final version of these KPAs was presented in D5.3 [24] and is reported in Table 1.

The research team scored the KPAs based on the review of the case study reports. For each of these KPAs the team has expressed a score on a five point scale ranging from 1-very low (meaning that the perceived contribution to the rated KPA appeared as very low) to 5-very high (meaning that the perceived contribution to the rated KPA was perceived as very high). Also, a "Not applicable" score was used to indicate situations for which it was not possible for the team to determine an informed score.

Table 1. KPAs for the proposed ASCOS certification approach.

KPA	Definition	Metric
1. Efficiency	The extent to which the proposed ASCOS certification approach allows to reduce the effort (cost, time, and training) needed by the applicant to obtain a certificate.	Expert rating
2. Soundness	The extent to which the proposed ASCOS certification approach promotes, in certification, the consideration of relevant hazards and safety requirements that today are not or are poorly considered—with specific reference to cross-domain hazards and safety requirements.	Expert rating
3. Cross-domain integration	The extent to which the proposed ASCOS certification approach promotes integration, coordination, and exchange of information across the different stakeholders that may be involved in the certification of a change.	Expert rating
4. Harmonization	The extent to which the proposed ASCOS certification approach looks compatible with the different certification approaches in use in different domains (e.g. ATM vs aircraft certification) and geographical areas.	Expert rating
5. Accommodation of Innovation	The extent to which the proposed ASCOS certification approach makes the certification of innovative products and systems, i.e. products and systems for which no standard are available, more likely.	Expert rating
6. Acceptability	The extent to which the proposed ASCOS certification approach looks acceptable to the applicant and the certifying authority.	Expert rating
7. Flexibility	The extent to which the proposed ASCOS certification approach can be applied to a broad range of different types of products, systems, and services, varying in size and complexity.	Expert rating

6.2 Results

6.2.1 KPA 1: Efficiency

Compliance based regulations	Very Low 1	**Low 2**	Neutral 3	High 4	Very High 5		Not applicable
Performance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable

This KPA assesses the contribution of the proposed ASCOS certification approach to the effort needed to obtain the initial certificate. The contribution of the ASCOS certification approach to this KPA is rated as low in the context of compliance based regulations and high for performance based regulations. It was noted that at least in one of the case studies (D4.4) the perceived effort required for implementing the approach in a compliance based environment was relatively high, especially for people not familiar with the ASCOS approach and the use of the safety argument Goal Structured Notation. Two case studies (D4.1, D4.2) found that the effort to apply the logical argument approach was significant. Considering that for these two case studies existing certification means are mature and well defined, the ASCOS approach was experienced as an extra

effort. It was observed that the ASCOS approach would not improve the efficiency in the current certification practice. However, in the context of a performance based approach the ASCOS certification approach would provide a structure and means to the applicant, which would have a positive effect on efficiency.

6.2.2 KPA 2: Soundness

Compliance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable
Performance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable

This KPA deals with the contribution of the ASCOS certification approach to the quality of certification or safety case. In other words, this KPA addresses the extent to which the proposed logical argument approach supports the identification and traceability of cross domain hazards and safety requirements, together with the related evidences and (contextual) assumptions.

The ASCOS approach positively contributes to this KPA and receives a high rating for the compliance and performance based regulations environment. Indeed, the approach allowed the consideration of the identified changes not in isolation but in the context of the Total Aviation System. As a result of the implementation of the approach, all cases have described the involved organizations, domains, and interfaces, and have provided a preliminary identification of the hazards that may affect other domains, and the related safety requirements. Hence, the case studies provide support to the idea that the proposed certification approach can promote that the applicant thinks across the boundaries of the specific change from the start (i.e. definition of the change) and before an initial certification plan is defined.

Note that the contribution to soundness can be increased by further enhancing the consideration of human factors issues and organizational factors impacting safety. The current version of the approach should provide further guidance about how human factors issues can be identified and managed in certification. While no specific reference was made to human factors methodologies in the four case studies, the ASCOS approach seems flexible enough to integrate different human factors assessment methods. Therefore, the guidance material on the ASCOS approach should specify which types of human factors assessment methodologies can complement the approach. The need to better consider organizational factors impacting safety emerged specifically in case study D4.3. In this case study the safety analyst has to consider hazardous aspects that may result from organizational factors such as changes in roles and responsibilities across organizational boundaries. These organizational aspects are usually not covered by “classic” risk models, i.e. risk models that focus on sequences of events at the level of system’s actual operation, without considering the underlying organizational contributing factors. The application of the ASCOS approach to the certification of services and organizations demands that the approach will be enhanced with methods that are able to address such aspects.

6.2.3 KPA 3: Cross-domain integration

Compliance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable
Performance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable

This KPA concerns the extent to which the approach promotes the sharing of information, coordination of effort et cetera, between domains and stakeholders. The KPA receives a high rating for the compliance and performance based regulations environment. The case studies show that Step 1 of the ASCOS certification approach, the 'Definition of the Change', promotes the consideration of all the affected domains and organizations involved in a change. All of the cases have acknowledged the relevant TAS stakeholders that may be affected by the change, and the relevant interfaces and dependencies.

The case studies provided feedback that the guidance material should be improved to support the applicant in the (practical) arrangements for the cross-domain integration, by providing further guidance and criteria about how the practical, process-oriented aspects can be addressed. In practice, when the approach is implemented, the applicant needs to interact with other organizations/stakeholders. The contribution of the ASCOS approach to cross-domain integration could be further enhanced by considering in the certification plan how the effort of the different stakeholders involved in the change comes together during the system lifecycle. This requires the applicant to further specify aspects such as which stakeholder is responsible for the TAS certification safety argument, which actual TAS stakeholders will be approached (e.g. which specific (group of) air operator(s), maintenance organization(s), etc.), how and when the TAS certification team (the team composed by the relevant specialists from the different involved organizations and responsible for TAS safety assessment) is established, when and what types of specialists the team should include, etc. Note that the quality of the guidance material was not taken into account, and did not influence, the scoring of this KPA.

6.2.4 KPA 4: Harmonization

Compliance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable
Performance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable

This KPA addresses the extent to which the ASCOS certification approach is compatible with existing (local) approaches in certification in use across different domains. The KPA receives a high score in both a compliance and performance based regulatory environment. The ASCOS certification approach was implemented by the four case studies consistently, i.e. all cases followed the predefined steps of the approach as defined in D1.3

and ASCOS guidance material [14, 15] that lead to the definition of the certification plan. This consistency suggests that the approach has potential for becoming a standard approach used across different domains and organizations. The developers of the four case studies had different backgrounds and came from different certification domains (e.g. ATM, aircraft system development) and from different organizations (e.g. an OEM, R&D and CAA). Furthermore, the positive contribution to harmonization is supported by the observation that no inconsistency with existing certification and safety standards has emerged. The approach seems sufficiently flexible to accommodate safety methods currently used in certification, such as a Functional Hazard Assessment and a Preliminary System Safety Assessment. These current methods are able to deliver the evidences required to support the claims in the logical argument structure. For these reasons the KPA received a high rating.

6.2.5 KPA 5: Acceptability

Compliance based regulations	Very Low 1	Low 2	Neutral 3	High 4	Very High 5		**Not applicable**
Performance based regulations	Very Low 1	Low 2	Neutral 3	High 4	Very High 5		**Not applicable**

This KPA considers the extent to which the ASCOS certification approach is found acceptable to certification stakeholders. It needs to be acknowledged that it is difficult to express an informative judgement about the potential contribution of the ASCOS approach to this KPA based on the case studies alone. Hence, this KPA was not rated. Recommendations about the practical way in which the ASCOS approach can be implemented have emerged from the case studies. The ASCOS certification approach and guidance material needs to address them so as to contribute to the acceptability of the approach, see also sections 2.3, 3.3, 4.3, and 5.3.

6.2.6 KPA 6: Accommodation of Innovation

Compliance based regulations	Very Low 1	Low 2	**Neutral 3**	High 4	Very High 5		Not applicable
Performance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable

This KPA considers the adequateness of the proposed ASCOS certification approach to improve the certification of innovative products and systems, i.e. novel products and systems for which no reference standards exist. The KPA is rated as high for a performance based regulatory environment. The use of a logical argument approach can add structure and clarity to the certification process, and this will be especially helpful for performance based regulations or in cases where (prescriptive) standards do not exist. It is concluded that

the ASCOS approach supports the definition of the certification basis. While this does not mean that the ASCOS approach simplifies the certification of innovative systems, the benefit is that it provides a means to conduct performance based certification. In a compliance based regulatory environment the KPA is rated as neutral because the added value of the ASCOS approach is perceived as limited. The case studies appeared to be able to apply current certification practices to the innovative subjects of the case studies with little added value from the ASCOS approach.

6.2.7 KPA 7: Flexibility

Compliance based regulations	Very Low 1	**Low 2**	Neutral 3	High 4	Very High 5		Not applicable
Performance based regulations	Very Low 1	Low 2	Neutral 3	**High 4**	Very High 5		Not applicable

This KPA addresses the extent to which the proposed ASCOS certification approach can be applied to the certification of different types of systems, products, and services. The flexibility score depends on the regulatory framework within which the ASCOS approach is applied. It is noted that the current version of the approach seems more directly applicable in the context of performance based regulations, and is considered to provide high flexibility in such an environment. Different certification subjects and assessment methods can be applied within the logical argument structure and certification stages for example. On the other hand, the application of the ASCOS approach in the compliance based regulatory environment, with predominantly prescriptive rules/standards, limits its flexibility as by nature there is less freedom in compliance with these rules/standards than in a performance based framework.

6.3 Conclusions and recommendations

This section reports the results of an evaluation of the outline of the ASCOS certification approach as implemented in the four case studies for the seven KPAs, which can be taken into account in the updating of the certification approach in WP 1.5. The scores for the seven KPAs in a compliance and performance based regulatory framework are summarised in Table 2.

The evaluation concluded that the ASCOS certification approach has clear potential in the area of Soundness (KPA 2), Cross-domain integration (KPA 3) and Harmonization (KPA 4), in both a compliance and performance based regulatory environment. In fact the ASCOS certification approach promotes the early consideration of cross domain hazards and safety requirements across the TAS in the early certification phases and prior to the definition of the certification plan. The ASCOS approach seems compatible with existing practices.

Table 2. Resulting ratings of the KPAs for compliance and performance based regulatory environment.

KPA		Very low 1	Low 2	Neutral 3	High 4	Very High 5	Not applicable
1. Efficiency	CBR [1)]		●				
	PBR [2)]				●		
2. Soundness	CBR				●		
	PBR				●		
3. Cross-domain integration	CBR				●		
	PBR				●		
4. Harmonization	CBR				●		
	PBR				●		
5. Accommodation of Innovation	CBR			●			
	PBR				●		
6. Acceptability	CBR						●
	PBR						●
7. Flexibility	CBR		●				
	PBR				●		
1) CBR: Compliance based regulations; 2) PBR: Performance based regulations.							

The contribution of the ASCOS certification approach to the areas of efficiency (KPA 1), Accommodation of innovation (KPA 5) and Flexibility (KPA 7) is rated as high in a performance based regulatory context and is rated as low (KPA 1 and 7) and neutral (KPA 5) in the context of a compliance based regulatory environment. From the case studies it is observed that the ASCOS certification approach has potential in these three KPAs when performance based regulations apply. It promotes the certification of innovative systems in a performance based environment because of the added clarity and structure resulting from the logical argument structure approach, and because of the possibility to support the development and/or adaptation of certification standards. However, its contribution to the current certification practice with prescriptive or compliance based regulations is considered low and has to be further demonstrated. Regarding KPA 1, gaining more experience with the application of the ASCOS certification approach can lower significantly the (currently) experienced effort required for its implementation.

The contribution of the ASCOS approach to Flexibility (KPA 7) was less evident. Although the ASCOS approach may be adapted to different types of certification cases and is able to include different assessment techniques,

the ASCOS project should provide further guidance about how the approach can be applied to the certification of organisations.

The KPA Acceptability (KPA 6) was the most difficult area to rate. The case studies highlighted relevant uncertainties related to the definition of the risk acceptance criteria in the TAS, the development of the safety argument, and specific roles and responsibilities of authority and the applicant.

Recommendation 29: It is recommended to ASCOS to improve guidance material about how the effort of different stakeholders can be integrated and coordinated along the system lifecycle. This can further improve the ASCOS contribution to cross-domain integration (KPA 3).

Recommendation 30: It is recommended to ASCOS to address in guidance material the issues related to risk acceptability across the TAS, development of the safety argument structure and roles and responsibilities of the stakeholders. This can contribute to the acceptability of the approach (KPA 5). Refer also to previous recommendations in section 2.3.

Recommendation 31: It is recommended to ASCOS to develop guidance material to support the identification of organizational hazards and associated (safety) requirements to increase the feasibility of the approach to the certification of services and organizations (KPA 7).

7 'Verification' of the ASCOS certification approach

7.1 Approach

This chapter describes the result of the evaluation of the case studies against principles defined in the ASCOS deliverable D1.2 [23]. This evaluation has the character of a 'verification' exercise to determine how well the ASCOS certification approach and the results achieved by the case studies meet the high level principles. The ASCOS D1.2 document [23] proposed a set of principles to be considered in the development of the proposed certification approach. Taking these principles into account, 'verification questions' were developed which can be used in the review of each case study in order to evaluate the ASCOS certification approach, and suggest improvements. Note that there is not a one-to-one mapping between the principles and the questions below because some of the principles would be difficult to test in the case studies, and some have been merged when devising the questions below. It is recognised that, owing to the widely differing nature of the case studies, the extent to which the verification questions are meaningful and useful will vary between case studies. The intention was to use these questions to explore the efficacy of the ASCOS approach, and how it could be improved, rather than as a "scoring mechanism" for the (quality of) case studies.

1. To what extent has the case study shown that the approach is capable of considering the impact on the total aviation system? What enhancements can be made to the ASCOS approach to facilitate this consideration of the impact on the Total Aviation System?
2. To what extent has the case study ensured that safety issues at the interfaces between domains are fully captured and managed? What enhancements can be made to the ASCOS approach to improve the effectiveness of this process?
3. What existing methods already in use within the affected domains are applied by the case study? How has the case study shown that these methods remain applicable for application within the argument which it makes? Did the ASCOS approach make it easy for the existing methods to be reused?
4. Has the case study introduced assessment methods which are not usually applied in the domain(s) in question? (These may be novel methods, or they may be methods more usually applied in other aviation domains or in other industries.) Did the ASCOS approach ease the introduction of these methods? How could the approach be adapted to make an introduction of these methods more straightforward?
5. Has the case study applied harmonised assessment methods across domains? How was this facilitated by the ASCOS approach? How has this benefited the overall certification argument?
6. Has the ASCOS approach simplified the certification process? How could the approach be further adapted or improved to further simplify the certification process?
7. How was the case study affected by the differences in regulatory approach between different domains (in particular between aircraft certification and air traffic management)? To what extent did the ASCOS approach enable these differences to be addressed, allowing a single argument to be made for the proposed change? How could the ASCOS approach be improved to make it easier to address these differences?

8. In what ways does the case study demonstrate that the ASCOS approach achieves improvements over existing certification approaches? What bottlenecks and / or shortcomings does the case study encounter and how were they resolved?
9. To what extent has the case study suffered from conflicting use of terminology? It is recognised that the ASCOS approach does not currently provide support in addressing such conflicts, but how could the approach be improved to allow such conflicts to be addressed in future?

7.2 Results

Reviewing the case studies by means of these nine 'verification' questions delivered the following results.

- The case studies have demonstrated that the ASCOS approach is capable of considering impacts on the Total Aviation System (TAS), but has also identified some issues that need to be resolved:
  - How to deal with safety benefits in one domain that are accompanied by safety reductions in another domain.
  - How can safety objectives be consistently applied over the various domains?
  - How can the acceptable level of safety be set across the TAS?

  These issues are the responsibility of the regulator(s) and cannot be solved by the ASCOS project.

Recommendation 32: It is recommended that ASCOS informs EASA and national CAAs of these potential issues so that they can be considered if changes are made to regulations.

- The case studies have demonstrated that safety issues at the interfaces between the domains can be identified, but the extent to which they are fully captured and managed is unclear. The process for identifying safety issues across domains can be improved by providing a definition of hazard that is consistent and agreed across domains and by providing guidelines on hazard identification.
- The ASCOS approach allows reuse of existing certification methods. Particularly the decomposition of the arguments allowed simultaneous application of different methods.
- In the context of the current primarily prescriptive (compliance based) regulatory requirement it seems to be unlikely that assessment methods which are not usually applied will be introduced when the ASCOS approach is applied. If the regulatory framework shifts towards performance based, new methods may be used, although it was observed that the ASCOS approach seems to be 'failure' oriented and therefore does not easily facilitate methods which are 'control' oriented such as STAMP or FRAM.
- The ASCOS approach does not directly contribute to harmonisation of assessment methods. The case studies have highlighted differences in the approaches currently used in the various domains and identified several issues that need mitigation to harmonise the ASCOS approach, e.g. on the definition of hazard, safety objectives, the level of scenarios and assigning levels of development assurance.

Recommendation 33: It is recommended to ASCOS to alert the users of the ASCOS approach to the different definitions of hazard, safety objectives, level of scenarios and development assurance that exist in assessment methods in various TAS domains and to advise using common definitions if these different methods are applied in a single certification case.

- Essential stages of the ASCOS approach broadly align with existing methods and are therefore not expected to simplify the certification process. The set-up of a logical argument structure is not without difficulties. To define a consistent set of claims to an appropriate level of detail is a laborious and complex task, which could benefit from appropriate guidance material. Such guidance material is not yet sufficiently available).
- The case studies seem not to be affected directly by differences in regulatory approach between different domains such as the aircraft certification and air traffic management domain. However, this issue was not really tested in the case studies, so no firm conclusions can be drawn yet.
- According to the experiences in the case studies, the main benefit of the ASCOS approach is that it takes the TAS into account, and helps to identify interfaces and stakeholders across domains. However, these benefits will be achieved at the cost of added complexity to the initial design and certification process and an increased management and communication burden. Addressing the TAS early in the design cycle may result in lower cost in the end, but this hypothesis could not be tested during the case studies. In a performance based regulatory approach, the ASCOS approach may have other benefits but this could not be verified in the case studies.
- During the case studies, the ASCOS approach suffered a bit from the introduction of ASCOS specific terminology such as ‘pre-existing hazard’, ‘external hazard’, ‘system generated hazard’ etc., without properly defining these in the guidance material or explaining why this specific nomenclature is necessary.

Recommendation 34: It is recommended to ASCOS to refrain from introducing ASCOS-specific terminology. See also recommendation 06.

8 Conclusions and recommendations

8.1 Conclusions

The ASCOS certification approach

The ASCOS certification approach is applicable and beneficial in the light of a performance based approach to certification. The aviation industry is moving towards the introduction of performance based regulations, which can only be successful if the certification approaches are adapted to this new environment. The ASCOS certification approach provides added value because it considers the Total Aviation System (TAS) from the start of design/certification activities and covers the entire lifecycle. Additionally, the coordination and sharing of safety requirements between stakeholders and across domains is one of the key characteristics and main benefits of the ASCOS approach. Safety benefits may be anticipated by using an approach that takes into account the TAS. However, these benefits will require early involvement of all stakeholders and authorities from all aviation domains. This will add complexity to the initial phase of the design and certification process, which involves increased management and communication as compared to the current way of working.

The ASCOS certification approach is a suitable approach if there is a clearly defined change in the operation, e.g. in the ATM, airport or airline operation, in the context of performance based regulations. The application of the ASCOS certification approach in the current, mainly compliance-based certification framework introduces additional complexity as a result of the logical argument framework, and provides consequently – for compliance based certification – little to no benefits.

The set-up of the logical argument structure can provide the certification basis in a performance based regulatory framework. However, the set-up of the argument structure itself can be a complex and laborious task, especially for novices. Application of a logical argument framework requires appropriate guidance material, which is not yet sufficiently available. In a performance based regulatory framework the argument structure may be worth the effort. However, it is questionable if this benefit will materialize for a practical case and if it is worth the additional effort, especially in the context of a compliance based regulatory framework and/or in a domain such as aircraft system certification which applies well developed certification practices.

The tool for continuous safety monitoring

The tool for continuous safety monitoring was not applied by the case studies, because these focused on the definition, design and specification of proposed changes in the TAS (and the tool is initially developed for *monitoring*, i.e. use after proposed change(s) are approved, implemented and transferred into operation). Hence, from ASCOS WP4 there is no hands-on experience and feedback available about the application and benefit of the tool.

The tool for safety risk assessment

The ASCOS tool for safety risk assessment can support safety assessment activities in the context of certification. The tool was applied by two case studies for a safety effect assessment and a safety target

allocation. The tool supports the TAS approach and a safety effect assessment of a change or subject of certification. It also helps to define relevant accident scenarios for the subject of certification. The tool can be applied during the hazard identification process as means to perform a cross-check whether all relevant types of accident scenarios and hazards have been covered. In the context of performance based regulations, the tool and risk model can support safety objective or safety requirement allocation to domains and stakeholders provided that the format of the safety performance target is in the form of an accident, incident or failure probability target.

The FAST AoC list

Three case studies applied the FAST Areas of Change (AoC) list as part of the certification approach stages. It is concluded that the FAST AoC list is helpful in defining the future environment as part of the description of the certification case in the context of the TAS. Furthermore, the FAST AoC list can be used as a source for hazard identification. However, it takes significant effort to assess all possible AoCs for the certification of a certain change. Another issue is that the FAST AoC list includes generally high-level, TAS related changes which may be difficult to "translate" to a specific, low-level change in a domain.

The evaluation of the ASCOS certification approach against Key Performance Areas (KPAs)

The evaluation of the case studies against the seven KPAs concluded that the ASCOS certification approach has clear potential in the areas Soundness (KPA 2), Cross-domain integration (KPA 3) and Harmonization (KPA 4), in a compliance and performance based regulatory environment. The contribution of the ASCOS certification approach to the KPA Efficiency (KPA 1), Accommodation of innovation (KPA 5) and Flexibility (KPA 7) is rated as high in a performance based regulatory context. In the context of a compliance based regulatory environment the ASCOS contribution to KPAs Efficiency and Flexibility is rated low, and for KPA Accommodation of innovation it scores neutral. The KPA Acceptability (KPA 6) was not rated because it was not possible to form an informative judgement about the potential contribution of the ASCOS approach to this KPA based on the case studies alone.

'Verification' of the ASCOS certification approach against 'design requirements'

A set of 'design requirements', considered by ASCOS WP1 in the development of the initial proposed certification approach, was used to formulate 'verification' questions. The questions were used to explore the efficacy of the ASCOS approach, and how it could be improved, rather than as a "scoring mechanism" for the (quality of) case studies. The case studies demonstrated that the ASCOS approach is capable of considering impacts on the TAS and that safety issues at the interfaces between the domains can be identified, but the extent to which they are fully captured and managed is unclear from the case studies. Addressing the TAS early in the design cycle may result in lower cost in the end, but this hypothesis could not be tested during the case studies. These benefits will be achieved at the cost of added complexity to the initial design and certification process and increased management and communication in the early stages (as compared to the current process). In a performance based regulatory approach, the ASCOS approach may have other benefits but this could not be verified in the case studies. The review also identified some issues related to safety target setting,

safety requirement allocation and risk acceptability across the TAS that need to be resolved by the regulator(s).

8.2 Recommendations

Recommendation 01: It is recommended to ASCOS to develop guidance material explaining criteria for determining whether the ASCOS certification approach is suitable and efficient to apply to a particular certification case.

Recommendation 02: It is recommended to ASCOS to include this section in guidance material to explain how the ASCOS approach stages align with the current (aircraft system) certification practice.

Recommendation 03: It is recommended to ASCOS to develop guidance material that helps the user to define the "change X" (i.e. Claim 0, in D1.3) and its scope or "boundaries". The definition of the change should cover technical, organizational, operational, procedure, environmental aspects. It should also identify all involved stakeholders, including those outside the TAS that may interact with the subject of certification. In this stage the applicant should collect information from all stakeholders how the change will impact them, and include this information in the definition of the change.

Recommendation 04: It is recommended to ASCOS to provide an extensive explanation about the following topics with examples of logical argument structures in guidance material:

- The level of detail of the claims and sub-claims;
- The process that can be followed for decomposing the claims;
- How to address safety management requirements, and in which claim;
- How to reduce the effort or complexity of the logical argument structure;
- How to take into account whether associated regulations already exist, and how to do this;

Recommendation 05: It is recommended to ASCOS to change the nomenclature in the logical argument structure and to adapt the argument template(s) to make it generally applicable, including to the certification of organisations and operations. The D1.3 report on the ASCOS approach seems rather focused certification of a (system) change, whereas it should be broadly applicable. The case study D4.3 shows that it is more appropriate to focus on the 'subject of certification' or the 'scope of the certificate' rather than 'a change X' as D4.3 focuses on the certification of an organisation. It is recommended to change the definitions and explanation such that the approach focusses on the certification of the performance of a function (which can be fulfilled by an operation, procedure, system, etc.).

Recommendation 06: It is recommended to ASCOS to adapt the terminology used in the guidance material on the ASCOS certification approach so that it is understandable for a wide range of users and all domains.

Recommendation 07: It is recommended to ASCOS to provide guidance to stage 2 about the development of the argument decomposition, and on how to link the common, detailed certification activities to the high-level logical argument approach. Guidance material needs to explain what kind of decomposition of the claims

could be followed for a change that is of an organisational nature rather than of a technical nature and what process can be followed to satisfy these Claims in such cases.

Recommendation 08: It is recommended to ASCOS to explain in guidance material how domains and stakeholders should work together and coordinate in the ASCOS certification approach and logical argument structure development. Guidelines should address:

- How to define jointly for each involved stakeholder the change (e.g. operational, organisational, functional, and system description);
- How to organise traceability of involvement of stakeholders in the different elements of the argument structure (e.g. in claims);
- How to develop and agree upon safety targets and risk criteria (e.g. severity levels, safety objectives definitions, risk matrices);
- How to develop and agree upon a process to allocate safety objectives or design requirements across stakeholders and domains.
- Where and when coordination between stakeholders and domains needs to take place. It should explain at which stage in the process the safety targets are to be defined, and who is responsible for the overall TAS safety target.
- How the logical argument structure should include the roles and responsibilities of different certifying authorities and stakeholders.

Recommendation 09: It is recommended to EC and EASA that the adoption of the ASCOS certification approach will be accompanied with organisational changes in the current certification process such that responsibilities of certifying authorities and stakeholders are clearly defined within the Total Aviation System and taken into account in the argument structure.

Recommendation 10: It is recommended to ASCOS that guidance material explains how the argument structure should cover the issue of which authorities or regulators are involved and how to deal with a case where multiple regulators are involved. The guidelines should explain:

- How to identify applicable safety targets across stakeholders and domains;
- How to agree on a single safety target for the TAS that is acceptable to all domains and stakeholders, or how to handle different safety targets for different domains in a single argument structure;
- How to determine the contribution of each stakeholder to the safety objective, and how to properly allocate (share) safety requirements (e.g. what sort of “formula” can be used to distribute safety requirements);
- How the tool for safety risk assessment and tool for continuous monitoring can be used to determine the current risk level for the TAS and/or domains, which may be used as a basis to demonstrate an equivalent level of safety in case the regulations do not provide a specific safety target.

Recommendation 11: It is recommended to ASCOS to explain in guidance material how the net safety effect can be determined and how the aforementioned situation can be addressed.

Recommendation 12: It is recommended to EC and EASA to develop a process and method to 1) allocate an overall TAS level safety target to domains and stakeholders in a performance based certification approach and 2) determine the acceptability of the net safety effect of the introduction of a certification subject or change in the TAS.

Recommendation 13: It is recommended to ASCOS that the description in D1.3 is updated to reflect the characteristics of the FHA. The added value of stages 4 and 5 would be increased if the approach is not focussed on mitigation of failure conditions or hazards, but also on achieving a certain performance level by the intended function and its design.

Recommendation 14: It is recommended to ASCOS to define 'hazard' in guidance material using the wide definition of hazard, i.e. "any condition, event, or circumstance, which could introduce an accident" (refer to the ICAO Safety Management Manual).

Recommendation 15: It is recommended to ASCOS to explain in guidance material that in stage 4 sub-claims are specifically directed to hazards in the various domains across the TAS (e.g. flight technical, flight operational and ATM) such that responsibilities for mitigating these hazards can be clearly assigned to specific stakeholders. The scope of the hazards that are dealt with in stage 4 should be clarified. It concerns:

- hazards that are pre-existing and which the subject of certification aims to mitigate,
- hazards that are pre-existing which may or may not be mitigated by the subject of certification,
- hazards due to the introduction of the change.

Recommendation 16: It is recommended to ASCOS to explain connecting common FHA and PSSA approaches to the logical argument structure. Furthermore, guidance material should define that the high level safety requirements need to be developed for all claims in the argument, and covers functions, operations, organisations, SMS etc.

Recommendation 17: It is recommended to ASCOS to provide guidance concerning the consistent application of safety objectives over the various domains of the Total Aviation System.

Recommendation 18: It is recommended to ASCOS that guidelines are developed to explain how a safety objective that is supported or "delivered" by different stakeholders can be allocated or "shared" across stakeholders. It is remarked that two case studies mentioned that besides safety requirements, requirements related to quality, integrity, availability, continuity, performance etc. for all types of functions could be shared between stakeholders (in and outside the TAS).

Recommendation 19: It is recommended to ASCOS to explain in guidance material the "power" of the current tools for continuous safety monitoring and safety risk assessment, their differences and similarities.

Recommendation 20: It is recommended to ASCOS to address in guidance material the following potential applications of the continuous safety monitoring tool within the 11 stages of the certification approach.

Stage 1 (Definition of the change)
The tool can be used to derive the current safety performance in areas that are relevant for the change. As a result the applicant is made aware of the actual safety performance in the TAS in the domain(s) of interest. These data may be used to define the current risk level as a basis for safety target setting as part of the argument structure that defines the applicable safety criteria in stage 2. It may also be used to assess the potential safety impact of the change in the TAS.

Stage 2 (Define the certification argument) and stage 3 (Development of certification plan)
In the development of Claim 5, "The service(s) introduced by change X will continue to be demonstrated as acceptably safe in operational service", the tool and supporting SPI framework can be used to define the SPIs that need to be monitored to ensure continuous monitoring and feedback on the safety performance of the approved "change" or certification case.

Stage 4 (Specification) and stage 5 (Design)
The tool for continuous safety monitoring can provide accident/incident statistics, complementary to the data from the tool for safety risk assessment. These data may for example provide input to the Fault Tree analysis of an applicant. However, it remains to be seen whether the current maturity level, completeness, reliability of the ECCAIRS dataset is sufficient to use these data to adapt the quantification of the ESDs and FTs in the ASCOS risk model in the tool for risk assessment. Note that the OEMs get operational data directly from the end-users, and not through ECCAIRS. ECCAIRS may be just one of the many data sources that need to be considered to collect operational (safety) feedback for stage 4 and 5.

Stage 9 (Define arrangements for continuous safety monitoring)
The tool can be used to identify existing SPIs, to assess the feasibility of new SPIs specific for the certification case, and to implement those new SPIs.

Stage 11 (Ongoing monitoring and maintenance of certification)
It is useful for the applicant and authority to collect feedback on the operational performance of the implemented change. The applicant may use these data for instance in the context of product support, design improvements, reliability improvements, safety enhancements etc. For the authority the operational (safety) performance feedback loop will provide input to a continuous operational safety process. For instance, based on safety performance feedback (e.g. occurrence data) in combination with a risk assessment, an authority can decide to issue an airworthiness directive in case of a detected safety deficiency in the design, or it may decide to develop new regulations or specifications to reduce certain risks and improve aviation safety. The tool can support this stage by performing the actual monitoring of the safety performance of the TAS and the certification case. The tool also enables the monitoring of assumptions made in the certification case, which requires that appropriate SPIs are defined in stage 9 to do so. This type of monitoring provides feedback to the applicant and certifying authority about the safety performance in service compared to the performance assumed during certification. This information can be used to update the certification argument (safety case).

Recommendation 21: It is recommended to ASCOS that domain(s) and stakeholder(s) are allocated to the risk model elements.

Recommendation 22: It is recommended to ASCOS to further develop the airport and ATM related parts of the ASCOS risk model. Eurocontrol has developed a similar risk assessment tool, called IRP or AIM, that can be used to analyse risks and assess the impact of changes to the ATM system. It is proposed to consider using IRP/AIM (sub)model elements in the ASCOS risk model.

Recommendation 23: It is recommended to ASCOS that guidance material will describe how to solve the following issues:

- How exactly can the safety risk assessment tool assist in identifying Design Safety Requirements, specifically considering that the events and faults in the risk model are generally at a different level than the logical elements at which the Design Safety Requirements need to be identified?
- It is unclear to what level the ESDs and Fault Trees need to be decomposed to assess how the various stakeholders work together to satisfy the high level safety requirements.

Recommendation 24: It is recommended to ASCOS that guidance material explains the potential use of the tool in the following stages.

Stage 1 (Definition of the change)
The tool can be used to derive the current risk picture for the TAS, including different domains and stakeholders. As a result the applicant is made aware of the actual risks or safety performance in the TAS in the domain(s) of interest. These data can be used to assess the potential safety impact of the change in the TAS and to define the current risk level as a basis for safety target setting as part of the argument structure that defines the applicable safety criteria in stage 2. The ASCOS guidance material should explain how the tool for safety risk assessment can be used as part of stage 1 and explain its value and difference compared with the tool for continuous safety monitoring.

Stage 2 (Define the certification argument)
The tool can be used to derive and allocate safety objective/requirements as explained in section 4.3.3. The ASCOS guidance material should include a process to ensure that the tool reflects correctly the operational environment and scenarios if it is to be used by multiple stakeholders for safety objective allocation. In addition, guidance material should explain what process to follow for the allocation of safety requirements to human factors (events related to human performance).

Stage 4 (Specification)
When the topic of certification is a technical system, stage 4 includes a FHA where the hazards are 'driven by' the functional design. In these cases the tool cannot properly provide a functional hazard identification and assessment.

Stage 5 (Design)
The tool can support stage 5 when a PSSA is conducted. The ASCOS risk model and tool can be used as an overall safety assessment model/tool for the TAS, integrating 'local', case specific risk models from different domains or stakeholders (provided that these models use similar modelling techniques). Although the Fault Trees are not yet developed to the level of detail that is immediately useful for application in a certification case, the tool is flexible so that the safety practitioner can update, modify and expand the risk model (ESDs and Fault Trees) as required.

Recommendation 25: It is recommended to FAST to provide an assessment of the timeframe within which the change and future hazards are expected to develop. This would prevent applicants to do such an assessment based on their own perception without knowing the precise background of the AoC. In addition, it is suggested to better structure and classify the FAST AoC list and to enable search according to the main topic, domain, time frame and geographic function to improve the usability.

Recommendation 26: It is recommended to ASCOS to provide guidance on the use of the FAST AoC list in stages 1, 4 and 5 to ensure that the FAST AoCs are consistently interpreted, understood and applied in the definition of the change (stage 1), in the hazard identification, in the specification (stage 4) and design (stage 5). In stage 1 the first step would be to identify all relevant AoCs and to determine which AoCs should be considered for the subject of certification in the short term and which AoCs may become relevant for the subject of certification in the long term. During the specification and design, and possibly in the safety assessment prior to a change, only the AoCs of significant importance could be considered. 'Significant importance' could be determined for example by the degree of the effect of the AoC on the certification case or the time horizon in which the AoC may impact the certification case. An AoC that will occur in the short term needs to be addressed more urgently in the specification and design stages than a long term AoC. Addressing long term AoCs can be undertaken by Safety Management Systems (SMS) and continuous safety monitoring processes in due course.

Recommendation 27: It is recommended to ASCOS to link the FAST AoCs and related hazards to the risk model elements in the tool for safety risk assessment. If the link between the AoC and the main accident categories, the accident scenarios, Event Sequence Diagrams and/or Fault Tree elements can be established, then the user of the FAST AoC list may be able to identify how the AoC affects the safety of the TAS. The applicant can use this information to determine which accident scenarios are relevant to consider during certification.

Recommendation 28: It is recommended to ASCOS that guidance material for the application of the FAST AoCs and hazards in the ASCOS certification approach stages includes the following activities:

- Identify relevant FAST AoCs and hazards in stage 1 for the certification subject.
- Determine for each FAST AoC if there is a short-term significant relevance, or whether the AoC could be addressed in the future as part of the safety management systems or continuous safety monitoring process. This step aims to identify which AoCs and hazards should be addressed in the current certification case compared to those that can be addressed in the future. If the AoC is to be

addressed in due course as part of the SMS or continuous safety monitoring process, then the arrangements for this activity should be developed in stage 2.

- After identifying the relevant FAST AoCs and hazards for the certification subject, the tool for risk assessment can be used to identify relevant accident categories, accident scenarios and risk model elements for further consideration in stages 1, 4 and 5.
- Assess the potential impact of the FAST AoCs and their related hazards on the subject of certification, i.e. consider these hazards as part of the stage 4 and 5 complementary to the “FHA” or ”PSSA” type of analysis. Especially in stage 5, when the concept or system design is developed, the applicant could take into account the expected FAST AoCs and hazards. Three situations may occur:
- There is no impact foreseen of the AoC, so no further assessment is needed.
- The FAST AoCs and their hazards are a cause for (new) hazards in the context of the subject of certification or they are relevant for the safety of the change. This may require for example further risk assessment or design considerations.
- The subject of certification will have an impact on the FAST AoC or its hazards, and this would require an assessment of the safety effect of the subject of certification on the FAST AoC and hazards (this could also be input to stage 1).

Recommendation 29: It is recommended to ASCOS to improve guidance material about how the effort of different stakeholders can be integrated and coordinated along the system lifecycle. This can further improve the ASCOS contribution to cross-domain integration (KPA 3).

Recommendation 30: It is recommended to ASCOS to address in guidance material the issues related to risk acceptability across the TAS, development of the safety argument structure and roles and responsibilities of the stakeholders. This can contribute to the acceptability of the approach (KPA 5).

Recommendation 31: It is recommended to ASCOS to develop guidance material to support the identification of organizational hazards and associated (safety) requirements to increase the feasibility of the approach to the certification of services and organizations (KPA 7).

Recommendation 32: It is recommended that ASCOS informs EASA and national CAAs of these potential issues so that they can be considered if changes are made to regulations.

Recommendation 33: It is recommended to ASCOS to include the ICAO definition of a hazard in its guidance material.

Recommendation 34: It is recommended to ASCOS to alert the users of the ASCOS approach to the different definitions of hazard, safety objectives, level of scenarios and development assurance that exist in assessment methods in various TAS domains and to advise using common definitions if these different methods are applied in a single certification case.

Recommendation 35: It is recommended to ASCOS to refrain from introducing ASCOS-specific terminology. See also recommendation 06.

References

Authors(s), Title, Year	
1.	ASCOS D1.3: Outline proposed certification approach, A. Simpson, S. Bull, T. Longhurst, v1.2, 18-12-2013.
2.	ASCOS D3.2, Risk models and accident scenarios, A.L.C. Roelen, J.G. Verstraeten, V. Bonvino, J.-F. Delaigue, J.-P. Heckmann, T. Longhurst (CAAi), L. Save, version 1.3, 21-08-2013.
3.	ASCOS D2.4, Tools for continuous safety monitoring, Reinhard Menzel, Wietse Post, Simone Rozzi, Luca Save, version 1.1, 25-11-2014.
4.	ASCOS D3.3, Tool for risk assessment, User Manual, H. Udluft, P.C. Roling, R. Curran, version 1.2, 16-1-2014
5.	FAST Areas of Change Catalogue: Ongoing and future phenomena and hazards affecting aviation, compiled by the Future Aviation Safety Team, February 19, 2013.
6.	ASCOS D4.1, Use Case: Aircraft System Failure Management, J.F. Delaigue, J.P. Heckmann, J. Teyssier, S. Bravo Muñoz, G. Temme, E. van de Sluis, M. St Stuip, S. Bull, version 1.0, 25-2-2015.
7.	ASCOS D4.2, Certification of an Automatic Aircraft Recovery System – AARS, P.J. van der Geest, J.A. Post, M. Stuip, E. van de Sluis, S. Bull, G. Temme, S. Bravo Muñoz, version 1.0, 21-2-2015.
8.	ASCOS D4.3, Case study for the testing of a novel certification approach, certification of an organisation, J.J. Scholte, S. Bull, G. Temme, S. Bravo Muñoz, A.D. Balk, N. Aghdassi, version 1.0, 16-2-2015.
9.	ASCOS D4.4, WP4.4 Integrated Surveillance Use Case Initial Certification Approach, F. Orlandi, B. Pauly, H. Neufeldt, S. Bull, version 0.4, 10-2-2015.
10.	ASCOS risk assessment tool, available on http://www.ascos-project.eu/risk-tool
11.	Leveson, N.G., Engineering a safer world, Systems thinking applied to safety, 2011
12.	ASCOS D5.1: Validation Strategy, R. Wever, L. Save , S. Rozzi, T. Longhurst, v1.2, 31-08-2014
13.	ASCOS D2.3 Process for Safety Performance Monitoring, A. Iwaniuk, P. Michalak, G. van Es, B. Dziugieł, W. Miksa, M. Mączka, N. Aghdassi, R. Menzel, L. Save, v1.0, 21-03-2014.
14.	Bull, S., Briefing on Stage 4 Assessment for WP4.3, EBENI P12011.43.1.3 (0.3), 11th July 2014.
15.	Bull, S., Briefing on Stage 5 Assessment for WP4.2, EBENI P12011.42.1.4 (0.1), 6th October 2014.
16.	ED78A Guidelines for approval of the provision and use of air traffic services supported by data communications, December 2000.
17.	ASCOS Briefing on Stage 5 Assessment Process for WP4.2, P12011.42.1.4.
18.	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.
19.	ASCOS D2.1 A.L.C. Roelen, J. Verstraeten, L. Save, N. Aghdassi. Framework Safety Performance Indicators. ASCOS D2.1, version 1.5, 14-01-2014.
20.	ARP4754A/ ED-79A - Guidelines for Development of Civil Aircraft and Systems - Enhancements, Novelties and Key Topics.
21.	JARUS Scoping Paper to AMC RPAS.1309, Remotely Piloted Aircraft Systems – System Safety Assessment, Issue 1, January 2014.
22.	Certification Specifications, CS-25, EASA.
23.	ASCOS D1.2, Definition and evaluation of innovative certification approaches, U. Dees, P. van der Geest, A. Simpson, S. Bull, P. Blagden, T. Longhurst, A. Eaton, G. Temme, B. Pauly. Version 1.3, 20-08-2013.
24.	ASCOS D5.3, Validation exercises execution, S. Rozzi, L. Save, M. Torelli, R. Wever, B. van Doorn, H. Udluft, R. Menzel, W. Post, N. Adhgassi. Version 0.2, 2 April 2015.

Appendix A Outline of the ASCOS certification approach

Appendix A.1 Overview of the approach

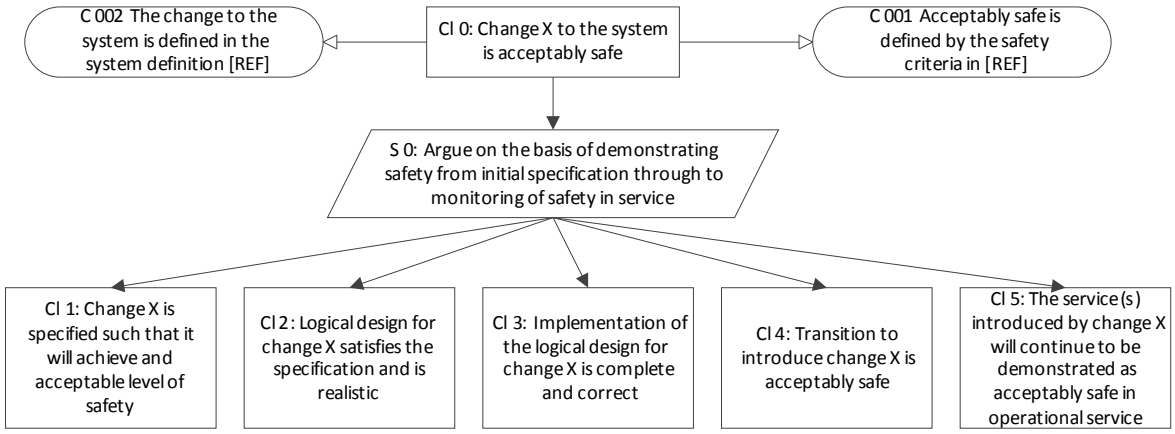
The proposed ASCOS certification approach is to use a logical argument for the certification of any changes to the Total Aviation System (TAS), and support the top level claim that the change is acceptably safe. The argument is then broken down into supporting claims, each addressing a smaller portion of the top level claim. The outline of the ASCOS approach is described in D1.3 [1], which will be updated in WP 1.5 and described in ASCOS deliverable D1.5.

The approach has been successfully used to build logical arguments for complex systems across multiple domains, including Air Traffic Management (ATM). The approach builds on the method adopted by EUROCONTROL and further developed by the Single European Sky ATM Research (SESAR) research programme. It provides the flexibility to retain existing approaches where appropriate, while also supporting certification of novel concepts and systems.

The logical argument approach advances the state of the art by driving unification of the argument across all domains and improving the rigour and consistency in the application of safety arguments.

The logical argument approach will not replace existing certification approaches (e.g. application of current standards) and evidence hierarchies, it will augment the current processes and allow for development of new strategies while identifying and managing gaps and deficiencies in existing certification processes. The logical argument approach can facilitate interactions between individual domains and organisations, allowing for maximum retention of existing certification processes where these remain applicable. It will also enable the integration of different approaches taken in different domains by ensuring the dependencies between each are clearly defined and managed.

The logical argument is developed from a template. The top level of the argument divides into 5 key claims covering the whole lifecycle of the system. Each of these claims is developed further to contain the claims, arguments and evidence required to support higher level claim. At this top level, the argument addresses the whole TAS; the contribution and responsibilities of individual organisations or domains become apparent at lower levels of the argument.



As the logical arguments for each claim are developed further they can quickly become complex, involving multiple organisations across different domains. To manage these, the argument architecture can be clustered together to form a module. Each module encompasses the argument for a particular constituent component of the overall (TAS) argument. Modules are usually defined to coincide with boundaries of organisational responsibility and system interfaces, whilst also considering which parts of the argument are subject to most change. Interaction between modules are captured by assurance contracts, these communicate conditions, context, caveats and dependencies which may exist in a module and need to be adhered to by other modules, in order to make an overall argument. For example an assurance contract will exist between an aircraft manufacturer and operator/maintainer. The manufacturer warrants the safe operation of a system provided it is used and maintained correctly (i.e. as per the manual). Whilst this is a more obvious example the implicit reliance of the manufacturer on the end – user performing correct maintenance actions may not always be fully understood by the end-user.

Appendix A.2 Stages of the approach

The logical argument approach is made up of the following stages:

1. Define the change – Ensure the proposed change to the TAS is fully understood.
2. Define the certification argument (architecture) – development of initial certification argument; top level claim and context.
3. Develop and agree certification plan – Present the certification philosophy to the acceptance authority (ies) and obtain agreement to proposed approach.
4. Specification – Demonstration that claim 1 is met by the change, namely that the change is specified to achieve an acceptable level of safety.
5. Design – Show the logical design for the change satisfies the specification derived within claim 1 thus satisfying claim 2.
6. Refinement of argument – This is a continuous process through all stages of the approach.

7. Implementation – Demonstration that claim 3 is met by the completion and correctness of the physical implementation of the logical design for the change.
8. Transfer into operation: transition safety assessment – Show that the transition to introduce the change is acceptably safe.
9. Define arrangements for continuous safety monitoring.
10. Obtain initial operational certification – Presentation of evidence to authorities in order to introduce change into service.
11. Ongoing monitoring and maintenance of certification

It is important to note that in some instances the steps above may be omitted or combined, depending upon the level of change (whether the change is “minor” or “major”). The logical argument approach supports mapping of argument legs to the E-OCVM lifecycle stages.

If a progressive certification approach is adopted, acceptance would be obtained from the relevant authorities in a staged manner, in order to “de-risk” the achievement of operational certification.

Appendix A.3 Details for stages 1-3 of the approach

Stage 1 – Define the change

The goal of Stage 1 is to provide sufficient definition of the change to support the further stages of assessment. At stage 1 the change should primarily be defined in terms of the concept of operations particularly how the change affects the TAS; the definition of the detailed implementation comes later in the process.

The information gathered at Stage 1 should be sufficient to define the top level of the argument along with any required context. Stage 1 has the following outputs:

- Definition of the overall goal of the change;
- Identification of the change to be made, including:
    - Which organisation is proposing the change;
    - Which organisations are affected/involved in the change, and what their role is;
    - The functional and operational concept of the change;
    - Definition of the timescales for actual implementation;
    - Identification of which elements of the system are affected by the change (e.g. process, products, roles, domains);
- Identification of which requirements (safety and non-safety) need to be fulfilled by the change;
- Creation of a high level architecture, and identification of assurance contracts;

- Identification and consideration of any expected TAS Areas of Change (AoC)[1];
- Determining what existing regulations, certification specifications, standards, AMCs or other relevant guidance material are applicable to the change;

Identification of the regulations, standards AMCs etc. guides the development of the safety argument and the identification of assurance contracts.

Stage 2 – Define the certification argument (architecture):

Unless evident from the outset that an alternative argument is appropriate, the generic argument shown above should initially be adopted and developed further into an argument architecture. The use of generic or alternative argument should not affect the modularisation of the argument, as this is driven by commercial and physical partitions within the TAS.

At this stage the argument should identify any potential impact either from or on assurance contracts or modules outside the initial scope. The argument architecture will follow established certification approaches where these remain appropriate.

The development of the initial argument architecture provides the foundation for development and agreement of the certification plan, at this stage the argument can only be developed to a limited detail, until assessment activities in stage 4 and stage 5 are complete.

Stage 3 – Develop and agree certification plan:

The role of the certification plan is to show how the certification argument architecture will be developed and substantiated with evidence to the point where it can be presented for acceptance by the relevant authorities.

The certification plan presents the argument architecture, along with the certification activities to be undertaken, including how impacts, if any, on existing assurance contracts will be addressed.

It is necessary for the certification plan to define the parts of the argument which require endorsement, and by which authorities. This is because a given change may require endorsement from multiple authorities, each of whom are only competent to endorse part of the system residual risk, and not likely that any one authority can endorse the top level of the argument.

The certification plan is presented to the relevant authorities and other stakeholders, to gain their agreement that, if the plan is followed and the evidence is presented, they will accept the change into service. Agreement at this stage reduces risk that the argument and evidence will not be accepted when formally presented.

This method can be adapted into progressive certification, where agreement is obtained for the argument progressively as the individual claims are completed.

[1] An AoC is a concept introduced by the FAST, it is defined as any (future) phenomenon/events that will affect the safety of the aviation system either from within or from important domains external to aviation

Appendix A.4 Benefits of the approach

The approach has the following benefits:

- ***Single approach considering whole TAS –*** Currently arguments for safety and the supporting evidence are distributed widely between various organisations, and often constructed in isolation:
    - This results in the essential information such as dependencies, context, assumptions or constraints being lost. The logical argument approach builds an integrated argument for each proposed change to the system which identifies issues at the boundaries between domains and facilitates their management.
    - It also makes it difficult to fully consider the impact of any change on the TAS. The logical argument approach supports the consideration of the overall impact of the change.
- ***Reuse of existing processes –*** The existing processes are largely effective at ensuring safety within individual domains, and are well understood. The logical argument approach allows these to be retained for use within their respective domains, and provides the means for integrating them across the domains, while ensuring that any implicit context is fully considered within the overall argument.
- ***Flexibility for novel solutions –*** the logical argument approach allows alternative approaches to be adopted where existing specifications do not cover the change being implemented. Thus allowing for innovation in a) technologies and concepts and (b) certification approaches
- ***Improved communications –*** The logical argument approach provides the framework for improved communications and integration between domains.

Appendix A.5 Ownership of the argument

Effective application of the approach requires an argument architect to take the overall responsibility for the development and maintenance of the argument architecture across all the affected domains. The responsibility of the argument architect extends beyond the introduction of the change, as key elements of the argument will require confirmation throughout the lifetime of the system. The role of the architecture architect can be assumed by a number of actors, and may transfer between parties throughout the lifecycle of the change. Where the change is primarily within a single domain the applicant of the change may be best placed to act as argument architect. However where the change is more widespread, someone with a wider responsibility would be required to ensure implications of the change on the argument are followed through all domains. This requires further exploration.

Appendix B ASCOS tool for continuous safety monitoring

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 [19] while the continuous safety monitoring process is explained in D2.3 [13]. Since the SPI definitions may be subject to reconsiderations and alterations the tool supports the modification and reconfiguration of SPIs.

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 D1.3 [1] 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 [19].

Appendix C ASCOS tool for safety risk assessment

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 [2], the functionalities of the software tool are defined in [18], and the user manual of tool is D3.3 [4].

The ASCOS tool for risk assessment consists of a risk model, i.e. a repository of accident and accident avoidance scenarios. 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.

As D1.3 [1] 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. The risk model can support and enhance safety management in various ways. Report D3.2 [2] 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.