Validation results

Simone Rozzi, Luca Save, Simone Pozzi (DBL) , Rombout Wever (NLR),

Heiko Udluft (TUD), Nuno Aghdassi (AVA), Gerard Temme (CFLY)

The present deliverable summarizes the key results from the ASCOS validation exercises and presents the recommendations for improvement that have been developed in the course of the ASCOS project. These include both recommendations developed in the context of WP5 (Validation) and recommendations developed in the context of the WP4 (Certification case studies). This material provides the basis for future developments of the evaluated ASCOS products. In particular, the recommendations addressing the proposed ASCOS certification approach are addressed by WP1.5, which will deliver a more advanced version of the ASCOS approach than initially proposed in D1.3.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	L. Save (Deep Blue)
Grant Agreement No.	314299
Document Identification	D5.4
Status	Approved
Version	1.1
Date of Issue	27-08-215
Classification	Restricted

This page is intentionally left blank

DOCUMENT CHANGE LOG

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	S. Rozzi et al	25-06-2015	All	Version for PMT approval
1.1	S. Rozzi et al.	27-08-2015		PMT comments processed

REVIEW AND APPROVAL OF THE DOCUMENT

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	J. Scholte, A.L.C. Roelen	29-06-2015
CAAi	T. Longhurst	16-06-2015
JRC	W. Post, R. Menzel	16-06-2015
CertiFlyer	G. Temme, M. Heiligers	29-06-2015
TU Delft	R. Curran, H. Udluft	16-06-2015
Thales Air Systems	B. Pauly	29-06-2015
Avanssa	N. Aghdassi	29-06-2015
APSYS	S. Bravo Munoz, J.P. Heckmann	29-06-2015
Organisation Responsible for Approval	Name of person approving the document	Date
Deep Blue	L. Save	06-08-2015
NLR	L.J.P. Speijker	27-08-2015

DOCUMENT DISTRIBUTION

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

ACRONYMS

Acronym	Definition
ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
ATCMS	ASCOS Tool for continuous safety monitoring
AVG	Average
CAA	Civil Aviation Authority
CATS	Causal model for Air Transport Safety
CMA	Continuous Monitoring Approach
CNS	Communication, Navigation, Surveillance
CPS	Certification Process study
CS	Certification Specifications
D	Deliverable
DOW	Description of Work
EASA	European Aviation Safety Agency
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems
ECF	ECCAIRS Common Framework
ECR	European Common Repository
E-OCVM	European Operational Concept Validation Methodology
ESD	Event Sequence Diagram
EU	European Union
FAA	Federal Aviation Administration
FAST	Future Aviation Safety Team
FDM	Flight Data Monitoring
FT	Fault Tree
GPWS	Ground Proximity Warning System
ICAO	International Civil Aviation Organisation
KPA	Key Performance Area
KPI	Key Performance Indicator
NASA	National Aeronautics and Space Administration
RIMCAS	Runway Incursion and Collision Avoidance System

SESAR	Single European Sky ATM Research
SPI	Safety Performance Indicator
TAS	Total Aviation System
TCAS	Traffic Collision Avoidance System
UG	User Group
WP	Work Package

LIST OF FIGURES

LIST OF TABLES

This page is intentionally left blank

Executive Summary

The present deliverable has two objectives:

1. First, to present a summary version of the results of the validation exercises conducted in the context of ASCOS Work Package 5.3. These exercises collected expert feedback about the fitness-for-purpose of the main ASCOS products by means of structured focus group discussions and questionnaires with certification and safety experts external to the ASCOS project. While deliverable D5.3 described these results in detail, the purpose of this deliverable is to provide a succinct, summarized version of these results functional to the understanding of the recommendations for improvement (which are also reported in this deliverable);
2. Second, to integrate and present all of the recommendations that have been developed in the project. These recommendations have been developed based on both the results of the three validation exercises conducted in the context of the WP5, and based on the experiences of the four certification case studies conducted in the context of the WP4. This latter work package investigated the benefits, lessons learnt and criticalities resulting from the use of the ASCOS certification approach to the certification of four innovative changes to the total aviation system (TAS).

The integration of the recommendations of WP4 and WP5 provides a comprehensive basis for improving the ASCOS products: Because of their research design, the two WPs covered different aspects of the evaluated products. In particular, the WP4 allowed to gain in-depth insights into the actual, low level practicalities of putting the ASCOS approach into use in four “simulated” contexts. The WP5, allowed to probe, by means of focus group discussions and questionnaire, the perceptions of the target users of the approach, i.e. certification and safety experts, about potential issues that have to be considered during the deployment of the approach in real life certification contexts. Thus the two WPs collected complementary data and generated a complementary set of recommendations that are presented in an integrated manner in this report.

Altogether, these recommendations will serve the purpose of informing future improvements of the evaluated ASCOS products. In particular, ASCOS WP1.5 will consider the recommendations presented in this deliverable in order to deliver a more refined, advanced version of the proposed ASCOS certification approach—a version more refined and advanced compared to the initial outline of the approach documented in deliverable D1.3. The other products—the SPIs framework, the ASCOS Tool for continuous safety monitoring, the ASCOS Risk Model and the ASCOS Tool for risk assessment—will not be specifically addressed by WP1.5, however the recommendations pertaining to these ASCOS products will be a useful resource for future research on the same topics.

Table of Contents

This page is intentionally left blank

1 Introduction

1.1 ASCOS Projects Background

ASCOS is an EU funded project aiming at bringing improvements in the certification practices of aeronautical products, operations and systems. The project delivers novel processes, supporting software tools and methodologies that are expected to increase the efficacy and efficiency of certification practices. More specifically, ASCOS should make the certification of (new) operations, systems and products safer, more cost-effective, more flexible, and more integrated across the different domains of the Total Aviation System [1]. Collectively, such enhancements are expected to translate on a reduction of fatal accidents due to loss of control in flight, aircraft system or component failure or malfunction, aircraft ground handling damage, and Air Traffic Management related incidents and accidents. These are the five top commercial air transport accident categories that include the higher number of fatal accidents. The established ASCOS User Group is involved in various stages of the project to keep the project focused and to facilitate the uptake of project results. They have an important role to play in the validation effort of the ASCOS products.

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

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

ASCOS WP5 is dedicated to the validation of ASCOS products and consists of four work packages:

- WP5.1 Validation Strategy;
- WP5.2 Validation Plan and Scenario;
- WP5.3 Validation Exercises and Execution;
- WP5.4 Results Analysis and Reporting.

To date, the WP5.1, WP5.2, and WP5.3 have been completed and their results are available under deliverables D5.1 : *Validation Strategy* [2], D5.2: *Validation Plan and Scenarios* [3], and D5.3: *Validation Exercises Execution* respectively [4]. D5.1 document applied the seven steps promoted by E-OCVM[5]—the EUROCONTROL standard validation framework—to the definition of ASCOS validation strategy. Deliverable D5.2 further refined this strategy by breaking it down into three validation plans for three different validation exercises. For

each exercise, the document reported aspects such validation objectives, methodology, roles, etc. Essentially, D5.2 completed the preparatory phase of the ASCOS validation exercises, while D5.3 reported on the results of these exercises. The three validation exercises collected feedback about the fitness-for-purpose of the main ASCOS products by mean of structured group discussions and questionnaires administered to selected experts external to the ASCOS project. The table below provides a summary view of the three ASCOS validation exercises, the product they evaluated, the structure of the exercises, and the dates in which the exercises took place (for more information the reader is referenced to the D5.3 [4]).

Table 1. Summary table of the three Validation Exercises carried in the context of WP5.3.

Validation Exercises	Evaluated ASCOS Product	ASCOS Reference	Structure of Exercise	Dates
Exercise 1	• ASCOS initial proposed certification process adaptations	D1.3 [6]	• Feedback gathering	10th Oct 2014 (2nd Day of ASCOS UG meeting 3)
Exercise 2	• ASCOS SPI framework • ASCOS software Tool for continuous safety monitoring	D2.1 [7] D2.4 [8]	• Familiarization • Feedback gathering	28th Nov 2014
Exercise 3	• ASCOS Risk Assessment Model • ASCOS Tool for risk assessment	D3.2.3 [9] D3.3 [10]	• Familiarization • Interactive session • Feedback gathering	14th Jan 2015

The present deliverable summarizes the main results of the three validation exercises, which provided the basis for the development of a set of WP5 recommendations. For the sake of simplicity, the deliverable also integrates the recommendations developed in WP4.5 and previously documented in ASCOS deliverable D4.5[11]. Note that WP4 was executed in parallel with WP5 and consisted on applying the initial proposed certification approach and supporting tools to four certification case studies pertaining to the certification of: (i) an Automated Failure Management System; (ii) an Automatic Aircraft Recovery System (AARS); (iii) an independent de-icing/anti-icing service provider; (iv) an Integrated Surveillance System (ISS) consisting of cooperative surveillance and independent non-cooperative surveillance systems. The application of the initial proposed certification approach and supporting tools to four certification cases allowed to identify potential benefits of the ASCOS products as well as areas that could be the target of future improvement.

Figure 1 shows the interaction between ASCOS WP5 and ASCOS WP4. Both WPs entailed some evaluation activities: In WP5, three validation workshops collected feedback from certification and safety management experts external to the ASCOS project. In WP4, the feedback was generated from the application of the ASCOS certification approach to four case studies for the WP4 by mean of selected partners internal to the project. The two evaluation perspectives led to a set of recommendations that are here presented in an integrated and complete manner.

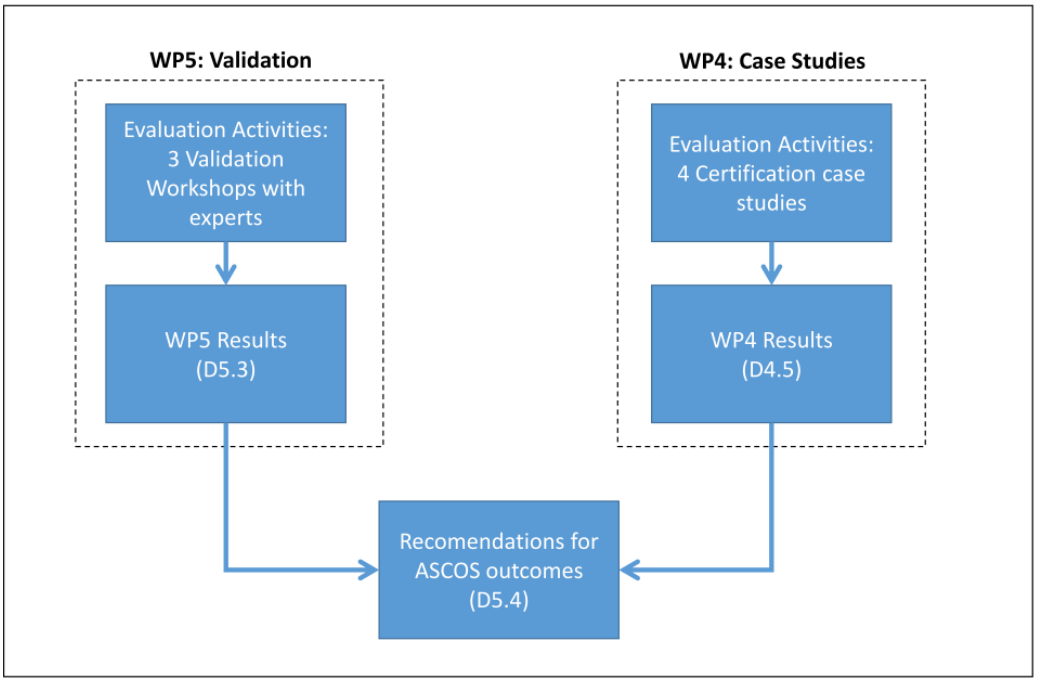

Figure 1. Integration of ASCOS WP4 and WP5.

1.2 OBJECTIVE

The present deliverable has the following two main objectives:

1. To develop the full set of **WP5 recommendations**, i.e. the recommendations developed in the context of WP5 and based on the results of the three validation exercises carried out in WP5.3 (note that 5.3 had an evaluative purpose only and did not contain yet recommendations for improvement).
2. To present, in an integrated manner, **the full set of recommendations developed by both WP5 and WP4**. This latter work package identified benefits and lessons learnt, as well as specific recommendations for improvement, based on the application of the ASCOS certification approach to four case studies about innovative changes to the total aviation system (TAS). The four cases, in particular, explored the value of the ASCOS approach in the initial phases of certification.

The integrated presentation of the complete set of WP4 and WP5 recommendations is intended as a way to provide an easy access to all the proposals for improvement both internally and externally to ASCOS. Internally to ASCOS, the recommendations are addressed to WP1.5 (Consolidation of new certification approach). While externally to ASCOS, they are intended for future research and development activities in the same area. When applicable the areas of overlaps, mutual support or contrast between the recommendations of the two WPs will be highlighted.

1.3 DOCUMENT STRUCTURE

The remainder of this document has dedicated sections for each of the evaluated ASCOS products. For each product the document reports:

1. A summarized version of the **key results of the WP5 validation exercises**, as executed in WP5.3 [4]. This summary version of WP5.3 results is intended to provide the reader with basic background information needed to understand the WP5 recommendations (see point 2). Also, these results are organized around key areas of performance, or KPAs. These KPAs capture important areas of performance that are relevant from a stakeholder viewpoint and which were elaborated taking into account the originally expectations in terms of ASCOS benefits. A description these KPAs and of their development is available in Appendix A. To note that for each KPA, the deliverable only reports a summarized version of the main validation results. For more details the reader is referenced to the original ASCOS validation report D5.3[4].
2. The complete set of the **WP5 recommendations** for improvement, i.e. the recommendations that have been developed based on the results of the WP5 validation exercises. Such recommendations represent the main contribution of this deliverable and are identified by two numbers. The first number represents the ASCOS product they refer to (1 for the ASCOS Certification Approach, 2 for the SPI Framework and the Tool for Continuous Safety Monitoring, 3 for the Risk Model and Risk Assessment Tool). The second number is just a progressive number. For example “1.03” is the third recommendation (i.e. 03) concerning the ASCOS Certification Approach (i.e. 1).
3. The complete set of the **WP4 recommendations**, i.e. the recommendations that have been developed in WP4.5, based on the experience of implementing the ASCOS products in the four WP4 certification case studies. These recommendations are reported here for the purpose of completeness, but have been originally documented in ASCOS deliverable D4.5. They will be referred to with the same progressive number they had in D4.5, but with the indication “WP4 recommendation” to make it clear their origin and distinguish them from the WP5 recommendations.

To note that in reporting the WP5 recommendations it emerged that some of them have a clear linkage with one or more of the WP4 recommendations. Whenever such linkage emerged, the related WP4 recommendation(s) has (have) been copied in a dedicated box at the end of the section describing the WP5 recommendation.

Some variations from the basic three-point structure described above apply, as not all the three points (WP5 Results, WP5 Recommendations, WP4 Recommendations) have been equally covered for each evaluated ASCOS product (as shown in Table 2). In particular, no WP4 recommendations have been reported relative to the ASCOS SPI framework, since the D4.5 did not contain findings and recommendations dedicated to this product specifically. Similarly, neither WP5 results nor WP5 recommendations have been reported relative to the FAST areas of change (AoC), as these products were not addressed by the WP5 validation exercises.

Table 2. Contents of the report at a glance.

ASCOS Evaluated Product	Section	Summary of main WP5 Results	WP5 Recommendations	WP4 Recommendations
Initial proposed ASCOS certification approach	§2	●	●	●
ASCOS Safety Performance Indicators framework	§3	●	●	*n.a.*
ASCOS Tool for continuous safety monitoring	§4	●	●	●
ASCOS Risk Model	§5	●	●	●
ASCOS Tool for Risk Assessment	§6	●	●	●
FAST Areas of Change	§7	*n.a.*	*n.a.*	●

Note that the following ASCOS products have not been addressed in this document:

- Process for safety performance monitoring (including precursors associated with SPIs) (see D2.3 [12]);
- Safety assurance process in operation (see D3.5 [13] and D3.6 [14]);
- Lessons Learned Requirements Process (see D3.5 [13] and D3.6 [14]);
- Overall safety impact assessment method (see D3.4 [15]).

The ASCOS Final Report (D7.2) and Exploitation Plan (D6.4) provide more insight into these ASCOS products.

2 ASCOS Initial Proposed Certification Approach (WP1 outcome)

2.1 SUMMARY OF MAIN WP5 VALIDATION RESULTS

This section reports a summary of the main validation results that were documented in D5.3 and that addressed at the initial proposed ASCOS certification approach.

2.1.1 KPA1: Effort

This section reports the impact on effort, i.e. 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. The key results for this KPA include the followings:

- The use of the ASCOS certification approach may increase the coordination effort needed to gain the initial type-certificate. This is the case because more specialists are expected to be involved compared to current certification practices. The increase in the number of specialists involved is due to the fact that, first, experts from different domains—and not just one--will have to be involved. And, second, new types of specialists will be required: The implementation of the approach will require in fact specialist familiar with risk assessment across the Total Aviation System, rather than single domain risk assessment. In conclusion, the ASCOS certification approach is likely to require a larger set of specialists compared to today, specialists whose effort will have to be coordinated.
- Furthermore, the expected increase in interactions between different organizations, as introduced by the approach, is likely to increase the effort required for considering legal aspects in certification.
- At the same time, possible reductions in the overall certification effort are deemed possible when considering the whole lifecycle of a change, and not only the initial certification approval phase. The ASCOS approach has the potential to reduce the risk of delays and major reworks later on in the process caused by relevant hazards becoming evident (too) late during the certification process.
- Also, the approach requires that appropriate resources are dedicated to the training of staff from both authority and applicant organizations. ASCOS requires specialists competent with safety argument, scoped at TAS level, and specialists in cross-domain risk assessment. These skills are not currently available in authority and applicant organizations, and therefore will need to be developed to adopt the approach. On the positive side, these skills adds to, and do not replace, existing knowledge and skill bases of authorities and applicants.

2.1.2 KPA2: Soundness

This section reports the impact on soundness, i.e. the extent to which the initial proposed ASCOS certification approach promotes 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. The key results for this KPA include the followings:

- The ASCOS certification approach places a strong focus on cross-domain hazards and safety requirements identification. Since the initial certification phase, the approach emphasizes the

identification of the affected domain potentially affected by the change, and how hazards and risks can be propagate there. This enlarged focus may promote a more comprehensive consideration of relevant safety hazards and requirements since the initial certification phases, and may reduce the likelihood of these hazards and requirements being missed or identified too late, when they will have already materialized into incidents and accidents.

- This increased capability of the approach to address more safety issues compared to today's approach will heavily depend on the expertise of the people involved—rather than solely on the formal steps of ASCOS certification process. In other words, the actual application of the approach requires further definition of roles, team composition, processes, process owner, than specified in D5.3.
- Another aspect that limits the potential of the approach to deliver in the area of soundness is the current lack of clarity about how human factors will be better considered in certification compared to today. From ASCOS validation exercise 1 it emerged that this aspect requires further consideration in the project.

2.1.3 KPA3: Cross-domain integration

This section reports the impact on cross-domain integration, i.e. the extent to which the ASCOS approach promotes integration, coordination, and exchange of information across the different stakeholders that may be involved in the certification of a change. The key results for this KPA include the followings:

- ASCOS has the potential for cross-domain integration; however this potential heavily depends on the availability of supporting regulation(s) mandating the sharing of safety risk information across the TAS stakeholders involved in a change. OEMs involved in a change may be reluctant to share safety risk information—e.g. safety hazards, requirements, risk models—because of confidentiality reasons. Therefore, the implementation of the approach requires that appropriate regulatory mechanisms are established to promote the sharing of safety risk information across the stakeholders involved in a change.
- Also, the roles and responsibilities of the TAS architect(s) should be further specified in order to appreciate the potential for improved coordination;

2.1.4 KPA4: Harmonization

This section reports the impact of the proposed ASCOS certification approach on harmonization, i.e. the extent to which ASCOS looks compatible with the different certification approaches in use in different domains (e.g. ATC vs aviation) and geographical areas.

- The approach looks compatible with existing certification approaches—either performance or compliance based—used across different domains. During the validation exercises the expert opinion was that the approach did not appear to conflict with existing approaches.

2.1.5 KPA5: Accommodation of innovation

This section reports the impact on accommodation of innovation, i.e. the extent to which ASCOS makes more likely the certification of innovative products and systems, i.e. products and systems for which no standard are available. One key result emerged for this area:

- The ASCOS approach is expected to increase the rate of success regarding the certification of innovative concepts, i.e. concepts introducing novel types of products, systems, or services which have no equivalent analogue in current operations. For this of type concepts, certification is notably difficult because they are no addressed by existing standards. For these concepts, the ASCOS approach makes certification more feasible, because it adds more clarity and structure to a certification process that is usually perceived as a highly uncertain for the applicant.

2.1.6 KPA6: Acceptability

This section reports the impact on acceptability, i.e. the extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority. The key results for this KPA include the following:

- Acceptability by both applicants and the certifying authorities may be challenged by the perceived significant effort required to adopt the approach. For both the applicant organizations and certifying authority the adoption of the approach may require significant effort and training.
- There is an expectation that national CAAs will see the approach as more helpful (and therefore more acceptable) for airports and ATM, since these domains are more performance based compared to aircraft system certification (which is compliance based);
- The wide spread adoption of the approach will be promoted by the acceptance of leading OEMs. In other words, the adoption can be promoted if large OEMs will see a commercial benefit in adopting the approach.

2.1.7 KPA7: Flexibility

This section reports the impact on flexibility, i.e. the extent to which the proposed ASCOS approach can be applied to a broad range of different types of products, systems, and services, varying in size and complexity. The key result for this KPA include the following:

- The approach seems more promising for innovative products for the reasons explained in relation to KPA5. The approach looks however potentially less useful for derivatives changes, i.e. changes for which an initial (pre-existing) certification base applies;
- It was difficult to estimate the potential for certifying novel services, such as independent de-icing operations—because this type of change is not covered by a dedicated certificate nowadays.

2.2 WP5 RECOMMENDATIONS

This section reports the full set of recommendations related to the initial proposed ASCOS certification approach. These recommendations have been developed based on the results of the first WP5 ASCOS validation exercises [4]. Note that:

- Some of the WP5 recommendations turned out to be similar or complementary to some of the recommendations developed by the WP4 (and documented in the deliverable D4.5 [11]). In these case, the relevant WP4 recommendation(s) has(have) been included into dedicated boxes at the end of the description of the concerned WP5 recommendation;
- Some of the WP5 recommendations have been consolidated during a coordination meeting between the WP4 and WP5 [16]. This meeting allowed to compare and check for differences and similarities between the recommendations developed by the two WPs. The recommendations consolidated during the meeting in question are identifiable by the label "(WP4-WP5)", which appears at the end of their headings.

2.2.1 REC 1.01: Define the minimum set of roles that should be involved in the use of the ASCOS certification process (WP4-WP5)

This recommendation is concerned with further defining the roles involved in the deployment and use of the ASCOS certification approach. At present, the main role included in the description of the guidance material described in ASCOS D1.3 is the "safety argument architect". However, more guidance need to be provided concerning the other roles involved in the application of the ASCOS approach.

In defining the structure of organizational roles and responsibilities, it is suggested to clarify, for each role, the high level set of responsibilities, expertise, and tasks. In particular, it is recommended to present at least a minimum set of roles including: the applicant, the safety argument architect, the authority and the representatives of other involved domains. It is acknowledged that it may be difficult to fully define the roles of the ASCOS certification approach; however, providing further detail on them is desirable. A useful basis for this exercise comes from section 7 of ASCOS deliverable D3.5a [13] (reported also in Appendix B of this document). That section provides an initial high-level definition of the organizational actors involved in the initiation, promotion, coordination, and monitoring of multi-stakeholders safety assurance activities. In particular, the document envisages two relevant types of actors: (i) Multiple local safety groups, i.e. safety groups located within each individual stakeholder organization involved in the change; (ii) one global or inter-stakeholder safety group, i.e. a group external to and placed on the top the individual local safety groups. This latter group is responsible for coordinating the activities of the local safety groups and managing the interfaces among them. To note that this safety management structure was essentially defined for the purpose of safety standard development and improvement. This being said, it is reasonable to assume that the same structure can be reused/adapted for the purpose of further specifying the structure of roles engaged in the execution of the ASCOS certification approach. Also the initiation, development, and monitoring of the TAS safety argument and its sub-modules is likely to require, as a minimum, a structure composed by both local, stakeholder-level roles and a global, inter-stakeholder level role.

Also, in defining the structure or role and responsibilities, the following considerations apply:

- It is suggested to consider the sequence of interactions that the different actors involved in TAS change will go through since the start of the change. In other word, this suggestion points at defining a high-level process indicating how the different roles can interact among each other during the implementation of the ASCOS certification approach.
- It is also suggested to consider the appropriateness of distinguishing between different types of applicants. In the application of the ASCOS approach, multiple applicants may be involved in different stages of the change lifecycle. Thus, it may be needed to differentiate between the applicant that has presented the change to the authority (the change initiator), and other applicants that may be involved later in the process. For instance, the authority may deem necessary to involve in the change some organizations (e.g. training organizations, maintenance organizations), which were not necessarily be considered by the applicant that presented the initial application, and that yet, as a result of the change, these organizations may require an update of their certificates.

Finally, it can be noted that the recommendation described in this section coheres with Recommendations 08 and 29 developed by the WP4.5 [11], which are reported in the box below. Also these recommendations were motivated by the observation that that while the integration of different certification stakeholders is one of the main benefits of the proposed ASCOS certification approach, it is not clear "where, when and how coordination between stakeholders and domains needs to take place in stages 1 to 3" [11]. These considerations point at the importance of providing further guidance about the integration of the different TAS stakeholders during the implementation of the ASCOS certification approach in order to better define how ASCOS can realize its benefits.

WP4 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.

Figure 2. Recommendation 08 from WP4.5 (Source [11])

WP4 Recommendation 29 (D4.5): 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).

Figure 3. Recommendation 29 from WP4.5 (Source [11]).

2.2.2 REC 1.02: Refrain, whenever possible, from introducing novel ASCOS-specific terminology (WP5-WP4)

It is recommended that ASCOS adopts existing definitions and terms whenever available and reduces the use of newly created ASCOS-specific terms to situations for which no existing term exists. This will make the approach more readily understandable for certification and safety experts not familiar with ASCOS. In turn, this will be beneficial for the acceptability of the approach.

2.2.3 REC 1.03: Adopt a consistent definition of "risk"

It is recommended that the risk terminology used in ASCOS is consistent with existing standard risk terminologies. In particular, it was observed that the definition of emerging risk was not immediately clear: ASCOS D3.1 defines it as a "familiar risk that is increasing or new risk that become apparent in new or unfamiliar conditions" [9]. This definition may not be immediately clear to the users of the approach: To them, emerging risks denote new and unknown risks [4]. This latter interpretation of the term is consistent with the usage of the term "emerging" in ICAO Doc 9859 Safety Management Manual [17], which uses the term as opposed to known risks.

2.2.4 REC 1.04: Adopt a consistent definition of "hazard"

It is recommended to provide a clear definition of "hazard". In particular, it is recommended to adopt a definition consistent with the ICAO definition: "any condition, event, or circumstance, which could introduce an accident" [17]. This definition is advisable as in principle it can be compatible with several TAS domains. The problem with the usage of the word "hazards" has been highlighted in D4.5. This deliverable notes that "[during the [execution of the WP4] case studies, the ASCOS approach suffered 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." This made it difficult to apply the methodology and it pointed at the need for having a common definition of the term "hazard".

2.2.5 REC 1.05: Reconsider the definition of the different types of TAS domains (WP5-WP4)

It is recommended that ASCOS defines a standard taxonomy of the domains that can be involved in a change. Two reasons motivate this request. First, such a taxonomy is very important in assisting the authority and the applicant in deciding whether a change should be limited to a single domain, or, instead, should be considered in relation to many. Second, the current taxonomy available in Appendix B of D1.3 mentions six domains (see Table 3). However, as a first consideration, it can be noted that no rationale has been illustrated for proposing such types of domains. Furthermore, the taxonomy seems to be biased mostly towards the consideration of

ATM domains, as four domains (out of six) are ATC-related. In reconsidering the definition of the TAS domains it is advised to consider if and how they "connect" with the EASA certification domains, i.e. the domains covered by EASA regulations. These are listed in Figure 4.

Table 3. Types of TAS domains defined under Appendix B of D1.3.

- ATM/ANS;
- ANSP;
- Aircraft manufacture and certification;
- Aircraft operator;
- Aerodrome;
- Airspace planning.

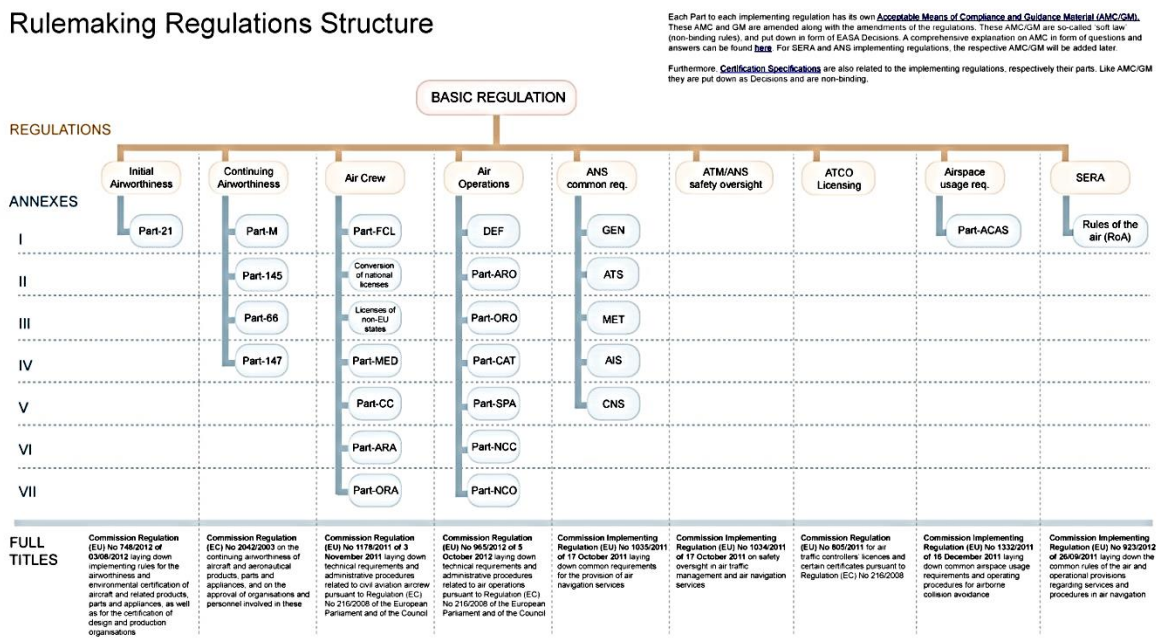

Figure 4. EASA Certification domains.

2.2.6 REC 1.06: Use consistently the expression "TAS domain" (WP4-WP5)

When providing the definition of "domain" and when referring to it, it is recommended to use the expression "TAS domain", and not just "domain", when reference is made to the kind of domains defined in ASCOS. This is to make sure that the term is interpreted consistently with the standard taxonomy of TAS domain of ASCOS (see also the previous recommendation).

2.2.7 REC 1.07: Complement the description of the proposed ASCOS certification approach with references to existing relevant Human Factors methods

It is recommended that the description of the ASCOS certification approach makes reference to existing human factors methods that can be used to identify, track, and manage human factors issues and requirements along the lifecycle of the change. Such methods include for instance the EUROCONTROL Human Factors Case [18] and the SESAR Human Performance Assessment Process [19]. In particular, Appendix A of the latter document contains a Human Performance argument intended to demonstrate that all the relevant human factors aspects are taken into account during a project. This argument could be considered for integration with the ASCOS safety argument: It could become, for instance, a human factors specific module that adds to the current modules of the ASCOS safety argument.

The need for further clarifying how the ASCOS certification approach addresses human factors issues emerged clearly during the first validation exercise. On the one hand, it was noted that the increased and sustained attention to human factors issues is important in certification, and this is indeed an important objective of the project [1]. On the other hand, it is was not clear to the experts how the ASCOS certification approach could actually increase the consideration of such issues.

2.2.8 REC 1.08: Complement the description of the proposed ASCOS certification approach with reference to organizational hazard assessment methods (WP5-WP4)

It is recommended to complement the description of the ASCOS approach with reference to organizational hazard assessment methods. The ASCOS approach may be applied to the assessment of organizational changes. A point in case is the introduction of a novel independent de-icing service provider. In cases such as this one the ASCOS certification approach requires support by (safety hazard) assessment methods that address specifically organizational hazards that may affect operational safety. Examples of organizational hazards include hampered coordination and communication across organizational boundaries, gaps and blind spots in safety decision making, hampered safety checks, decreased opportunities for safety learning [20]. Hazards such as these may inadvertently result from organizational changes such as changes of policies, roles and responsibilities. Also, these hazards are usually best addressed by methods such as MORT [21] and STAMP [20], i.e. by methods that do not focus on hazards and failure found in the sequence of events at system operation level, but on the organizational conditions and dynamics found at higher hierarchical levels. In summary, the user of the ASCOS approach needs to be aware that, depending on the change at hand, such kind of safety assessment methods may need to be used in alternative or in addition to classical safety hazards and human error assessment methods.

This recommendation is mirrored by recommendation 31 of D4.5 [11], which is copied in the figure below, and founds direct support from the WP4 case study that addressed the experience of applying the ASCOS certification approach to a novel de-icing service provider [22]. In that case it was observed that “the main complexities of certifying such a provider are of an organizational nature” [22], and that “[the D1.3 approach and the supporting safety tools appeared to deliver limited added value in that area”[22]. Essentially, these

considerations reinforce the urge for clarifying that ASCOS is not bound to specific safety assessment methods but can accommodates also assessment methods looking at organizational hazards and requirements.

WP4 Recommendation 31 (4.5): 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).

Figure 5. Recommendation 31 from WP4.5 (Source: [11]).

2.2.9 REC 1.09: EC or EASA to promote the sharing of safety risk information across the TAS stakeholders involved the use of the proposed ASCOS certification approach

In order to make the implementation of the ASCOS approach feasible, it is recommended to consider in future development how to foster the sharing of confidential safety risk information across the different TAS stakeholders. One main concern related to the introduction of ASCOS is the fact that the legal departments of the organizations involved in a change—especially manufacturers—may block the circulation of proprietary safety risk information, as this may damage the organization's reputation [4, pp. 46, 70]. Therefore, the successful introduction of ASCOS requires the availability of appropriate solutions that favour the sharing of safety risk information across the organizations involved in a change. It is expected that a combination of solutions may be used, such as:

- Creating a "protected legal environment", i.e. this equals to define confidentiality rules that limit the circulation of confidential safety risk information to the stakeholders involved in the change only. This could protect the unintended release of such information to the general public and the media;
- Making mandatory the sharing of safety risk information. Another solution, mentioned during ASCOS validation exercise 1 [4] by some experts, consists of introducing a legal requirement that mandates the sharing of safety risk information among the involved stakeholders, and that defines what are the penalties for the stakeholders unwilling to disclose such information;
- Promoting a "TAS sharing culture". Other solutions may target the attitudes and mind-sets of the stakeholders involved in certification. Promoting a TAS sharing culture implies engaging in initiatives that clarify the safety and efficiency benefits—both at system wide and individual organization level—that may ensure from the adoption of the ASCOS approach.

It is acknowledged that these initiatives fall outside the scope of ASCOS, and that they will not be addressed by the WP1.5. It is worth, however, to point them out as they will need to be considered by future efforts aimed at making the introduction of the ASCOS approach more feasible.

2.2.10 REC 1.10: Define guidance for establishing the team of experts that will have to manage the TAS change

It is recommended to define guidance that can be used in establishing the team of specialists (coming from different domains) that will be involved in the management of the change. As a minimum, it should be given consideration to the size of the team, and its composition. Composition may be considered, as a minimum, in terms of background (e.g. operational, engineering, and human factors), and represented stakeholders

perspective (e.g. air operators, ANSPs, etc.). In addressing this recommendation it is recommended to consider the handbook of the FAST methodology [23]. This document provides a good example of the kind of guidance needed for assembling a team of safety experts for TAS safety analysis purposes, and this focus makes it a good starting point for the definition of analogous guidance in the context of ASCOS.

2.2.11 REC 1.11: Define criteria for defining the actual organizations to be involved in the change

During the application of the ASCOS approach, after defining the change, it will be needed to define the specific organizations of one's own and of other domains that will be approached and that will be involved in the management of the change. This implies to define, for instance, which Air Operators, ANSPs, OEMs, and maintenance organizations will need to be actually involved. Note that identifying such organizations goes beyond identifying the type of the affected domain. This latter step is already covered by stage 1 of the ASCOS approach: definition of the change. This recommendation, instead, addresses the decision of which specific organizations (e.g. Alitalia, Air France, CAA UK) will have to be involved in the change. The ASCOS approach should provide guidance that directly support this decision.

2.2.12 REC 1.12: Define criteria for distinguishing changes that require the ASCOS approach from those that do not (WP5-WP4)

It is recommended to distinguish, as a minimum, between cases in which the certification can be made focusing on one domain (single-domain changes), from cases impacting on more domains (Multiple-domain changes). While the formers do not require the involvement of organizations from other domains in the management of the change, the latters, because of their size and impact, will do. So, while single-domain changes can be certified recurring to existing approaches in use in one particular domain without recurring to ASCOS approach, multiple-domain change will need it. It is important to distinguish between the two types of change, because ASCOS tends to be perceived as a resource-intensive process, and clarifying that it does not need to be necessarily applied to (relatively simple) changes may improve its acceptability.

2.2.13 REC 1.13: Map WP2 and WP3 products against the ASCOS Certification Process (WP5-WP4)

It is recommended to define when the ASCOS models and tools developed in the WP2 and WP3 can be used along the ASCOS certification approach. This implies mapping the use of the ASCOS SPI framework and the ATCSM (WP2 main outcomes), and the ASCOS Risk Assessment Model and Tool for risk assessment (WP3 main outcomes) against the stages of the ASCOS certification approach. The needs for clarifying this mapping emerged during validation exercises 2 and 3 [4] , where these ASCOS outcomes were perceived as relatively standalone items, potentially useful in the context of a safety management system—rather than as part of a larger certification process. Therefore, mapping the use of these ASCOS products to the stages of the ASCOS certification approach will be helpful in further showing their added value in the context of certification—and to promote a unitary view of the ASCOS products. This recommendation founds support in the D4.5: This deliverable has developed two recommendations that target the use, in the context of the ASCOS proposed certification approach, of (i) the ASCOS Tool for Continuous Safety Monitoring and o (ii) the ASCOS Risk tool for risk assessment. The recommendations in question are reported in the following figures.

WP4 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).

Figure 6. Recommendation 22 from WP4.5 (Source: [11]).

WP4 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. 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.

Figure 7. Recommendation 24 from WP 4.5 (Source: [11]).

2.3 WP4 RECOMMENDATIONS

This section reports the full set of recommendations developed by the WP4 for the proposed ASCOS certification approach. The development of these recommendations was based on the experience gained in the context of the same WP during the execution of the four certification case studies.

WP4 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.
WP4 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.
WP4 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.
WP4 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;
WP4 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.).
WP4 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.
WP4 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.

WP4 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.

WP4 Recommendation 09: It is recommended to the EC to define which authority is responsible for safety across the TAS.

WP4 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.

WP4 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.

WP4 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.

WP4 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.
WP4 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).
WP4 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.
WP4 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.
WP4 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.
WP4 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 SPI framework for continuous safety monitoring (WP2 outcome)

3.1 SUMMARY OF WP5 VALIDATION RESULTS

This section reports a summary of the main validation results that were documented in D5.3 and that addressed at the proposed ASCOS SPI framework for continuous safety monitoring.

3.1.1 KPA 1: Soundness

Three main results have emerged in relation to the area of soundness. First, it was evident, from Exercise 2, the need for further defining how the ASCOS SPI framework can be adapted/modified/extended for the purposes of safety monitoring related to a specific certification case. The framework tends to be perceived as a standard set of SPIs, and may however fail to acknowledge the specific SPIs associated to a given change. In other words, each change may have each on set of change-specific SPIs, and to the experts participating in Exercise 2 it was not clear how this should be accounted in the ASCOS SPI framework. Second, the ICAO view of safety monitoring, as described in the ICAO Safety Management Manual [17], includes also non-quantitative data sources. Therefore, it should be made explicit that ASCOS continuous safety monitoring concept focuses solely on quantifiable safety performance indicators based on reported occurrences. Else safety (and certification) experts would wonder why one should not consider non-quantifiable and non-reportable events in the context of safety monitoring. Third, the SPI framework appeared to the experts' taking part in Exercise 2 to be oriented mainly towards the consideration of indicators of negative safety performance. It was commented, however, that the framework could be improving by adding indicators that represent safety enhancing activities—i.e. indicators of positive safety performance.

3.1.2 KPA 2: Completeness

The ASCOS SPI framework aims to cover the whole TAS. For this reason, the experts participating in ASCOS Validation Exercise 2 stressed that the SPI framework should include other domains than only aviation and air traffic control. Other possible domains that could be included in the framework include ground handling, maintenance, and airport operations. This remark was partly mitigated by the observation that the development of the ASCOS SPI framework was scoped around the EASA key operational issues (as defined in the European Aviation Safety Plan [24]), so its scope was somehow set by this initial requirement.

3.1.3 KPA 3: Standardization

Regarding the potential of the framework to become a standard SPI framework, it emerged that safety practitioners would normally consider as a standard SPI framework the one developed by EASA. Any additional framework to this latter, risks to be perceived as a duplication. Therefore, it should be further clarified how the ASCOS SPI framework relates to the EASA SPI framework. In this context, it should be noted that EASA experts participating in the Network of Analysts (NoA) sub-group for SPIs have in fact reviewed the framework for Safety Performance Indicators proposed by ASCOS (comments have been processed satisfactorily by ASCOS).

3.2 WP5 RECOMMENDATIONS

This section reports the full set of recommendations related to the proposed ASCOS SPI framework for continuous safety monitoring. These recommendations have been developed based on the results of the second WP5 ASCOS validation exercise [4].

3.2.1 REC 2.01 Consider changing the name from "SPI framework for safety monitoring" into "SPI framework for continuous safety occurrence monitoring"

It is recommended to modify the name of the ASCOS SPI framework in order to make it clear that the framework applies specifically to the monitoring of quantifiable safety occurrences. This will make it clear that the tool deals exclusively with the quantifiable safety data that can be collected in the context of an SMS, and that other non-quantifiable safety data can still be collected by means of methods external to the framework. Clarifying the specific focus of the SPI framework is important because the continuous monitoring part of a SMS is not limited to the reporting of quantifiable occurrences only, but includes also other qualitative safety data, such as operators' narrative reports, incident reports etc.

3.2.2 REC 2.02: Provide guidance to adapt the SPI framework to the local context of the change

It is recommended that further guidance is provided about how to adapt the SPI framework to the local context of the applicant or authority organizations. These organizations usually have their own internal set of SPIs, as part of their SMS. Therefore, further guidance needs to be provided on how to adapt the ASCOS SPI framework, else the framework tends to be perceived as a standard framework intended to replace, and not complement/harmonize, local ones.

3.2.3 REC 2.03: Consider the possibility to include positive safety indicators in the SPI framework

It is recommended that the ASCOS SPI framework is enhanced with indicators of positive safety performance. This would make the development of the framework more consistent with recent safety developments, in particular more consistent with the Safety-II view of safety of EUROCONTROL[25]. This view suggests that the monitoring of also positive safety performances provides a larger focus for monitoring overall safety performance and for devising safety improvements compared to the monitoring of negative performance alone.

3.3 WP4 RECOMMENDATIONS

No WP4 recommendations have been reported under this section since the evaluation of the ASCOS SPI framework was outside the scope of D4.5 [11].

4 ASCOS Tool for Continuous Safety Monitoring (WP2 outcome)

4.1 SUMMARY OF WP5 VALIDATION RESULTS

This section reports a summary of the main validation results that were documented in D5.3 and that addressed at the proposed ASCOS Tool for Continuous Safety Monitoring (ATCSM). To note that ASCOS exercise 2, the exercise in which the ATCSM was evaluated, enjoyed a lower participation compared to the exercises 1 and 3, and for this reason results about the ASCOS Tool for continuous safety monitoring are available for one KPA only. However, note that this ASCOS Tool was directly introduced by the EC JRC to key aviation stakeholders (including EU CAA's, Safety Investigation Authorities, EASA, EC DG-MOVE, ICAO, EUROCONTROL, ...) at the ECCAIRS Steering Committee in October 2014. The Tool is now directly available for these organisations through the ECCAIRS Portal, which is managed by the JRC of the EC. The experience of these organisations with the ASCOS Tool (in the context of ECCAIRS) is not addressed in the present document.

4.1.1 KPA 4: Usefulness

The ASCOS Tool for Continuous Safety Monitoring was viewed by the experts participating in ASCOS validation exercise 2 as a valuable enhancement of the ECCAIRS database. The tool provides a useful graphic depiction of selected SPIs trends which can then be used for safety analyses. For instance, prior to the release of the type-certificate, the authority can use the tool for safety assessment of designs comparable to the one that has to be type-certified. In the same certification phase, the applicant can use the tool to collect the evidence that will be part of its own safety case.

One aspect limiting the perceived usefulness of the ATCSM is the fact that the tool is intended as an enhancement of the ECCAIRS system. Thus, organizations that are not using ECCAIRS will have to code their occurrences according to ECCAIRS and they have to use a similar physical data structure as ECCAIRS 5 in order to be able to use the tool. In acknowledging this potential limitation raised by the experts, it should be reminded that ECCAIRS compatibility is not optional but mandatory according to EC regulation 376/2014 [26] (see art. 7, paragraph 4). ASCOS is consistent, indeed, with this regulation. Therefore, this limitation, as formulated, may no longer be present once industry has managed to comply with the regulation in question.

4.2 WP5 RECOMMENDATIONS

This section reports the full set of recommendations related to the proposed ASCOS Tool for Continuous Safety Monitoring (ATCSM). These recommendations have been developed based on the results of the second WP5 ASCOS validation exercise [4].

4.2.1 2.04: Consider changing the name of ASCOS tool from "Tool for continuous safety monitoring" to "Tool for continuous safety occurrence monitoring"

Also regarding the "ASCOS tool for continuous safety monitoring" it is recommended to change its name into "ASCOS tool for continuous safety occurrence monitoring". Analogously to what already said for the ASCOS SPIs framework (See § 3.2.1), adding the term "occurrence" to the tool's name is important to avoid

generating the false expectation that the tool allows the monitoring of all the data that can be collected in the context of a SMS continuous monitoring context. The tool processes, in fact, quantitative safety occurrences only and this should be better reflected on its name.

4.3 WP4 RECOMMENDATIONS

This section reports the full set of recommendations developed by the WP4 for the proposed ASCOS tool for continuous safety monitoring [11]. The development of these recommendations was based on the experience gained during the execution of the four certification case studies.

WP4 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.

WP4 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).

5 ASCOS Risk Model (WP3 outcome)

5.1 SUMMARY OF WP5 VALIDATION EXERCISE RESULTS

This section reports a summary of the main validation results that were documented in D5.3 and that addressed at the proposed ASCOS Risk Model.

5.1.1 KPA1: Soundness

Regarding soundness, it was noted that the ASCOS Risk Model appears too generic if compared against local risk models developed and maintained at local level by individual organizations. In other words, since it is likely that more specific risk models will be available at local level, for organizations it is not clear the added benefits of replacing these models with the ASCOS Risk Model. On the other hand, the ASCOS Risk Model – on purpose designed at generic level to enable TAS-level risk assessment — is a model to support stakeholders in assessing how the risks associated with a specific change may propagate on other domains. This risk assessment level is not covered by current in-house risk models. It should be defined how to connect such models with the generic ASCOS risk model. Such a connection could be obtained by establishing proper hooks between the top event of (local) detailed FT to the relevant ESD or high level FT structure of the ASCOS risk model.

Furthermore, it should be further clarified how the ASCOS risk model can be used and by whom in a TAS risk assessment. This implies further defining the formal structure of roles and responsibilities that will engage with the development and maintenance of the risk model.

Finally, two limitations were noted regarding the ASCOS Risk Model. First, the model, because of its name, creates the expectation that it will serve as support for the identification of novel and unknown risks. In fact this is not the case: The risk model leaves this capability to other safety methods external to the model. In particular, in ASCOS this capability comes from the FAST methodology; therefore, it should be further clarified how FAST can be used to inform and maintain the Risk Model. The second limitations concerns the fact that the risk model should have the capability to assess severity levels and consider different probability units. These capabilities were not available on the version of the ASCOS Risk Model evaluated during the WP5.3, but yet they were expected by the experts that took part into ASCOS validation exercise 3.

5.1.2 KPA 2: Completeness

At least three views of completeness have emerged during the evaluation exercises, and all three deserve consideration as they provide insights for further increasing the validity of the risk model. These three views are listed below:

- *Domain completeness*. Domain completeness concerns the number of domains that are covered by the risk model. Here, it was noted that the ASCOS Risk Model seems to be biased towards the coverage of aircraft operations mainly. However, because the model aims at the TAS, ATM operations, at least, should have the same level of coverage.
- *Data completeness*. Data completeness concerns the type of data that has been used to inform the model. Notably, safety data informing a risk model can be historic, diagnostic, or prognostic [23, p. 3]. The ASCOS

Risk Model is based on one type of data—historic data. It was observed that limiting the model to historic data, although on the one hand it allows quantification, on the other makes the model incomplete with regard to the full range of risks that may occur. In fact, the model does not necessarily cover (dangerous) events that could occur, but which have not occurred yet. Moreover, the model would not necessarily keep up with system evolution. This is the case because it would covers only events related to the systems and environments that were in place at the time and place the accidents occurred. But this does not fully reflect the range of situations in which novel systems in modern environments may fail. This expert concerns, points at the importance of defining guidance for ensuring that the risk model is regularly updated, both in the quantification of events and the scenarios themselves, to account for recent evolutions and development.

- *Geographical completeness*. Geographical completeness concerns the variety of geographical areas the data informing the model comes from. To date the risk model is mostly informed by incident and accident data occurred in Europe. This was viewed as a limitation of the model because it does not account for risks that may occur in other parts of the world, especially third world countries, where working practices (and sources of hazards) are very different compared to Europe. The validity of the Risk Model could be enhanced by feeding it with worldwide safety data, so to make it more representative of the TAS worldwide.

5.1.3 KPA 3: Standardization

The model may become a standard model provided it is clear how it connects to existing Safety Management Systems and State Safety Programmes. These will have to be implemented by operators and authorities respectively; therefore, the integration of a novel risk model under SMSs and State Safety Programmes (SSM) will make the widespread adoption of the model it more likely.

The use of the term “emerging risks” associated to the ASCOS Risk Model was criticized for its potential ambiguity and limited compatibility with existing safety management standards. In particular ASCOS D3.1 defines an emerging risk as a “familiar risk that is increasing or new risk that become apparent in new or unfamiliar conditions” [9]. This definition appeared not immediately clear to the experts, who view emerging risks as new and unknown risks. This latter interpretation of the term seems consistent with the usage of the term “emerging” in ICAO Doc 9859 Safety Management Manual [17], which uses the term as opposed to known risks. In general, any definition of risk introduced by ASCOS should be compatible, whenever possible, with existing standard definitions.

5.1.4 KPA 4: Acceptability

Acceptability refers to extent to which the ASCOS Risk Model looks acceptable to its end users—competent authorities and applicant organizations. Regarding this KPA, it was noted that more information about the staff, expertise, and technological infrastructure needed to use the risk model within an organization would be needed to collect feedback on the acceptability of the model.

5.2 WP5 RECOMMENDATIONS

This section reports the full set of recommendations related to the proposed ASCOS Risk Model. These recommendations have been developed based on the results of the third WP5 ASCOS validation exercise [4].

5.2.1 REC 3.01: Further clarify the TAS level purpose of the ASCOS risk model

It is recommended to further clarify that the ASCOS risk model is intended for TAS level risk assessment. Service providers and manufacturers would be reluctant to adopt a risk model intended to replace their own, in house and more detailed risk models. On the other hand they see the added value of having a risk model specifically designed for TAS-level risk assessment model—i.e. a model to support stakeholders in assessing how the risks associated with a specific change may influence other domains. The use of this model would add, and not replace, their own in house risk model.

5.2.2 REC 3.02: Define the connection between the ASCOS risk model and local, in-house risk models

It is recommended to define how the (TAS level) ASCOS risk model can be connected with local, in house models owned by service providers and manufacturers. Clarifying such a connection is important to further define how the model can be used for the purpose of TAS-level risk assessment. Also, such a connection can be obtained by establishing proper hooks between the top event of (local) detailed FTs to the relevant ESD or high level FT structure of the ASCOS risk model.

5.2.3 REC 3.03: Ensure that the model covers all of the relevant TAS domains in a consistent manner

It is recommended that the ASCOS risk model will cover in a consistent manner all the different domains that are part of the TAS. This recommendation originates from the recognition that the model covers air operations in greater detail compared to ATC. In order to be more TAS covering, the model should be able to address in a consistent manner all of the relevant domains that are part of the TAS.

5.2.4 REC 3.04: Define guidance that regulate the regular update of the Risk Model

It is recommended that guidance is developed for ensuring that the ASCOS risk model is regularly updated, both in quantification of events and the scenarios themselves to account for recent system evolutions and developments. This recommendation arises from the recognition that the model is based mostly on historical data, and therefore, if not maintained and updated periodically, it cannot cover all dangerous events that could possibly occur.

5.2.5 REC 3.05: Further define the structure of roles and responsibilities that will engage with the development and maintenance of the risk model

It is recommended to further define the context of use of the ASCOS Risk Model: who is the user of the model, and especially which roles will be responsible for managing and updating the model. In addressing this question it is advised to consider section 7 of ASCOS deliverable D3.5a: This sections describes an initial organizational structure of organizational roles—at TAS-level and stakeholder-level—that have to interact and

coordinate their effort in order to establish and improve a safety standards. The same structure of role may be, in principle, effective in managing the risk model.

5.2.6 REC 3.06: Include severity values in the risk model

It is recommended to enhance the risk model with severity levels. In this way the model will be a true risk calculator. ICAO Safety Management Manual defines risks as "the estimated likelihood and severity of the consequences or outcome from an existing hazard or situation" [13] . The version of the model evaluated during ASCOS validation exercise 3 was seen more as a probability—rather than risk—calculator because it did not accounted for severity levels.

5.2.7 REC 3.07: Enhance the model with the capability to control different probability units

It is recommended that the ASCOS Risk model embeds the capability to handle different probability units. Probability units used in safety risk assessment may vary depending on the type of system, component, sub-component for which risk of failure is assessed. For instance, probability units may be expressed as occurrence x flight, x hour of flight, x hour of use. Therefore, the ASCOS risk model should be able to account for variations in these units in order to account for the different types of risk that may arise in the TAS system. The need for handling different probability units was highlighted during discussion groups with experts focused on the ASCOS Risk tool (see section 6.1.2: KPA 6: Quantification). However, such capability needs to be addressed by the risk model prior to be implemented in the tool.

5.3 WP4 Recommendations

This section reports the full set of recommendations developed by the WP4 for the proposed ASCOS Risk Model. The development of these recommendations was based on the experience gained in the context of the same WP during the execution of the four certification case studies. Only two recommendations have been reported because the WP4 evaluation focused more on the evaluation of the ASCOS Tool for risk assessment, rather than the underlying risk model.

WP4 Recommendation 21: It is recommended to ASCOS that domain(s) and stakeholder(s) are allocated to the risk model elements.
WP4 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, which 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.

6 ASCOS Risk assessment tool (WP3 outcome)

6.1 SUMMARY OF WP5 VALIDATION RESULTS

This section reports a summary of the main validation results that were documented in D5.3 and that addressed at the proposed ASCOS Risk assessment tool.

6.1.1 KPA5: Manipulability

The ASCOS tool for risk assessment was perceived as a useful support tool to interact with/modify the elements—i.e. the ESDs and the FTs—of the risk model. However, the tool was perceived to play mainly the role of an editor of the ASCOS Risk Model, rather than a proper risk assessment tool. This was due to the fact that the tool lacks a severity assessment output/functionality and that risk identification is done with safety methods external to the tool (and the risk model). The actual function of the tool should be better reflected on the tool's name to avoid generating unrealistic expectations on the potential users.

6.1.2 KPA 6: Quantification capability

In order to be seen as a true risk assessment tool, the ASCOS tool for risk assessment should handle both (i) severity levels (as already mentioned) and different probability units. Regarding this latter point, it was noted that different probability units (e.g. occurrence x flight, x hour of flight) may be used in the context of safety risk assessment, and they should be, therefore, properly handled by the risk tool (and the underlying risk model). Another important aspect that affects the usefulness of the figures generated by the tool is the availability of confidence data/indicators. These need to be further defined so to increase the meaningfulness of the probability estimates generated by the model/tool.

6.1.3 KPA 7: Cross-domain integration

Cross domain integration regards the potential of a proposed solution to promote the cooperation, and the sharing of information across the stakeholders involved in the management of a change. Regarding this KPI, on the positive side it was noted that the wide-spread adoption of the ASCOS risk assessment tool (and the underlying model) may help promoting the development of a standard "risk language" across the various TAS domains. This can be functional to bridge the boundaries existing between different domains, which usually are characterized by very different and specialist risk languages. At the same time, the wide-spread use of the tool (and the model) requires a regulatory requirement to promote/make it obligatory for TAS stakeholders the sharing of risk related information, so that quantitative risk assessment can be integrated. This should not be taken for granted as risk data is highly confidential and TAS stakeholders would not normally share it among each other's (see also § 2.1.3 and § 2.2.9).

6.1.4 KPA8: Standardization

The potential for standardization of the ASCOS risk model depends also on its capability to be hosted by different software than the ASCOS tool for risk assessment only. Therefore, a comparative benchmark with

other comparable FT editors would be desirable to understand the true potential of the tool in term of standardization and compatibility.

6.1.5 KPA 9: Acceptability

Regarding the acceptability of the ASCOS tool for risk assessment, the same considerations expressed for the acceptability of the risk model apply. It was noted that more information about the staff, expertise, and technological infrastructure needed to use the tool within an organization would be needed to collect feedback on the acceptability of the model. The definition of these aspect will enhance the possibility to collect more detailed feedback about the acceptability of the ASCOS tool for risk assessment.

6.1.6 KPA 10: Usability

The overall SUS score[1] for the ASCOS tool for risk assessment was 57, meaning that the tool usability level falls in the marginal acceptance range (50–70), i.e. some improvements are needed. The analysis of the experts' rationale besides this rating collected during ASCOS validation exercise 3 have allowed to diagnose the following areas of improvements:

- Providing suggestions for identifying which ESDs/FTs could be affected by a change;
- Providing further support for the graphical exploration of the model elements; Displaying hover boxes next to the selected model's element with information about the element;
- Supporting compatibility with other FT software packages (available on the market);
- Enhancing the user manual input of probability values;
- Integrating an audit trail capability.

These areas will be described, in the form of recommendations for improvement, in the next section.

6.2 WP5 Recommendations

This section reports the full set of recommendations related to the proposed ASCOS tool for risk assessment. These recommendations have been developed based on the results of the third WP5 ASCOS validation exercise [4].

6.2.1 REC 3.08: Consider to change the name of the "ASCOS Risk Assessment Tool" into "ASCOS Risk Model Editor"

It is recommended to change the name of the ASCOS Risk assessment tool into ASCOS Risk Model Editor. The current name tend to create the false expectation that the tool can actually be used to identify what are the hazards associated with a specific change. In fact this is something that is done using safety assessment methods external to the tool. The main function of this latter remains that of allowing a user to access, add,

[1] The System Usability Scale (SUS) [27] yields a single score representing a composite measure of the overall usability of the system under evaluation. SUS score can be interpreted based on the following: <50= not acceptable; 50-70= acceptance is marginal, some improvements are needed; >70: acceptable.

remove and modify the ESDs and FTs of the ASCOS risk model element and then calculate the overall changes in probability.

6.2.2 REC 3.09: Provide suggestions for identifying which ESDs/FTs could be affected by a change.

Currently, the use of the tool demands the user, a safety analyst, to be thoroughly familiar with the risk model—knowledge regarding the general structure of the model and the contribution of specific elements has to be "in the head" of the safety analyst to efficiently identify relevant parts of the model. Therefore, it is recommended to have a tool functionality that, depending on the change at hand, suggests which FTs of other ESDs could be affected. The tool should not change automatically the related FTs in other ESDs that should be considered. Rather it should only highlight related parts of the model. This functionality would be particularly helpful in cross-domain risk assessment: While an analyst is usually expert of her/his own domain, and might have sufficient knowledge about the related risk-model structure, she/he may be less familiar with the FTs of other domains, and therefore it could be useful if the tool highlights hazards (or FTs) to consider.

It is important to note that the functionality mandated by this recommendation, prior to be implemented in the tool, requires adequate support by the underlying ASCOS risk model (see rec 3.02).

6.2.3 REC 3.10: Provide further support for the graphical exploration of the model

It is recommended to investigate ways in which of the exploration of the ASCOS Risk model can be eased. In addressing this recommendation, it can be noted that the exploration of the risk model occurs at least two different levels, each of which can be addressed by dedicated improvements as follow:

- Within-ESD/FT exploration. This exploration concerns exploration of the elements found within individual ESD or FT diagrams. As a minimum, it can be enhanced by enlarging the size of the boxes within which these diagrams are displayed. While minimizing, or even removing, the need for using scroll bars, this solution would provide a more immediate at-a-glance view of the single ESD or FT diagram. If the size of a single box would not suffice to accommodate a whole FT or ESD, exploration could still be facilitated by implementing a "click-and-drag" interaction style;
- Cross-ESD/FT diagrams. This exploration concerns the exploration across different ESD/FT diagrams. As a minimum, it can be enhanced by reducing the number of interaction steps needed to move from one ESD element to the corresponding fault trees (currently, the access is not direct, but there is an intermediate page).

Also, there should be a function to facilitate the exploration/identification of the relevant model elements that should not be limited to the name of ESD and FT events only, but should also include the definitions of model elements.

6.2.4 REC 3.11: Display, in the FT and ESD views, model elements descriptions as hover boxes

It is recommended that the ASCOS Risk tool displays model element descriptions as hover boxes whenever the user hovers over any of the elements with the mouse pointer. A hover box is a box displayed when the mouse moves hover a pre-set trigger area. It can provide the user with useful background information and details about the about model element(s) of interest, while keeping an overview of the model structure.

6.2.5 REC 3.12: Support compatibility with other FT software.

File format compatibility with other FTs software is important to consider. The tool should be able to export the results of an analysis to other FT software programs. At the moment, the tool can export data to MS Excel, so compatibility depends on the ability of other FT software programs to read Excel files.

6.2.6 REC 3.13: Enhance user input of probability values.

The input of updated probability values could be enhanced in order to make it easier for the user while reducing the risk of data entry mistakes. When manually entering a new probability value, a simple typo, in fact, could result in a very significant—and mistaken—variation in the order of magnitude of the value. Such data input mistakes could be avoided by enhancing the tool's HMI with a safe guard that constraints the range of user inputs that are accepted by the tool. Having such a protection was considered quite important by the experts involved in exercise 3 to prevent erroneous entries of unrealistic probability values. In addition to that, it was suggested to further ease the data input method. In particular, the tool HMI (i) could suggest upper and lower threshold probability values, (ii) could provide pre-set modification factors of these values (e.g. 0.5, 1.5, 2, 2.5), (iii) could offer direct support for the calculation of an updated probability value depending on the chosen modification factor (currently, the user has to recur to calculators external to the tool, either paper or computer based).

6.2.7 REC 3.14: Further develop the audit trail capability of the tool.

It is recommended that the tool provides further support for an "audit trail" capability, i.e. the capability to maintain a detailed chronological record of the changes made to probability values of the risk model. Such record should contain and make available to the user information such as date of the change, person responsible for making the change, detailed description of the change, reason(s) for the change, evidence and underlying assumptions. This capability was considered important by experts because it provides an important means for safety practitioners to establish the confidence of the risk assessment outcomes produced by the tool. To note that the tool does already offer a functionality to keep track of changes; therefore, this could be further evolved to further cover the need for a detailed record of changes to the risk model.

6.3 WP4 RECOMMENDATIONS

This section reports the full set of recommendations developed by the WP4 for the proposed ASCOS Risk assessment tool. The development of these recommendations was based on the experience gained in the context of the same WP during the execution of the four certification case studies.

WP4 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.

WP4 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.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.

7 FAST Areas of Change

7.1 WP5 Recommendations

No WP5 result and recommendations have been developed for this ASCOS product because its evaluation fell out of the scope of the WP5 validation exercises.

7.2 WP4 RECOMMENDATIONS

The following section reports the four recommendations that have been developed in D4.5 in relation to the Areas of Change (AoC) envisaged by the FAST methodology [23], [28].

WP4 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.
WP4 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.
WP4 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.
WP4 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).

8 Conclusion

The present deliverable had two main objectives:

1. To develop the full set of WP5 recommendations, i.e. the recommendations developed in the context of WP5 and based on the results of the three validation exercises carried out in WP5.3. These recommendations represented the main contribution of this deliverable.
2. To present, in an integrated manner, the full set of recommendations developed by the WP5 and WP4. This latter work package identified the benefits and lessons learnt, as well as the recommendations for improvement, based on the application of the ASCOS certification approach to four case studies about innovative changes to the total aviation system (TAS). The four cases, in particular, explored the value of the ASCOS approach in the initial phases of certification.

The integrated presentation of the complete set of WP4 and WP5 recommendations was intended to provide an easy access to all the proposals for improvements both internally and externally to ASCOS. Internally to ASCOS, the recommendations are addressed to WP1.5 (Consolidation of new certification approach). While externally to ASCOS they are intended for future research and development activities in the same area.

Altogether, the main recommendations presented in this document can be clustered around six blocks, which have been listed below in order of priority:

1. Recommendations requiring to **further define the context of usage** of the proposed ASCOS products. These kind of recommendation s have been highlighted for both the ASCOS proposed certification approach and the ASCOS Risk Model. These recommendations essentially demand a better definition of the roles and areas of responsibilities of the stakeholders involved in the use of these products. Addressing these recommendations, especially those directed to the ASCOS certification approach, is important to further illustrate to potential users how the approach promotes the integration of the efforts of different stakeholders—i.e. how the approach delivers its main benefit of TAS certification.

2. Recommendations requiring to address some of the **inner logics involved in the development of the ASCOS TAS safety argument**. These recommendations address low level issues such as the management of the interfaces of the argument, the definition of an acceptable level or target level of safety across the TAS, the balancing of safety effects across domains. These recommendations have emerged essentially from the WP4. This is not surprising as the project partners involved in this WP actually had the opportunity to engage directly with the implementation of the ASCOS approach, and consequently to familiarize with many of the low level hindrances that may arise during the use of the approach. On the other hand, such level of familiarization with the working details of the approach was not available for the experts involved in the WP5 validation exercises. These recommendations are important to address, as they improve the integrity and feasibility of the TAS safety argument.

3. Recommendations about the **integration of the ASCOS approach with specific methodologies**. These recommendations include, in particular, human factors related methods (e.g. SESAR Human Performance Case) and organizational assessment methods.

4. Recommendations targeting the **definition of basic terms used in the context of ASCOS**. These recommendations are motivated by the intent to minimize inconsistencies across terms, and also minimize the introduction of novel terms that are unfamiliar for the users of the proposed ASCOS solutions. Examples of these recommendations include *REC1.03 Adopt a consistent definition of "risk"*, *REC1.04 Adopt a consistent definition of "hazard"*, and *REC1.06 Use consistently the expression "TAS domain"*. These recommendations are supposed to increase the clarity of the ASCOS products for novel users.

5. Recommendations about the **presentation of the ASCOS products**. These recommendations pertain to the way in which the ASCOS products are presented to the end-users: Some products, or their features, may generate erroneous expectations on the user side, depending on how they are presented. Example of these recommendations include *REC 2.01 Consider changing the name from "SPI framework for safety monitoring" into "SPI framework for continuous safety occurrence monitoring,* and *REC 3.05 Consider to change the name of the "ASCOS Risk assessment tool" into "ASCOS Risk model editor".*

6. Recommendations aimed at **software usability improvement**. These recommendations target essentially the ASCOS Risk assessment tool and aim at improving its usability.

Altogether, these recommendations will serve the purpose of informing future improvements of the evaluated ASCOS products. In particular, ASCOS WP1.5 will consider the recommendations presented in this deliverable in relation to the proposed ASCOS certification approach, in order to deliver a more refined and advanced version of it, compared to the initial outline documented in deliverable D1.3. The other products—the SPIs framework, the ASCOS Tool for continuous safety monitoring, the ASCOS Risk Model and the ASCOS Tool for risk assessment—will not be specifically addressed by WP1.5, or in the context of ASCOS. These recommendations, however, will be a useful basis for future research and development activities addressing the same kind of products.

References

[1] ASCOS, “Description of Work.” Jul-2012.
[2] R. Wever, L. Save, S. Rozzi, and T. Longhurst, “D5.1: Validation Strategy,” ASCOS deliverable D5.1, 1.2, 2014.
[3] Rozzi, S., Save, L., S. Pozzi, M. Torelli, R. Wever, and H. Udluft, “D5.2: Validation Plan and Scenarios, version 1.1,” D5.2 (Report prepared for ASCOS: Aviation Safety and Certification of New Operations and Systems, 7th Framework Programme, Grant agreement n. 314299), November 20014.
[4] S. Rozzi, L. Save, M. Torelli, R. Wever, B. van Doorn, H. Udluft, Menzel, R., W. Post, and N. Aghdassi, “D5.3: Validation exercises execution v1.0,” ASCOS Technical report D5.3, Apr. 2015.
[5] EUROCONTROL, “E-OCVM, Version 3.0, Volume I,” Feb. 2010.
[6] A. Simpson, S. Bull, and T. Longhurst, “D1.3: Outline Proposed Certification Approach,” ASCOS deliverable D1.3, version 1.2, Dec. 2013.
[7] A. L. C. Roelen, J. Verstraeten, Save, L., and N. Aghdassi, “D2.1: Framework Safety Performance Indicators v1.5,” ASCOS Technical report D2.1, Jan. 2014.
[8] R. Menzel and W. Post, “D2.4: Tools for continuous safety monitoring,” ASCOS deliverable D2.4, v. 01, 7/24/2014, 2014.
[9] V. Bonvino, J.-F. Delaigue, and Heckman, J-P., “D3.2.3: Total Aviation System Safety Assessment Methodology. Representation of future risks models,” ASCOS Deliverable D3.2.3, version 1.1, 2013.
[10] H. Udluft, P. C. Roling, and R. Curran, “D3.3: Tool for risk assessment: User Manual,” ASCOS Deliverable D3.3, 2014.
[11] Roelen, A., R. Wever, Rozzi, S., and S. Bull, “D4.5: Evaluation of certification case studies,” ASCOS deliverable D4.5, Dec. 2015.
[12] A. Iwaniuk, Michalak, P., van Es, G, B. Dziugiel, W. Miksa, Mączka, M., N. Aghdassi, Menzel, R., and Save, L., “D2.3: Process for Safety Performance Monitoring,” Technical report ASCOS deliverable D2.3 vo.1, Mar. 2014.
[13] Heckmann, J. P., S. B. Munoz, Delaigue, J., B. Dziugiel, B., T. Longhurst, and Pauly,B., “D3.5a: Total Aviation System Safety Standards Improvements v1.3,” ASCOS Technical report D3.5a.
[14] S. Bravo Muñoz, J. P. Heckmann, J. P. Magny, A. L. C. Roelen, L. Speijker, H. Udluft, M. Sanchez Cidoncha, and B. Dxiugiel, “WP3 Final Report Safety Risk Management, v1.2,” ASCOS Technical report D3.6, Aug. 2014.
[15] M. Sánchez and L. Save, “Overall Safety Impact Results and User Manual, v1.1,” ASCOS Technical report D3.4, Oct. 2014.
[16] S. Rozzi and Save, L., “Minutes of Meeting, WP4-WP5 Coordination Meeting, 28th April 2015, Deep Blue, Rome, Italy.” 28-Apr-2015.
[17] ICAO, “Doc 9859 Safety Management Manual (SMM) 3rd Ed.” International Civil Aviation Organization, 2013.
[18] Mellet, U. and Nendick, N., “The Human Factors Case: Guidance for Human Factors Integration,” EUROCONTROL, Jun. 2007.
[19] C. Chalon, “SESAR Sesar HP assessment process 2,” D26, 2013.
[20] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, Mass: The MIT Press, 2012.
[21] N. Knox and Eicher, R., “MORT User’s Manual.” US Departement of Energy, Feb-1992.
[22] J. . J. Scholte, S. Bull, G. Temme, M. Bravo, A. D. Balk, and N. Aghdassi, “D4.3: Case study for the testing of a novel certification approach.”
[23] FAST, “The FAST Approach to Discovering Aviation Futures and Associated Hazards--Methodology Handbook.” No date.
[24] EASA, “European Aviation Safety Plan 2014-2017,” European Aviation Safety Agency.
[25] EUROCONTROL, “From Safety-I to Safety-II: A White Paper,” Brussels, White Paper, 2013.
[26] EASA, “Regulation (EU) N. 376/2014.” 2014.
[27] J. Brooke, “SUS-A quick and dirty usability scale,” *Usability Eval. Ind.*, vol. 189, no. 194, pp. 4–7, 1996.

[28] “FAST Overview.” [Online]. Available: http://www.nlr-atsi.nl/fast/overview/index.html. [Accessed: 04-Mar-2015].
[29] “ASCOS Website,” 2014. [Online]. Available: www.ascos-project.eu.
[30] B. Pauly, T. Longhurst, A. Iwaniuk, M. Idzikowski, and B. Dziugiel, “D1.1: Analysis of existing regulations and certification processes v1.3,” ASCOS Technical report D1.1, Aug. 2013.
[31] FAA, “CPS Commercial Airplane Certification Process Study. An evaluation of selected aircraft certification, operations, and maintenance processes.” 2002.

Appendix A ASCOS Performance frameworks and Key Performance Areas

The present appendix reports the content of section 3.4 of D5.3 [4]*, which describes the development of the ASCOS performance framework and the corresponding KPAs.*

The validation of a novel product or concept is rarely a matter of evaluating the performance of a system along a single dimension, i.e. based on a single evaluative standard or point of view. Rather, the evaluation of the fitness-for-purpose needs to consider the multiple values, perspectives and viewpoints of the stakeholders that will be affected by the introduction of the novel system. This consideration is particularly relevant to the evaluation of complex products, systems, and concepts such as those proposed by ASCOS. The variety of actors involved in the certification domain, either in the certifier or applicant role, calls for the consideration of multiple view points during the validation process. These include supranational and national civil aviation authorities, manufacturers, airports, air navigation service providers, standard development bodies, etc.

For this purpose, three ASCOS specific performance evaluation frameworks, one for each Exercise, have been designed that captures the key areas of performance (KPA) in which the proposed solutions are expected to deliver their potential. An initial definition of the evaluation frameworks has been provided by the deliverable D5.1 [2, p. 1]. The definition of those frameworks was based on a review of the following sources:

- ASCOS dissemination material (brochures and website [29]);
- ASCOS deliverable D1.1 [30]. This deliverable consists of an analysis of existing regulations and certification processes aimed at identifying potential shortcoming and bottlenecks in current certification processes;
- Minutes of meetings with User Group members. In the ASCOS project a User Group (UG) was established with the intent to represent the relevant stakeholders involved in certification. These expectations of these stakeholders were extracted based on a review of past ASCOS technical meetings in which they participated;
- FAA Certification Airplane Certification Process Study (CPS) [31]. The FAA CPS is the most authoritative reference retrieved from the literature that documents the essential problems and bottlenecks in commercial aviation certification. The study is based on a comprehensive review of the processes and procedures associated with aircraft certification, operations and maintenance, commencing from the initial type certification activities, and extending to the continued operational safety and airworthiness processes. Cross-checking the areas of the framework with the findings of the CPS enabled to further ensure that the framework addresses areas that are of relevance for certification.

Table 4, Table 5, and Table 6 reports the final version of the performance frameworks that have been used during the exercises. These versions represents a refinement of their initial version (proposed under D5.1). In particular, while the initial versions were defined over the period Feb-May 2014, the refined versions were prepared immediately prior to each exercise, keeping into account the practical, logistics of the exercise

(mostly available time for discussion and number of participants) which were not yet defined when the D5.1 was prepared.

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.	Questionnaire items
2. Soundness	The extent to which the 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.	Questionnaire items
3. Cross-domain integration	The extent to which the ASCOS approach promotes integration, coordination, and exchange of information across the different stakeholders that may be involved in the certification of a change.	Questionnaire items
4. Harmonization	The extent to which ASCOS looks compatible with the different certification approaches in use in different domains (e.g. ATC vs aviation) and geographical areas.	Questionnaire items
5. Accommodation of Innovation	The extent to which ASCOS makes more likely the certification of innovative products and systems, i.e. products and systems for which no standard are available.	Questionnaire items
6. Acceptability	The extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority.	Questionnaire items
7. Flexibility	The extent to which the proposed ASCOS approach can be applied to a broad range of different types of products, systems, and services, varying in size and complexity.	Questionnaire items

Table 5. KPAs for the proposed ASCOS SPI framework and Tool for Continuous Safety Monitoring (Exercise 2).

Evaluated ASCOS results	KPA	Definition	Metric
ASCOS SPI Framework	1. Soundness	The extent to which the ASCOS SPI framework promotes, in certification, the consideration of relevant hazards that today are not or are poorly considered (with specific reference to the TAS related hazards).	Questionnaire items
	2. Completeness	The extent to which the proposed SPI framework covers the different (certification) domains of the TAS.	Questionnaire items
	3. Standardization	The extent to which the proposed SPI framework can become a standard reference framework in use across the different actors of the TAS.	Questionnaire items
ASCOS Tool for Continuous Safety Monitoring	4. Usefulness	The extent to which the proposed ASCOS is perceived as a tool useful for supporting continuous safety monitoring,	Questionnaire items

Table 6. KPAs for the proposed ASCOS Risk Model and the Tool for risk assessment (Exercise 3).

Evaluated ASCOS results	KPA	Definition	Metric
ASCOS Risk Model	1. Soundness	The extent to which the ASCOS Risk Model promotes, in certification, the consideration of relevant hazards that today are not or are poorly considered (with specific reference to the TAS related hazards).	Questionnaire item
	2. Completeness	The extent to which the ASCOS Risk Model covers, the different hazards of the TAS.	Questionnaire item
	3. Standardization	The extent to which the proposed risk model can become a standard model used by the different actors of the TAS.	Questionnaire item
	4. Acceptability	The extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority.	Questionnaire item
ASCOS Tool for risk assessment	1. Manipulability	The extent to which the Tool for risk assessment promotes a useful means to manipulate—i.e. access, edit, modify— the ASCOS ESDs and FTs.	Questionnaire item
	2. Quantification capability	The extent to which the Tool for risk assessment can calculate the risk quantification.	Questionnaire item
	3. Cross-domain integration	The extent to which the Tool for risk assessment promotes integration, coordination, and exchange of information across the different stakeholders that may be involved in certification.	Questionnaire item
	4. Standardization	The extent to which the proposed tool can become a standard reference framework in use across the different actors of the TAS.	Questionnaire items
	5. Acceptability	The extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority.	Questionnaire items
	6. Usability	The extent to which the proposed risk model provides a usable means for supporting risk assessment.	SUS index

Table 4. KPAs for the ASCOS proposed certification approach (Exercise 1).

KPA	Definition	Metric
8. 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.	Questionnaire items
9. Soundness	The extent to which the 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.	Questionnaire items
10. Cross-domain integration	The extent to which the ASCOS approach promotes integration, coordination, and exchange of information across the different stakeholders that may be involved in the certification of a change.	Questionnaire items
11. Harmonization	The extent to which ASCOS looks compatible with the different certification approaches in use in different domains (e.g. ATC vs aviation) and geographical areas.	Questionnaire items
12. Accommodation of Innovation	The extent to which ASCOS makes more likely the certification of innovative products and systems, i.e. products and systems for which no standard are available.	Questionnaire items
13. Acceptability	The extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority.	Questionnaire items
14. Flexibility	The extent to which the proposed ASCOS approach can be applied to a broad range of different types of products, systems, and services, varying in size and complexity.	Questionnaire items

Table 5. KPAs for the proposed ASCOS SPI framework and Tool for Continuous Safety Monitoring (Exercise 2).

Evaluated ASCOS results	KPA	Definition	Metric
ASCOS SPI Framework	5. Soundness	The extent to which the ASCOS SPI framework promotes, in certification, the consideration of relevant hazards that today are not or are poorly considered (with specific reference to the TAS related hazards).	Questionnaire items
	6. Completeness	The extent to which the proposed SPI framework covers the different (certification) domains of the TAS.	Questionnaire items
	7. Standardization	The extent to which the proposed SPI framework can become a standard reference framework in use across the different actors of the TAS.	Questionnaire items
ASCOS Tool for Continuous Safety Monitoring	8. Usefulness	The extent to which the proposed ASCOS is perceived as a tool useful for supporting continuous safety monitoring,	Questionnaire items

Table 6. KPAs for the proposed ASCOS Risk Model and the Tool for risk assessment (Exercise 3).

Evaluated ASCOS results	KPA	Definition	Metric
ASCOS Risk Model	5. Soundness	The extent to which the ASCOS Risk Model promotes, in certification, the consideration of relevant hazards that today are not or are poorly considered (with specific reference to the TAS related hazards).	Questionnaire item
	6. Completeness	The extent to which the ASCOS Risk Model covers, the different hazards of the TAS.	Questionnaire item
	7. Standardization	The extent to which the proposed risk model can become a standard model used by the different actors of the TAS.	Questionnaire item
	8. Acceptability	The extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority.	Questionnaire item
ASCOS Tool for risk assessment	7. Manipulability	The extent to which the Tool for risk assessment promotes a useful means to manipulate—i.e. access, edit, modify— the ASCOS ESDs and FTs.	Questionnaire item
	8. Quantification capability	The extent to which the Tool for risk assessment can calculate the risk quantification.	Questionnaire item
	9. Cross-domain integration	The extent to which the Tool for risk assessment promotes integration, coordination, and exchange of information across the different stakeholders that may be involved in certification.	Questionnaire item
	10. Standardization	The extent to which the proposed tool can become a standard reference framework in use across the different actors of the TAS.	Questionnaire items
	11. Acceptability	The extent to which the proposed ASCOS approach looks acceptable to the applicant and the certifying authority.	Questionnaire items
	12. Usability	The extent to which the proposed risk model provides a usable means for supporting risk assessment.	SUS index

Appendix B Management of safety activities for Total Aviation system

(The present appendix reports the content of section 7 of D3.5a [13]*)*

All the activities described in previous chapters and in relation with the setup of a common safety standard framework and a continuous improvement of safety standard loop are possible only if initiated, promoted, coordinated and monitored from the highest level to the lowest level of a project development.

In complex multi-stakeholder organization, interfaces are often responsible for gaps in safety assessment. It is then necessary to introduce high level organization standards defining interrelations and responsibilities and setting up strict management rules.

Of primary target are Project breakdown structures. These activities should be harmonized and coordinated at the highest level. Of most importance is the identification of safety standards to apply for development. These safety standards should formalize processes for requirement capture, requirement validation, requirement application verification, project organization /documentation, deliverables management, schedule management, process assurance, configuration management. Of most importance are also the "Safety plans" and the safety requirement validation plan, without which there will be no assurance of any safety method application.

Although the operational reliability and the integrated logistic support activities are not strictly speaking part of the safety and certification, these activities can be integrated within the same framework as safety activities

To assure a good interface management between the different stakeholders of a project, a sound and seamless engineering, the continuity of safety assessment practices and the seamless application of the rules, all the activities described in previous chapters should be promoted, initiated, coordinated and monitored at:

- TAS inter-stakeholder level by a central coordination group called here after "TAS Engineering and Safety Group" (TESG)
- TAS stakeholder level by a stakeholder level coordination group called here after stakeholder "Engineering and safety group" (SESG).

The ESG groups are coordination groups that can be under the responsibility of existing bodies or new body as necessary.

At total aviation system the TESG group should include participants from each stakeholder of the total aviation system. It will be the interface with EASA and ICAO

At each stakeholder level the SESG group should include participants from each sub stakeholder in relation with the considered stakeholder. It is the interface with the TESG and local authorities as needed

The organization of the different level ESG groups is illustrated in the following figure:

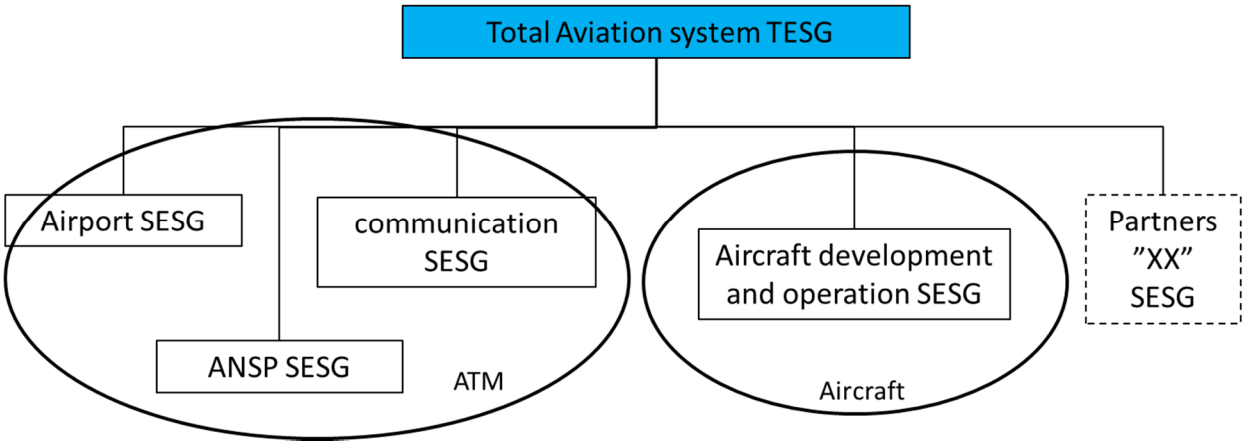

Figure 8- Safety management organization at TAS inter-stakeholder level and at stakeholder level

These Engineering and safety group organization should be implemented in the earliest phase of a development plan. The organization description of these groups, their management activities, their responsibility and the deliverables they should produce should be described in the inter-stakeholder safety plan and in each stakeholder safety plan.

The Total Aviation system "Engineering and Safety Group" (TESG) will be chartered to perform and/or monitor the inter-stakeholder total aviation system safety tasks during development and during operation. To structure product development safety tasks the TESG responsibilities may be to:

1. Identify and promote coherent safety standards framework to apply at inter-stakeholder level and at each stakeholder level for product development, interface management, safety assessment methods, software item development, electronic hardware item development, procedure and services development (including human factor)
2. Develop a safety plan and methods for the inter-stakeholder safety activities
3. Assure coherency between the tools used by the different TAS stakeholders
4. Promote safety culture and assure that safety training courses are available and given to safety involved people
5. Assure that lessons learned processes are established within each stakeholder organization
6. Identify safety lessons learned from previous accidents and provide visibility to each stakeholder
7. Establish and communicate the principles and data to apply to assure coherency between the safety assessments performed by each stakeholder
8. Assure compliance with ICAO SMM and European Aviation Safety Plan (EASP)

9. Identify inter-stakeholder accident scenarios with associated “Event Sequence Diagrams” (ESD)
10. Identify Area of Change to consider with associated future accident scenarios and ESD
11. Establish and allocate the safety objectives and the studies to perform by each stakeholder that contribute to the inter-stakeholder ESD
12. Monitor the completion of each stakeholder contribution to inter-stakeholder ESD
13. Perform inter-stakeholder Common Mode Analyses and evaluate Common Mode Analysis from each stakeholder
14. Issue total aviation system safety results
15. Coordinate with TAS certification authorities
16. Monitor the TAS level lessons learned and standards improvement process

To structure in operation safety assurance task and perform an efficient in operation safety follow up the TESG responsibilities are to set a unifying TAS Safety Management Process guide to allow exchanges of safety information necessary to perform the safety assurance at TAS level. For each organizational activity the management process may be based on the following:

1. A safety assurance plan describing the Safety Management Strategy and associated tasks for in operation safety assurance. This plan should be compliant with the TAS Safety Management Process Guide and with the regulation applicable to each individual organization. The safety assurance plan should particularly identify all the tasks associated to dissemination of safety information between the TAS stakeholders through the TAS level ESG (TESG).

   This plan may be structured around the activities recommended in:
   - **a.** the ARP 5150 for aircraft Safety Assessment in operation
   - **b.** The document “Management of risk: Guidance for Practitioners” (published by TSO (The Stationary Office) on behalf of Office of Government Commerce) applied by some ATM bodies
2. The safety methods to perform the tasks described in the safety plan

If a list of task to perform at TESG level is detailed in the above section, the details on the way the ESG groups will work together and be managed are not detailed further on purpose. This level of detail should be left to the internal decision inside the ESG structure to select the best and simplest way of working together at TAS level and at each stakeholder level.