WP4 Final Report
Certification case studies

A.L.C. Roelen, P.J. van der Geest, J.J. Scholte (NLR), S. Bravo Munoz, J.P. Heckmann, J.F. Delaigue (APSYS), F. Orlandi (TR6), H. Neufeldt (TATM), S. Bull (Ebeni), G. Temme (CertiFlyer)

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

Grant Agreement No.	314299
Document Identification	D4.6
Status	Approved
Version	1.1
Date of Issue	29-06-2015
Classification	Public

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	A.L.C. Roelen et al.	22-05-2015	All	Version for approval by PMT
1.1	A.L.C. Roelen et al.	24-06-2015		Comments PMT processed

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	M. Stuip, E. van de Sluis	15-05-2015
CAAi	A. Eaton	15-05-2015
Ebeni	A. Simpson	15-05-2015
Deep Blue	L. Save, S. Rozzi	15-05-2015
Avanssa	N. Aghdassi	15-05-2015
TR6	B. Pauly	15-05-2015
TATM	G. Schichtel, J.M. Kraus	15-05-2015
CertiFlyer	M. Heiligers	29-06-2015
Organisation Responsible for Approval	Name of person approving the document	Date
NLR	A. Roelen	21-05-2015
NLR	L.J.P. Speijker	30-06-2015

Document Distribution

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

Acronyms

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

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

This page is intentionally left blank

Executive Summary

This report describes the activities and results for ASCOS WP4 'certification case studies'. The objective of this WP is to apply the new certification approach and supporting tools in four case studies to evaluate the practical application of the proposed certification process adaptations. The four cases were the following:

- Certification of an Autonomous System Failure Management System for RPAS
- Certification of an Automatic Aircraft Recovery System
- Certification of a de-icing/anti-icing service provider
- Certification of an Integrated Surveillance System.

Each of these cases attempted to apply stages 1 to 5 of the initial proposed ASCOS certification approach (as described in ASCOS D1.3 [1]), which is being updated following constructive feedback and comments.

The case studies were then evaluated from three angles: Firstly, the application of the certification approach and tools, the experienced benefits, lessons learned, conclusions and recommendations from the four case studies were analysed at an aggregate level to formulate conclusions and recommendations regarding the ASCOS certification approach and supporting tools. Secondly, the four case studies were reviewed against the performance framework that defines Key Performance Areas (KPAs) for the ASCOS approach to evaluate the 'fitness for purpose' of the certification approach. Thirdly, the case studies were reviewed from a 'verification perspective' against a set of 'design' principles that was considered in the development of the certification approach. The aim was to evaluate the efficacy of the ASCOS approach and how it could be improved, rather than as a scoring mechanism for the quality of the case studies.

The evaluation resulted in 35 recommendations that are fed into ASCOS WP 1 to further improve the certification approach.

This page is intentionally left blank

Table of Contents

1 Introduction

1.1 Background

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

1.2 Objectives

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

1.3 Approach

Four case studies are defined involving the following topics:

- D4.1: Automated Failure Management System (AFMS) installed on an Remotely Piloted Aircraft System (RPAS). This AFMS is a system that replaces the pilot in all decision making and surveillance tasks normally performed by a pilot on board in case of failure. [6]
- D4.2: The (initial) development of a hypothetical Automatic Aircraft Recovery System (AARS) intended to reduce the number of Loss of Control accidents by providing an on-board system that can recover the aircraft automatically from Loss of Control or Loss of Situational Awareness events. [7]
- D4.3: The certification of a de-icing/anti-icing service provider. This case study assumes a hypothetical situation in which the de-icing/anti-icing service provider is responsible and accountable for its safe operation in compliance with assumed novel regulations. [8]
- D4.4: The certification of an Integrated Surveillance System (ISS) consisting of cooperative surveillance and independent non-cooperative surveillance systems. [9]

The proposed ASCOS certification approach consists of the following stages:

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

11. Ongoing monitoring and maintenance of certification

The certification approach and stages are further explained in Appendix A.

After conducting the four case studies, they are evaluated from three angles:

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

1.4 Document structure

The document is organised as follows. Chapters 2-5 describe the case studies and chapter 6 describes the evaluation of the case studies. Conclusions and recommendations are provided in Chapter 7.

2 Case study 1: Certification of an Autonomous System Failure Management System for RPAS

2.1 Description of the change

The change consists in the Autonomous Failure Management System of a Remote Piloted Aircraft System. The RPAS is conceived as a modification of a civil cargo piloted aircraft similar in size to an Airbus A320. RPAS is expected to fly in airspace class A, B and C.

The RPAS presents several modes of autonomy, from autonomous mode to manned mode. In the autonomous mode, the RPAS can adapt its speed and execute flight commands received from ATC, it can as well take decisions relative to failure management or/and to an external events. In this mode the remote pilot is considered as a backup. The remote pilot can, at any moment, revert to manned mode.

In manned mode the remote pilot performs all functions currently allocated to a pilot on board, specific sensors and cameras can be envisaged to replace the physical sensations of a pilot on board. The RPAS is permanently automatically protected by system (flight envelope limitations, protection against stall, overrun…). These protections are already in place in the current aircraft. The level of protection corresponds to the level of the law used by flight controls (normal laws to direct laws).

The “see and avoid” duty performed by the pilot is replaced on the RPAS by a “detect and avoid” function based on specific sensors having capability to detect small, non-cooperative traffic (e.g.: gliders, VLAs), in particular when flying in class B or C airspaces.

The remote pilot communicates with the RPAS thought a C2 link. The C2 is used for transmitting commands from remote pilot station to RPAS (telecommand) and for transmitting data from RPAS to remote pilot station (telemetry). The remote pilot station is similar to a current cockpit. For the purpose of Use Case, the performance of the C2 link is sufficient for the continuity and integrity of the function, in the case of erroneous/loss C2 link between the RPAS and the remote pilot station the AutoFailMS will manage the failure.

The Autonomous Failure Management system function is to detect and react to failures of the RPAS and to respond autonomously to these failures as far as possible (using reconfiguration of the systems on the aircraft where appropriate), with the intention to remain on the original intended flight path if possible.

From the point of view of aircraft architecture the AutoFailMS is divided into two sub systems, the Failure Management sub-System (FailMS) and the Failure Reconfiguration sub-System (FailRS). The main difference among them lies in the logic implemented.

The FailMS considers the continuous monitoring of system status and the decision making process (prioritization) usually performed by the pilot during the course of the flight. The FailMS assesses the aircraft system technical status and authorize reconfiguration of aircraft systems in abnormal situation according to prioritization rules implemented on FailMS logics.

The FailRMS is in charge on failures and reconfiguration associated to one single system and it replaces the pilot on board in all those procedures that can be automated internally to one single system (e.g. in an aircraft equipped with several RA, pilot inhibits erroneous RA data and continues flying with remaining RA). The FailRMS, itself, is implemented internally to each system and it can be considered as an evolution of the current failure management already existing in the current systems. The FailRS collects the data of system status and transmits them to the FailMS.

2.2 Definition of the certification argument

The argument structure proposed for this case study is developed from the generic argument presented in D1.3 [1] section 3.2. For the purposes of the case study, only claims 1 and 2 of the argument will be developed in detail. The other claims will be developed only in respect of dependencies on and interface to other domains. Figure 1 shows the adaptation of the top level of the generic argument (see D1.3 **Error! Reference source not found.** section 3.2) to this case study.

The claim is that the Autonomous Failure Management system adequately supports safe RPAS operations. For the purpose of this case study it is decided that it is up to the certification authorities (EASA, CAA, etc.) to define the proper level of safety for RPAS operations.

For the purpose of this case study it is agreed that the proper level of safety for RPAS operations means "that introduction of the RPAS must achieve a level of safety which is no worse than that achieved in equivalent manned operations"

Note the following points.

- *The claim covers the lifecycle of the change* – i.e. it covers specification, design and implementation of the AutoFailMS for RPAS; it also covers transition into operation and monitoring while in operation. Each of these elements is covered in a separate subclaim.

- *We do not claim that RPAS operations as a whole are acceptably safe* – we are only considering how the *Autonomous Failure Management System* contributes to the safety of the operation of the RPAS. To make a claim for RPAS operations as a whole, we need to consider significant areas outside the scope of the case study (i.e. the normal operation of an RPAS, including the need for a Detect and Avoid function);

- *We will consider both the positive and negative effects of the Autonomous Failure Management System on the safety of the RPAS* – i.e. we consider how the *Autonomous Failure Management System* benefits the RPAS by "rescuing" it from failures of other systems, as well as how failure of the *Autonomous Failure Management System* itself may threaten the RPAS (and the wider TAS).

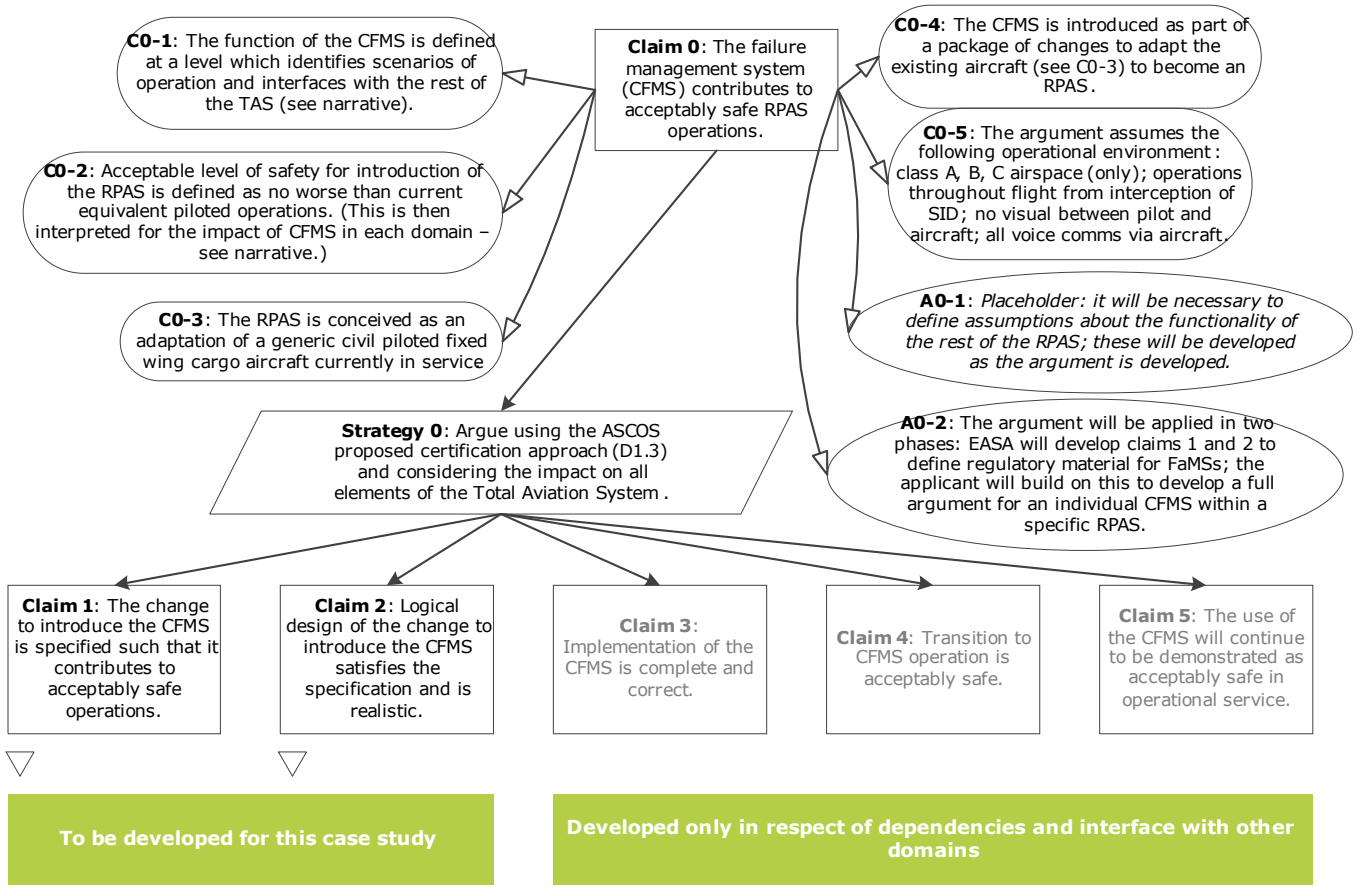


Figure 1: Top Level Argument Structure (Claim 0)

We define items of *context*, to add detail to the claim being made. These items of context are defined further in the following sections.

- **C0-1** provides(a pointer to) the definition, at an abstract functional level, of the operation of the Autonomous Failure Management System
- **C0-2** defines the level of safety which needs to be achieved by the introduction of the Autonomous Failure Management System.
- **C0-3** identifies that the RPAS is conceived as an adaptation of an existing civil piloted fixed wing cargo aircraft.
- **C0-4** identifies that the Autonomous Failure Management System will be introduced as part of a package of changes (to include provision of a Sense and Avoid function) to adapt the existing aircraft (as identified in C0-3) to become an RPAS.
- **C0-5** defines the operational environment to which the safety argument applies.

In addition, we introduce the following assumptions:

- a (placeholder) assumption (**A0-1**) to note that we will need to make a significant number of assumptions about the interface between the Autonomous Failure Management System the other RPAS systems.
- the assumption (**A0-2**) that the argument is applied in two phases.

The top level claim (Claim 0) is then decomposed into subclaims (Claims 1 – 5), each making a "smaller" claim about the Autonomous Failure Management System and its introduction as part of the RPAS system. The premise of the argument is that, when taken together, the subclaims are sufficient to demonstrate that the top level claim has been achieved. **Strategy 0** documents the approach which is taken in subdividing the claim – i.e. the approach proposed in ASCOSD1.3 **Error! Reference source not found.**– which considers specification, design, implementation, transition into operation and operational service.

2.3 Development and agreement of the certification plan

The certification plan is the reference for communication between the stakeholder which is seeking for certification of its product and the certification authority, which need to be entirely satisfied of the application by the stakeholder of applicable regulatory requirements before granting the certificate. The Certification Plan needs to contain at least the following elements:

- An overall description of the system, its limits and the way it is interfaced with other systems. This description is primarily intended for experts of the authority. It may highlight relevant aspects as technical novelties, and for changes involving multiple stakeholders, relationship with other products

for which a certification is sought by a partnering stakeholder. When more domains are affected the description must mention the relationships between the domains and the relevant assumptions

- Agreement with the authority on a full and consistent set of applicable regulatory requirements and related guidance material. This may require establishing a common agreement between the different authorities involved
- A framework to the authority on how to seek agreement on any further technical issues related to the interpretation of the regulatory requirements that may arise during the design and development of the product
- A comprehensive description of how the evidences will be produced that all the regulatory requirements are complied with
- Agreement with the authority on the organisation of Certification Deliverables. The Certification Deliverables are documents that need either to be approved or agreed or received by the authority prior to granting the certificate. They are to be considered as the core part of the Safety Case
- An overall description of how the "Continuing Safety activities" will be organized in compliance with the reference standards as the response to the mandatory requirements on safety, introducing actors, activities and key documents as output of these activities, including safety activity interface with partnering stakeholders

It can be seen from the applicable regulations on airborne products that they actually cover through essential requirements, lower level specifications and AMC all the safety aspects an RPAS aircraft product shall comply with: design, manufacture, maintenance, operation & training.

As a consequence, the development of an "argument architecture" for the RPAS product or for the AutoFailMS system is to be constructed as the elaboration of a full and consistent set of applicable regulatory requirements as the "baseline for certification", focusing primarily on existing acceptable guidance material and standards. The elaboration of the certification baseline is a key element of the certification plan, with the agreement of the plan requiring agreement of the baseline by the authority. This may require establishing an agreement in coordination with the partnering stakeholders and between the authorities involved in the different aviation domains, in order to ensure overall consistency of the different certification baselines proposed by the partners.

2.3.1 High level claim

The applicant of the RPAS airborne segment and designer of the AutoFailMS system has to seek for an agreement with its supervisory authority on a full and consistent set of applicable regulatory requirements and related guidance material. In order to ensure that the authority will be fully satisfied with the demonstration activities and results provided, this agreement needs to be established since the initial step of the RPAS product design.

The certification plan is presented to the relevant authorities and other stakeholders, to gain their agreement that, if the plan is followed and the evidence is presented, they will accept the change into service. Although lack of agreement at this stage does not prevent progress to later stages, the benefit of gaining agreement is

to reduce the risk to the certification programme at later stages. This approach can be developed further into requirements. These requirements may all (or mostly) be beneficial, but they introduce significant cost increases if they are introduced progressively through the project.

The ASCOS D1.3 approach proposes to structure the demonstration of safety by building upon the approach of [1] as per Stage 2, suggesting a top-level safety claim (Claim 0) that could be of the form: "The introduction on an RPAS/several RPAS in the air traffic environment shall keep the same level of safety", and then cascading this higher level claim in sub-claims.

Besides, and as part of their overall duty of protecting the public in general and the environment, the authorities of the aviation system continuously develop common safety and environmental rules. These rules are usually formulated as a structured argument of safety requirements. In some domains the argument is more formulated as a performance requirement than as a defined means of compliance (e.g. in the ATM domain).

As consequence, it must be checked whether the current rules and standards are an adequate argument to satisfy the claims it must also be checked whether the assumptions that are used between the domains are adequately addressed.

2.3.2 Means of Compliance argument for Claim 0

Within the Product Certification Domain

An RPAS considered as an aircraft of CS25 category should without restriction comply with the Essential Requirements for Airworthiness referred to in Article 5 of the Basic Regulation EC216/2008. These Essential Requirements are stated in the Basic Regulation Annex I, which first requirement reads:

1. *Product integrity: product integrity must be assured for all anticipated flight conditions for the operational life of the aircraft. Compliance with all requirements must be shown by assessment or analysis, supported, where necessary, by tests.*

This requirement and all subsequent requirements of Annex I are mandatory to the RPAS. Claim 0 of RPAS could thus be directly inferred from it:

> **Claim 0 of RPAS:** *The integrity of the RPAS product (i.e.: the RPAS system and operation)* ***is*** *assured for all anticipated flight conditions for the operational life of the RPAS system.*

All the subsequent requirements of Annex I applicable to RPAS are then as many points that can be expressed as sub-claims for the RPAS.

Now, developing on the safety requirements that would apply to the AutoFailMS as part of the RPAS system, two requirements of Annex I can be put under focus (amongst many others):

1. C.2. The aircraft, including those systems, equipment and appliances required for type-certification, or by operating rules, must function as intended under any foreseeable operating conditions,

throughout, and sufficiently beyond, the operational envelope of the aircraft, taking due account of the system, equipment or appliance operating environment. Other systems, equipment and appliance not required for type-certification, or by operating rules, whether functioning properly or improperly, must not reduce safety and must not adversely affect the proper functioning of any other system, equipment or appliance. Systems, equipment and appliances must be operable without needing exceptional skill or strength.

1. C.3. The aircraft systems, equipment and associated appliances, considered separately and in relation to each other, must be designed such that any catastrophic failure condition does not result from a single failure not shown to be extremely improbable and an inverse relationship must exist between the probability of a failure condition and the severity of its effect on the aircraft and its occupants.

Practically, there is actually no need to cascade claims for AutoFailMS from the RPAS level claims as the Essential Requirements have set up so far the essential requirements applicable to the RPAS constituent systems. Thus, Claim 0 of AutoFailMS could directly mirror ER 1.c.2 & ER 1.c.3:

> **Claim 0 of AutoFailMS:** The AutoFailMS system, **does** function as intended under any foreseeable operating conditions, throughout, and sufficiently beyond, the operational envelope of the RPAS, taking due account of the system operating environment.
>
> The AutoFailMS system considered separately and in relation to the other RPAS constituent systems **is** designed such that any catastrophic failure condition does not result from a single failure not shown to be extremely improbable and an inverse relationship must exist between the probability of a failure condition of AutoFailMS and the severity of its effect on the RPAS operation.

As a consequence, the very high level of safety requirements expressed in Annex I is rarely referred by the designers of aircraft products when more convenient and detailed requirements are expressed in some lower level regulations, like the CS25[1], which are accepted as means of compliance to the higher level requirements of Annex I. For example, article CS 25.1309 "Equipment, systems and installations" reads:

(a) The aeroplane equipment and systems must be designed and installed so that:

(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the aeroplane operating and environmental conditions.

(2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a) (1) of this paragraph.

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) does not result from a single failure; and

[1] CS (resp. FAR) are maintained by EASA (resp. FAA) and have no official mandatory status. They are established on grounds of previous experience cumulated by authorities, which gives them a "compulsory" status and explain their designation of "soft law".

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote.

It can be noted that the CS25.1309 details and extends the Essential Requirements on aircraft systems to Hazardous and Major Failure Conditions. So, same as above, the Claim 0 of AutoFailMS could be developed in two sub-claims, by directly mirroring CS25.1309 requirements:

> **Sub-claim 1 of AutoFailMS:** The AutoFailMS system **is** designed and installed so that it performs as intended under *all anticipated* operating and environmental conditions of the RPAS product.

> **Sub-claim 2 of AutoFailMS:** The AutoFailMS system, considered separately and in relation to the other RPAS constituent systems, **is** designed so that -
>
> (1) Any catastrophic failure condition is extremely improbable; and does not result from a single failure; and
>
> (2) Any hazardous failure condition is extremely remote; and
>
> (3) Any major failure condition is remote.

Where AMC25.1309, supplemented with AMC-RPAS.1309, provides for the agreed definitions and the qualitative and quantitative objectives for all the terms introduced in CS.

The reasoning can be pursued down to the AMC of CS25, with the example of AMC25.1309. Application of the well-known ARP 4754A/ED79A and its related standards is recognized by authority as the backbone of demonstration of compliance to the AMC25.1309.

Finally, as all aspects of certification cannot realistically be completed prior to the starting of design activities, the safety plan should propose to the authority a framework on how to seek agreement on any further technical issues related to the interpretation of the regulatory requirements and the need to consolidate the certification baseline that may arise during the design and development of the product. For EASA or FAA this would be the framework of EASA CRI process (Certification Review Item), or FAA IP process (Issue Paper), which is rather similar framework of discussion and agreement on technical issue in interpretation of the regulatory requirements established by these authorities.

Within the Remote Pilot

In a same way than any product intended for sale to the general public must be provided with a “notice of use” leaflet informing the customer of any limitation, precaution and limitation of use, an RPAS product will be required by the supervisory authority of the design to be provided with all necessary documentation for RPAS operation that will define the baseline and specific aspects of the handling of RPAS product for the intended operations. This approach will be very similar to the current approach done for an aircraft product for which operational documentation shall be established as component of the certified product. In addition to the operating manual (the FCOM) which is required by authorities, the AFM (Aircraft Flight Manual) is a document

specifically stating all the limitations and particular aspects the operator needs to comply with for safely handling of the product. The authority will have to certify the content of the AFM as part of the aircraft certification.

The RPAS operator will have to demonstrate to its supervisory authority it operates the RPAS system in conformance with the FCOM and AFM established by the RPAS designer. In case an RPAS operator would seek approval for RPAS operations that were not foreseen or anticipated during the design and certification of the RPAS, supplemental demonstration activities are required in order to demonstrate that safe operation is maintained. This demonstration is likely to involve the design authority (i.e.: the design organisation) and its authority, if the change is deemed significant by the operator's authority in terms of operational context or performance (for example, the extension of the maximum distance allowed to an emergency landing site).

Within the ATM domain

The demonstration of safe operation of RPAs would probably require specific involvement and handling of the ATCo (e.g.: contingency handling, specific communication channels, etc…) and key assumptions on ATCo working procedures or Air Traffic Services have to be done, entailing a change in ATM operation, it is expected that the description of the change is properly coordinated between the ATM partner(s) and the RPAS design partner(s).Based on this description of the change in ATM operations, each ATM partner will have then to demonstrate to its authority its ability to maintain safe operation of the ATM services following the change and the introduction of RPAS within the controlled traffic.

For those changes requiring coordination between the RPAS system holder and the ATM side, it is important to ensure that the certification process engaged by an RPAS applicant and its ATM stakeholder(s) towards their respective authorities is consistent and coordinated. Noting that for the ATM domain the structure of regulatory requirements is very similar to the airborne domain, with essential requirements (in 216/2008), "common" requirements (in 1035/2011) and future AMC[2], it is expected that the requirement for a risk based approach (i.e.: hazard identification, risk assessment and mitigation approach) would be led commonly by all stakeholders on grounds of a standard previously agreed with the authorities (for example by applying a standard methodology ED78A[3], AMC25.1309, ARP4754/ED79A, ARP 4761/ED135 or a similar approach formerly accepted by the authorities).

Within the Maintenance domain

The RPAS product will be required by the supervisory authority of the operator to be maintained in airworthy condition by an approved maintenance organisation complying with regulation EC2042/2003 and addendums ("Part M"). Maintenance shall be carried on in accordance with the maintenance instructions provided by the RPAS designer.

[2] It is worth noting that AMC or agreed industry standards are still to be published.
[3] ED78A methodology has been developed and applied in a number of air-ground applications involving multiple stakeholders, initially for datalink.

The RPAS product will be required by the supervisory authority of the design to be provided with all necessary documentation for maintenance. This approach will be very similar to the current approach done for an aircraft product for which maintenance documentation shall be established as component of the certified product. In addition to the maintenance manuals (the AMM, SRM, etc…) which are required by authorities, the Instructions for Continued Airworthiness (ICA) document all the maintenance aspects that are critical for maintaining safe operation of the product. In the case of an RPAS system it might include the ground station. The authority will have to certify the content of the ICA section as part of the aircraft certification.

2.4 Specification and design

The normal, abnormal and failure scenarios have been developed to identify the generic hazards. The proper level of detail to include in the scenarios is a key element to ensure that all the hazards at TAS level have been identified. The failure scenarios also desribe the impact on the remote pilot (e.g. increase of pilot workload). Although the objective of this case study is restricted to AutoFailMs, the failure scenarios include explicitly description of combination of AutoFAilMS failure with “C2 failure” or “detect and avoid” failure or “loss of datalink” failure. These combinations of failure can impact on the ATM emergency procedures.

The complete and correct identification of hazards need to be supported by an agreed methodology that common to all TAS stakeholders. In this case study the identification of hazards has been performed by analysis the impact of the failures in several domains on several domains.

Table 1 presents the list of hazards. The hazards have been classified according to three domains:

- Aircraft and AutoFailMS system.
- Remote Pilot.
- ATM.

For this case study, it is suggested that the quantitative safety objective associated to each hazard is:

Severity	Probability
CAT	Extremely improbable
HAZ	Extremely remote
MAJ	Remote
MIN	Probable

Table 1: Hazard list

Ident	name	Effect on RPAS (aircraft level)	Effect on Air Crew (remote pilot)	Effects on Air Traffic Service	Final severity
GEN_HAZ_1	**slight increase of controller workload**	N/A	N/A	Class IV according to ER-010	MIN
GEN_HAZ_2	**significant increase of controller workload**	N/A	N/A	Class III according to ER-010	MAJ
GEN_HAZ_3	**large increase of controller workload**	N/A	N/A	Class III according to ER-010	MAJ
GEN_HAZ_4	**slight increase of pilot workload**	N/A	MIN as per JARUS Class IV according to ER-010	N/A	MIN
GEN_HAZ_5	**significant increase of pilot workload**	N/A	MAJ as per JARUS Class III according to ER-010	N/A	MAJ
GEN_HAZ_6	**large increase of pilot workload**	N/A	HAZ as per JARUS Class III according to ER-010	N/A	HAZ
GEN_HAZ_7	**Loss of RPAS C2 link No loss of datalink ATC. RPAS controlled by AutoFailMS**	MAJ. Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in functional capabilities.	N/A pilot cannot control the RPAS	AutoFailMS managed the RPAS, detect and avoid function is not lost. FP 1 Class V as per ER-010 However it is expected that situation might increase controller workload. Class IV.	MAJ
GEN_HAZ_8	**loss of RPAS communication no loss of C2 RPAS controlled by AutoFailMS**	MAJ. Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in functional capabilities.	Increase on pilot workload as part of pilot duties. MIN. Pass to voice communication	It is expected that situation might increase controller workload. Class IV.	MAJ

Ident	name	Effect on RPAS (aircraft level)	Effect on Air Crew (remote pilot)	Effects on Air Traffic Service	Final severity
GEN_HAZ_9	**Loss of RPAS communication and C2. RPAS controlled by AutoFailMS**	HAZ Loss of the RPA where it can be reasonably expected that a fatality will not occur The RPAS does no send reports although it is controlled by AutoFailMS and it is reasonable to expect that it follows last flight plan update.	N/A pilot cannot communicate with the RPAS	AutoFailMS managed the RPAS, detect and avoid function is not lost. FP 1 Class V as per ER-010 However it is expected that even if the RPAS cannot report its position (loss of datalink) so the controller will probably need deviate aircraft in the vicinity Class III...	HAZ
GEN_HAZ_10	**Loss of AutoFailMS (pilot revert to manned mode)**	MAJ significant reduction in functional capabilities.	Increase on pilot workload as part of pilot duties. MIN.	Remote pilot manages the RPAS, detect and avoid function is not lost. FP 1	MAJ
GEN_HAZ_11	**Total loss of RPAS control (no AutoFailMS and no pilot)**	CAT Failure conditions that could result in one or more fatalities.	N/A pilot cannot communicate with the RPAS	Total loss of RPAS control. RPAS is not supposed to follow last flight plan update. It is supposed to have detected and avoid function operative. Class II	CAT
GEN_HAZ_12	**loss of adherence to flight plan**	NSE failure conditions that would not affect the operational capability of the RPAS	MIN, slight increase of pilot workload As per JARUS	MIN slight increase in remote crew workload, such as flight plan changes. As per JARUS Class V as per ER-010	MIN
GEN_HAZ_13	**Slight Reduction in separation assurance**	MIN slight reduction separation assurance.	MAJ failure condition has a significant increase in remote crew workload	Class II as per ER-010 (or class III)	MAJ
GEN_HAZ_14	Large reduction of separation	MAJ significant reduction in separation assurance.	MAJ e failure condition has a significant increase in remote crew workload	Class II as per ER-010	MAJ
GEN_HAZ_15	Total loss of separation	HAZ large reduction in safety margins	MAJ e failure condition has a significant increase in remote crew workload	Class II as per ER-010	HAZ
GEN_HAZ_16	**loss of collision avoidance**	HAZ large reduction in safety margins	HAZ large increase of pilot workload. Pilots needs to avoids collision	FP 1 no collision avoidance. Class I	HAZ

Ident	name	Effect on RPAS (aircraft level)	Effect on Air Crew (remote pilot)	Effects on Air Traffic Service	Final severity
GEN_HAZ_17	**missed approach**	NSE failure conditions that would not affect the operational capability of the RPAS	MIN slight increase in remote crew workload	At worst class III, Significant increase of air traffic controller that needs to separate other traffic.	MAJ
GEN_HAZ_18	**landing emergency site**	NSE failure conditions that would not affect the operational capability of the RPAS	MIN slight increase in remote crew workload	At worst class III, Significant increase of air traffic controller that needs to separate other traffic.	MAJ

The safety objectives (both in terms quantitative and qualitative) need to be cascaded to each of the stakeholder. Once it is agreed which is the safety contribution of each stakeholder to the safety objective, it is possible to properly allocate safety requirements. For this use Case, it has been suggested that the safety objectives are allocated to the RPAS and to the AutoFailMs, and therefore, they are met by ARP 4754A/ED 79A standards. In this case study it is assumed that the quantitative and quantitative overall safety objective should not be less demanding than currently required for aircraft.

3 Case study 2: Certification of an Automatic Aircraft Recovery System

3.1 Description of the change

The change is defined as the introduction of a technical device on-board of commercial aircraft that recovers the aircraft automatically from a loss of control or loss of situational awareness situation with one pilot button push. The proposed function to be provided by the auto-recovery system is to provide after pilot initiation a rapid and automatic recovery of the aircraft to a stable flight regime within the flight envelope from any initial flight condition within or outside the normal flight envelope and with or without failures to the automatic and/or primary flight control system and/or to engines. The stable flight regime should be maintained for sufficient time for the pilot to regain adequate situational awareness, to diagnose any problem and to identify correct interventions to ensure continued safe flight.

Functional requirements for the system, at highest level, are:

1. The system shall be initiated by the pilot;
2. The recovery shall be performed without any further intervention of the pilot;
3. The recovery shall be performed succesfully, from any intial condition, in the presence of failures in the automatic and/or primary flight control system and/or engines.
4. The recovery shall result in restoring a stable flight regime for some period of time.

The system design will take into account the following (initial list of assumptions):

- The AARS will always in hot stand by, when the aircraft is airborne
- Actuation systems are fully operational
- The AARS will be installed in large aircraft (CS25)
- The recovery system can be used in case of failures to the automatic and/or primary flight control system and/or engines, but also in case there are no failures and the flight crew has lost control or when the flight crew is disorientated. It is assumed that the automatic and/or primary flight control system provides “commands” to the actuators (whatever type they are, electrically or hydraulically), which are assumed to function correctly. When the automatic recovery system is activated it will also generate commands to the actuators. If there are failures in the actuators the recovery system will not be able to recover stable flight. The same applies to the control surfaces, which are assumed to be intact. It is assumed that the engine control system is a dedicated system (such as FADEC) to control the engines. When the automatic recovery system is activated it will generate commands to the engine control system, which must be available and working such that (remaining) engines can still be controlled.

3.2 Definition of the certification argument

The following figure provides an initial argument structure for the certification of an Aircraft Automatic Recovery System (AARS).

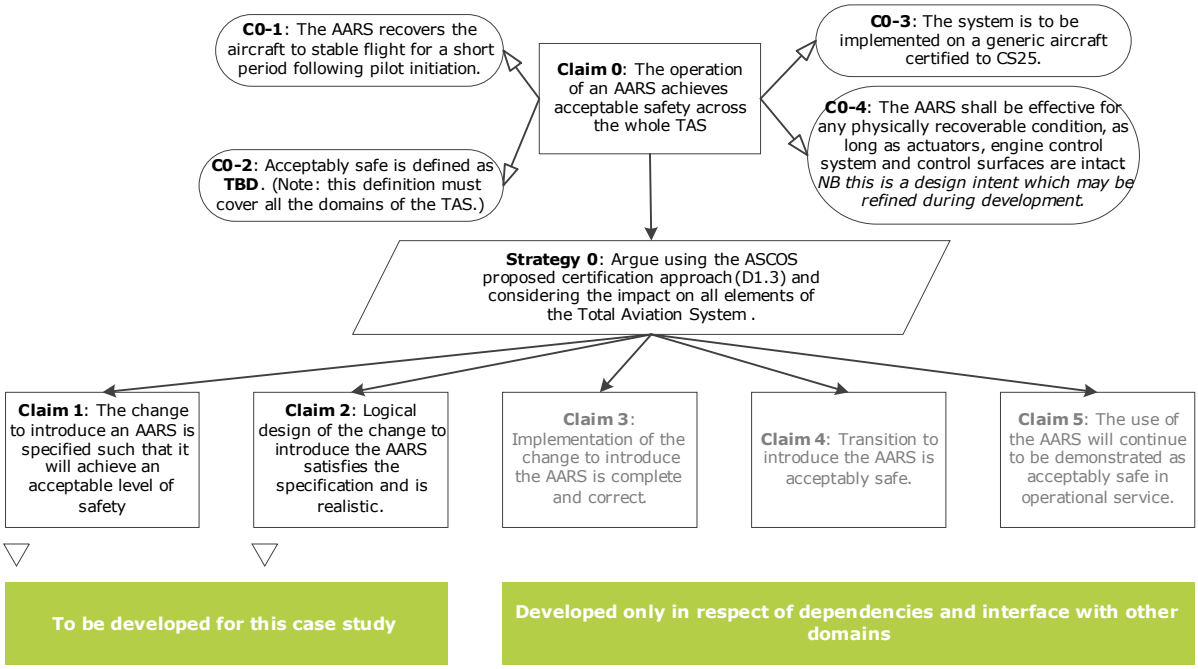


Figure 2: Top Level Argument Structure (Claim 0).

3.3 Development and agreement of the certification plan

The certification plan is presented to the relevant authorities and other stakeholders, to gain their agreement that, if the plan is followed and the evidence is presented, they will accept the change into service. Although lack of agreement at this stage does not prevent progress to later stages, the benefit of gaining agreement is to reduce the risk to the certification programme at later stages. This approach can be developed further into requirements. These requirements may all (or mostly) be beneficial, but they introduce significant cost increases if they are introduced progressively through the project.

The ASCOS D1.3 approach proposes to structure the demonstration of safety by building upon the approach of the initial argument architecture as per stage 2, suggesting a top-level safety claim (Claim 0) that could be of the form:

Claim 0 : The operation of an AARS achieves acceptable safety across the whole TAS

and then cascading this higher level claim in sub-claims.

Besides, and as part of their overall duty of protecting the public in general and the environment, the authorities of the aviation system continuously develop common safety and environmental rules. These rules are usually formulated as a structured argument of safety requirements. In some domains the argument is more formulated as a performance requirement than as a defined means of compliance (e.g. in the ATM domain).

As a consequence, it must be checked whether the current rules and standards are an adequate argument to satisfy the claims. It must also be checked whether the assumptions that are used between the domains are adequately addressed.

Means of compliance argument for Claim 0:

- It will be shown by testing that the AARS fulfils the required functionality of stabilizing the aircraft after for a short period after pilot initialization. (CO-1)
- The required level of safety will be defined by the current level of safety combined with the required improvement as defined by EASA in their Safety Plan. The safety objective for the addition of an Aircraft Recovery System is described as “acceptably safe”. This needs to be further refined in order to be able to set the safety standard in the Certification plan. Each domain will constitute an argument on a lower level with its correlated CO’s. The total safety level of this change will then be built from the safety levels achieved in the different domains that are considered to be involved:
    1. Aircraft certification
    2. Air operator certification
    3. ATM certification
- It would be logical to use the current certification methods that are used in the different domains and focus for ASCOS on the combination of these. This would enable the application of the new certification method (as in D1.3) on this level. If there is then a problem detected with the fusion of these domains, a further investigation on the applicability in a particular domain can be made. This will then require a much more detailed description of the impact in that domain. In order not to lower the current safety standard it may be necessary to include EGPWS and TCAS in the system definition. Otherwise, an uncontrolled move of the aircraft could infringe on the margins of terrain clearance and aircraft separation. (CO-2)
- The conditions in which the service provider takes action are not crisply defined currently, but the service provider must take action based on the inspection of aircraft if the conditions are “conducive to ice accretion”. This philosophy is not like to change in the near future. There have been attempts to design systems that can measure ice accretion on aircraft services, but these have not been found acceptably reliable yet. (CO-3)
- The current standards and practices are designed based also on previous accidents and incidents. All the knowledge and experience from these accidents and incidents is condensed in these standards and practices and therefore it is advised to use these in order to comply with CO-4. If the way of working will be different from the current standard, the applicant will argue the level of safety to the Authority by means of established techniques (e.g. FHA / PSSA / HF evaluations etc.)

The main difference lies in the division of responsibilities. These will have to be defined in detail and laid down in the compliance documents.

3.4 Specification

Stage 4 of the certification methodology broadly aligns with the Functional Hazard Analysis process. The functional hazard analysis basically addresses four elements:

1. What are the **system generated hazards**, that are related to the system performing its intended function. A system-generated hazard is one which is generated (or affected) by the introduction of the new function, but which is not a hazard which the function is designed to mitigate. Examples are: when the AARS is engaged it might interfere with TCAS or EGPWS and introduce a hazard (such as increased probability of CFIT or MAC) that otherwise would not exist (in the technical or operational domain), or it might interfere with the function of ATC to provide separation (in the ATM domain).
2. What are the hazards, related to a **detected failure of the system** to perform its intended function. For example: the system is not functional and the flight crew is aware of the unavailability of the system. In other words, when a LOC situation occurs the flight crew cannot rely on the system to perform a recovery manoeuvre. This is related to the reliability of the system.
3. What are the hazards, related to **an undetected failure of the system** to perform its intended function. For example: the system is not functional and the flight crew in not aware of the loss of functionality of the system. In other words, when a LOC situation occurs the flight crew will rely on the system to perform a recovery manoeuvre. However, the system will not perform its intended function. This is related to the integrity of the system.
4. What are the hazards, related to **erroneous operation of the system.**
   For example, the system provides erroneous control inputs (e.g. soft or hard over), or provides misleading information, before or after engagement of the system.

Table 2 provides a list of identified hazards and their severities.

Nr	Hazard	Hazard type	Hazard Domain	Severity
TS.1	TCAS alert during recovery manoeuvre	System generated	Technical	major
TS.2	EGPWS alert during recovery manoeuvre	System generated	Technical	hazardous
OS.1	Pilot follows TCAS alert during recovery manoeuvre	System generated	Operational	catastrophic
OS.2	Pilot follows EGPWS alert during recovery manoeuvre	System generated	Operational	catastrophic
OS.3	Pilot does not recognize LOC or LSA condition properly and fails to engage AARS.	System generated	Operational	hazardous
AS.1	During recovery manoeuvre the aircraft deviates significantly from the assigned ATM clearance (laterally or vertically)	System generated	ATM	major
TD.1	LOC or LSA condition occurs while the AARS is flagged as unavailable	Detected failure	Technical	hazardous
TD.2	AARS fails during a recovery procedure in progress, and provides an annunciation to	Detected failure	Technical	catastrophic

Nr	Hazard	Hazard type	Hazard Domain	Severity
	the pilot of its failure			
OD.1	Pilot unable to perform a manual recovery in case AARS is unavailable.	Detected failure	Operational	catastrophic
TU.1	AARS unable to initiate and perform recovery manoeuvre when LOC or LSA conditions occur	Undetected failure	Technical	catastrophic
TU.2	AARS unable to terminate the recovery manoeuvre, after successful recovery	Undetected failure	Technical	minor
AU.1	Failure to communicate with ATC that recovery is in progress	Undetected failure	ATM	hazardous
TE.1	AARS is self-engaged, without appropriate pilot input	Erroneous operation	Technical	major
TE.2	The AARS drives one or more control surfaces or engine controls to the limit, at maximum rate (hard-over)	Erroneous operation	Technical	catastrophic
TE.3	The AARS drives one or more control surfaces or engine controls to an incorrect position, during recovery	Erroneous operation	Technical	catastrophic

The high level safety requirements are derived from the results of the Functional Hazard Analysis. From the severity of the hazards, that are associated with the introduction of the system functions (and corresponding functional failures), the safety requirements for each of the functions can be derived. In order to achieve acceptable safety the probability of occurrence of a functional failure shall be inversely related to the corresponding severity.

3.5 Design

the objective of stage 5 (‘Design’) is to demonstrate that Claim 2 of the generic safety argument is met, namely that the logical design of the AARS has the functionality and behavioural and performance attributes necessary to satisfy the functional specification considered in Claim 1. This claim considers all normal, abnormal, degraded and emergency conditions of the operational environment. In addition, this claim considers all the possible hazardous failure modes of the logical design and sets mitigations and assurance requirements such that the system is acceptably safe in the presence of these failures.

In this context, logical design is a high-level architectural representation, independent from the physical implementation. As such it considers the functions provided by the system elements (i.e. human roles and tasks and machine-based functions), but not the equipment, personnel or procedures which provide these functions.

Levels of development assurance (DALs) must be determined to ensure that the mitigating requirements are successful in making the system sufficiently safe.

Table X provides for number of logical elements the assigned DAL. For the sake of brevity not all hazards have been addressed.

Table X: AARS related functional failures and DAL assignments

Fail. ID	Description	Logical element(s)	Domain(s)	Severity	(F)DAL
MF.1	One or more functions in the AARS HW/SW unit fail.	AARS processing	A/C manuf.	CAT	B
MF.2	The display functionality of the CMD/CTL display unit fails.	AARS CMD/CTL & display unit	A/C manuf.	CAT	B
MF.3	The recovery initiation functionality of the CMD/CTL display unit fails	AARS CMD/CTL & display unit	A/C manuf.	CAT	B
MF.4	The recovery termination functionality of the CMD/CTL display unit fails.	AARS CMD/CTL & display unit	A/C manuf.	MIN	n/a
…					
OF.1	The flight crew fails (timely) to initiate the recovery action upon reaching a LOC or LSA situation	Flight crew	Aircraft operational	HAZ	?
…					
AF.1	The communication link between the flight crew and ATC (to inform ATC that the aeroplane is in recovery action) fails	AARS processing ATM equipment	A/C manuf. ATM equipmnt	HAZ HAZ	C ?
…					

4 Case study 3: Certification of an organisation

4.1 Description of the change

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

4.2 Definition of the certification argument

Figure 3 provides an initial argument structure for the certification of a de-icing/anti-icing service provider.

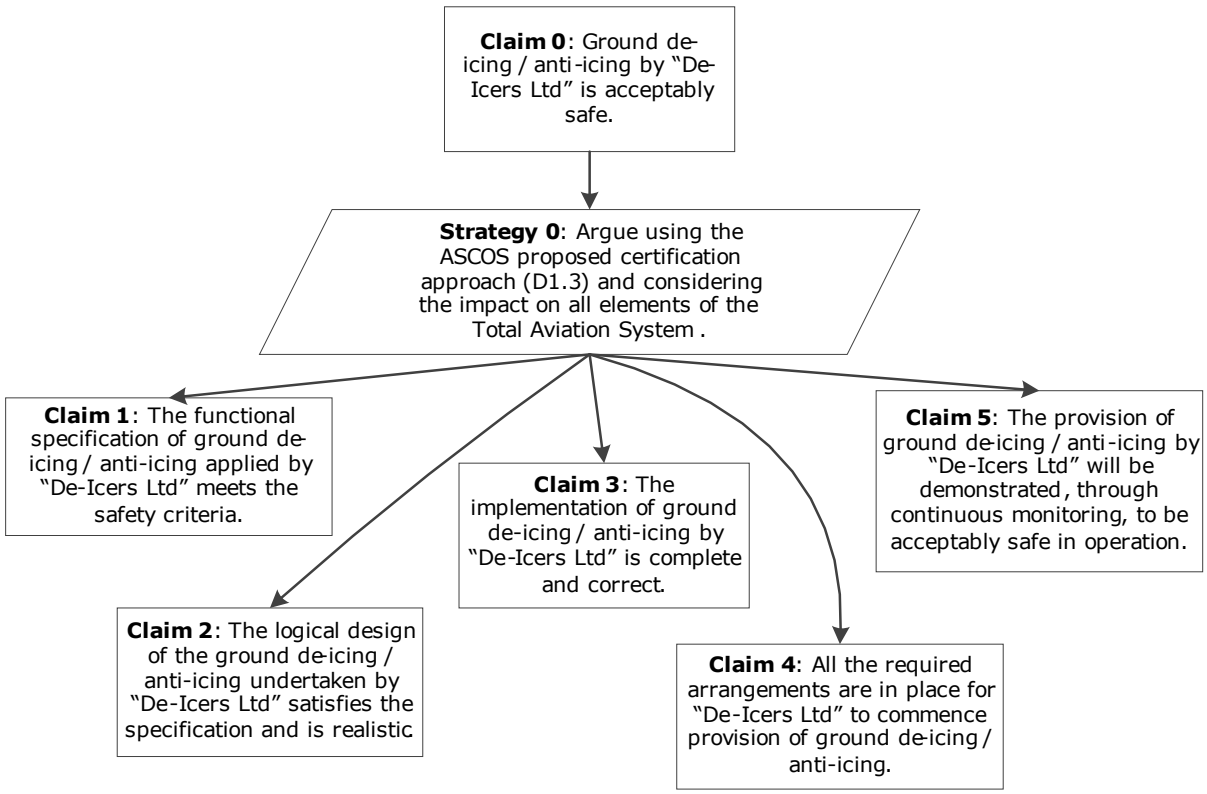


Figure 3: Initial argument structure for the certification of a de-icing/anti-icing service provider

4.3 Development and agreement of the certification plan

Claim 0 is the top level safety claim that the ground de-/ anti-icing by the provider achieves an acceptable level of safety. Relevant context was provided as follows:

- C0-1 defines the scope of operations to be provided by the service provider, in terms of the airports at which they operate, the air operators who they serve and the aircraft types for which they provide a service.
- C0-2 interprets "acceptable safety". The service provider is required to make a safety assessment for risks for which it has a 'view of safety'. For other risks it will also need to provide assurance that it delivers a required level of service. For both, it is assumed to be sufficient to provide evidence that the safety performance does not decrease.
-

The main strategy to provide evidence for this claim was described as follows:

- *Strategy 0*: Argue that the provider achieves an acceptable level of safety, using the ASCOS proposed certification approach and considering the impact on all elements of the TAS.

In this stage it is of importance that agreement is reached over the context elements, and the strategy to be followed. Accordingly:

- The required level of safety will need to be agreed upon. This could include considering the current level of safety combined with the required improvement as defined by EASA in their Safety Plan. In this case, it has been assumed that the current level of safety and level of quality are required levels.
- Agreement is reached over the conditions in which the service provider takes action. These are not crisply defined; the likely requirement is that the service provider must take action based on the inspection of aircraft if the conditions are "conducive to ice accretion". This philosophy is not likely to change in the near future. There have been attempts to design systems that can measure ice accretion on aircraft services, but these have not been found acceptably reliable yet.
- Agreement is reached over the main requirements and acceptable means of compliance. By complying with those requirements, the applicant shows compliance with the required safety level. This can also require that a check of whether the rules and standards are an adequate argument to satisfy the claims. It must also be checked whether the assumptions that are used between the domains are adequately addressed.

Claim 1 is that the ground de-icing / anti-icing function delivered by the de-icing/anti-icing service provider is specified to achieve an acceptable level of safety. This considers ground de-icing / anti-icing at a conceptual level, without considering how it is actually implemented. At this level there is no consideration of equipment or specific human roles – the function considered is the abstract function of de-icing and anti-icing of an airplane on the ground. The means of compliance argument for Claim 1 is summarised in the following strategy:

- *Strategy 1:* Argue that the specification as defined by the regulations is sufficient to meet the safety criteria and any specific variations required for the provider's operation have been fully assessed.

The main assessment to support Claim 1 will be an assessment of the operations at a conceptual level, using a technique that assesses the process of ground de- anti icing operations and establishes safety objectives for those operations. This is likely to be a relative assessment, which compares the operations with current operations, and assesses the associated change in level of safety. This strategy is further detailed using more detailed claims and compliance arguments below under a separate header.

Claim 2 is that the logical design of the ground de-icing / anti-icing operations as provided by the de-icing/anti-icing service provider satisfies the specification which was defined in support of Claim 1 and is realistically achievable. At this level the actors implementing the provision and the interfaces between them are identified, along with the interfaces with the other elements of the TAS (including the aircraft operator, the other ground staff at the aerodrome and the aircraft manufacturer). This will require an assessment that includes these interfaces and the interactions needed to ensure the safety of the ground de-icing / anti-icing operations. The associated means of compliance argument could include:

- A main assessment of a logical model of the operations and the establishment of requirements. This model needs also to take into account all the assumptions that are coming from the other domains, in line with element CO-1. It will be argued that the techniques currently used are effective.

Claim 3 is that the implementation of ground de-icing / anti-icing operations by the de-icing/anti-icing service provider is complete and correct. At this stage the actual equipment, procedures and staffing used to implement the provision of ground de-icing / anti-icing are defined. For the associated means of compliance argument this could mean:

- The applicant will show that the actual procedures documented and used by the applicant fulfil the requirements as derived in Claim 2.
- The applicant must show that all the assumptions as coming from other domains are still fulfilled.

Claim 4 is that all the required arrangements are in place for the de-icing/anti-icing service provider to commence provision of ground de-icing / anti-icing. The associated means of compliance argument could include evidence that:

- The equipment has been procured and tested, any required spares are available and arrangements are in place to ensure suitable maintenance of the equipment.
- Suitably qualified staff has been recruited.
- Staff has been trained in the procedures.
- Any arrangements for interfacing with other organisations (e.g., ground operations, air operator) are in place and any affected staff (e.g., pilots) have been suitably briefed.
- The transition between the old and the new process is properly documented and organized. Where appropriate, fall back or reversion procedures are in place.

Claim 5 is that ongoing operations demonstrate an acceptable level of safety. The associated means of compliance argument could include:

- Continuous safety monitoring to collect appropriate metrics to confirm the results of the safety assessments undertaken under earlier claims.
- Reporting and investigating any safety-related incidents and making any changes required as a consequence of the investigations.
- Maintaining staff competence (e.g. through refresher training).
- Maintaining equipment.
- Assessing any subsequent changes to the operation.

4.4 Specification

A total of 63 hazards were identified for the de-icing/anti-icing operation. To mitigate these hazards, the following high level safety requirements were derived:

HSR1. The need for ground de-icing and anti-icing shall be determined, taking into account the expected weather conditions and holdover time.

HSR2. If there is a need, ground de-icing and anti-icing shall be performed.

HSR3. After ground de-icing/anti-icing, a post de-icing / anti-icing check shall be performed.

HSR4. After ground de-icing/anti-icing, the aircraft shall be checked for contamination as part of the pre-take-off check.

HSR5. The de-icing/anti-icing operation shall satisfy the selected target level(s) of safety.

HSR6. The de-icing/anti-icing service provider shall have an SMS.

HSR7. The high level safety requirements 106 shall apply to all identified scenarios (normal conditions/poor weather conditions; de-icing at the gate/de-icing at a remote location)

HSR8. The probability that ice adversely affects the performance or controllability of an aircraft in take-off in such a way that it ends up in a loss of control or rejected take-off with catastrophic consequences shall not be higher than in current operations.

4.5 Design

Stage 5 of the certification process could not be completed because from the available guidance material it was not fully clear how this step should be interpreted when the topic of certification is an organisation.

5 Case study 4: Certification of an Integrated Surveillance System

5.1 Description of the change

This case study considers consider the deployment of an ISS over Frankfurt PAM area (slightly greater than the TMA). This system shall be in charge of all the ATC Surveillance functions as the primary mean of surveillance. Its aim is also to progressively replace (by attrition) all current PSR and SSR of the area. In the case of SSR, a possible conclusion of the system deployment maybe that after the attrition period coverage with SSR shall still be kept as a secondary mean of surveillance. The system is constituted of:

→ *Cooperative Surveillance with distributed independent Wide Area Multilateration (WAM) and aircraft dependant ADS-B.*

→ *Independent Non-Cooperative Surveillance (INCS) constituted of a network of "small" Multi-Static Primary Surveillance Radar able to mitigate failures of the Cooperative Surveillance systems.*

Both systems are fully independent in term of resources (HW&SW) but are also dissymmetric in principle of operation. From the previous situation they shall provide in term of Operational Improvements the benefit of: SESAR CM-0801 Ground Based Safety Nets for TMA and En Route. ISS shall trig changes as follow:

→ Increases choice of surveillance techniques for ground surveillance.

- Down to the ground surveillance, coverage shaped to the needs,
- Higher update rate (>1s instead of 5s) with an accuracy shaped to the needs,
- Precision Runway Monitoring (PRM) 2 parallel runways separated by only 600 m,
- *Surveillance systems providing coverage tailored to specific volumes of airspace (rather than coverage over 360 degrees out to maximum range) with a user defined, at installation, performances in the volume.*
- *Multi rather than Mono-Static deployments (ADS-B, WAM and INCS-MSPSR).*
- *Obsolescence management of old/ existing technology at reduced cost.*

→ Better spectrum management and reduced band needs.

The envisioned time frame is at near term (~2020) with an extension of the system to a wider area in 2020 - 2030.

5.2 Definition of the certification argument

Figure 4 provides the high level initial certification argument structure.

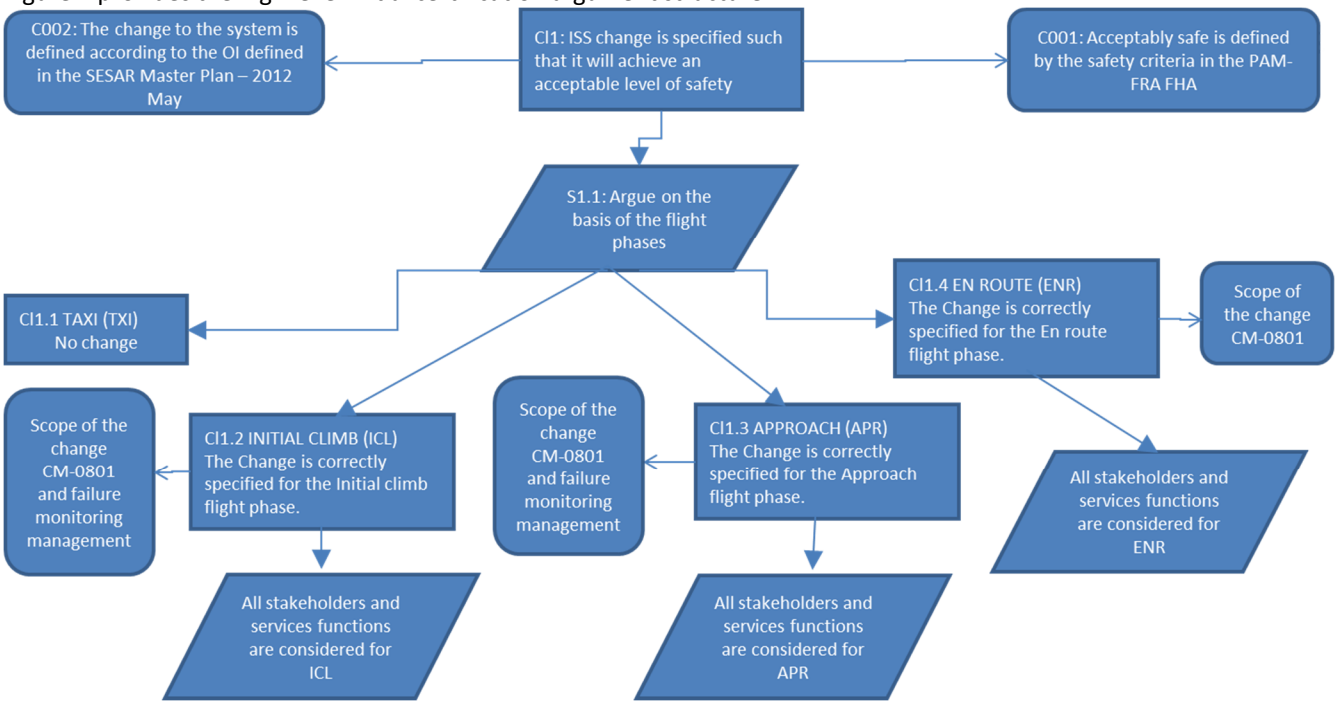


Figure $: ISS certification argument structure

5.3 Development and agreement of the certification plan

The ASCOS D1.3 approach proposes to structure the demonstration of safety by building upon the approach of the initial argument architecture as per stage 2, suggesting a top-level safety claim (Claim 0) that could be of the form:

Claim 0 : The operation of an ISS achieves acceptable safety across the whole TAS

and then cascading this higher level claim in sub-claims.

Besides, and as part of their overall duty of protecting the public in general and the environment, the authorities of the aviation system continuously develop common safety and environmental rules. These rules are usually formulated as a structured argument of safety requirements. Especially in the ATM domain, the one of ISS, the argument is more formulated as a performance requirement than as a defined means of compliance.

As a consequence, it must be checked whether the current rules and standards are an adequate argument to satisfy the claims. It must also be checked whether the assumptions that are used between the domains are adequately addressed.

Means of compliance argument for Claim 0:

- It will be shown by testing that the ISS fulfils its performance requirements (probability of detection, accuracy …). These tests shall be demonstration and measures of these performances parameters during the deployment phase when ISS is still monitored by the legacy systems SSR/PSR.
  The demonstration shall be completed by extrapolation using simulation tools and dedicated flight tests in the areas that the tools identified as safety critical. (CO-1)
- The required level of safety will be defined by the current level of safety combined with the required improvement as defined by the SESAR Master Plan.
- It would be logical to use the current certification methods that are used in the different domains and focus for ASCOS on the combination of these. This would enable the application of the new certification method (as in D1.3) on this level. If there is then a problem detected with the fusion of these domains, a further investigation on the applicability in a particular domain can be made. This will then require a much more detailed description of the impact in that domain. (CO-2)
- The current standards and practices are designed based also on previous accidents and incidents. All the knowledge and experience from these accidents and incidents is condensed in these standards and practices and therefore it is advised to use these in order to comply with CO-3. If the way of working will be different from the current standard, the applicant will argue the level of safety to the Authority by means of established techniques (e.g. FHA / PSSA / HF evaluations etc.)

5.4 Specification

Hazards that have already been identified for WAM used, supplemented with two new hazards:

- Increased update rate and accuracy of the tracks could generate undue confidence in the system from ATCO that will lead to procedural omissions.
- New areas controlled, especially at low altitude in the approach and departure area, are identified as a new hazard as current procedures were not defined for the management of such areas. In particular liaison with aircraft crew has to be cautiously defined.

6 Evaluation of the case studies

This chapter describes the evaluation of the four case studies that are described in chapter 2-5. The evaluation focussed on the initial proposed ASCOS certification approach described in ASCOS D1.3, the continuous safety monitoring process and tool, the tool for safety risk assessment, and the Area of Change (AoC) list from the Future Aviation Safety Team (FAST).

The evaluation is based on an analysis from three angles. Firstly, the application of the certification approach and tools, the experienced benefits, lessons learned, conclusions and recommendations from the four case studies were analysed at an aggregate level to formulate conclusions and recommendations regarding the ASCOS certification approach and supporting tools. Secondly, the four case studies were reviewed against the performance framework that defines Key Performance Areas (KPAs) for the ASCOS approach to evaluate the 'fitness for purpose' of the certification approach. Thirdly, the case studies were reviewed from a 'verification perspective' against a set of 'design' principles that was considered in the development of the certification approach. The aim was to evaluate the efficacy of the ASCOS approach and how it could be improved, rather than as a scoring mechanism for the quality of the case studies.

6.1 The initial proposed ASCOS certification approach

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

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

The set-up of the logical argument structure can provide the certification basis in a performance based regulatory framework. However, the set-up of the argument structure itself can be a complex and laborious task, especially for novices. Application of a logical argument framework requires appropriate guidance material, which is not yet sufficiently available. In a performance based regulatory framework the argument structure may be worth the effort. However, it is questionable if this benefit will materialize for a practical case

and if it is worth the additional effort, especially in the context of a compliance based regulatory framework and/or in a domain such as aircraft system certification which applies well developed certification practices.

Sixteen recommendations are made to ASCOS concerning mainly the improvement of guidance material on the application of the certification approach. Two recommendations are made to the EC and EASA about safety target setting for the TAS and its distribution across domains, and the acceptability of the TAS level risk and net safety effect of the introduction of a change in the TAS.

6.2 The tool for continuous safety monitoring

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

6.3 The tool for safety risk assessment

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

6.4 The FAST AoC list

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

recommendations to FAST are made to improve the application of the FAST AoC list as part of the ASCOS certification approach stages.

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

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

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

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

7 Conclusions and recommendations

7.1 Conclusions

This study describes the activities and results for ASCOS WP4 'certification case studies'. The objective of this WP is to apply the new certification approach and supporting tools in four case studies to evaluate the practical application of the proposed certification process adaptations. The four cases were the following:

- Certification of an Autonomous System Failure Management System for RPAS
- Certification of an Automatic Aircraft Recovery System
- Certification of a de-icing/anti-icing service provider
- Certification of an Integrated Surveillance System.

Each of these cases attempted to apply stages 1 to 5 of the initial proposed ASCOS certification approach (as described in ASCOS D1.3 [1]), which is being updated following constructive feedback and comments.

The case studies have then been evaluated from three angles: Firstly, the application of the certification approach and tools, the experienced benefits, lessons learned, conclusions and recommendations from the four case studies have been analysed at an aggregate level to formulate conclusions and recommendations regarding the ASCOS certification approach and supporting tools. Secondly, the four case studies have been reviewed against the performance framework that defines Key Performance Areas (KPAs) for the ASCOS approach to evaluate the 'fitness for purpose' of the certification approach. Thirdly, the case studies have been reviewed from a 'verification perspective' against a set of 'design' principles that was considered in the development of the certification approach. The aim was to evaluate the efficacy of the ASCOS approach and how it could be improved, rather than as a scoring mechanism for the quality of the case studies.

7.2 Recommendations

The recommendations resulting from the evaluation of the case studies are listed below.

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

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

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

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

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

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

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

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

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

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

- How the logical argument structure should include the roles and responsibilities of different certifying authorities and stakeholders.

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

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

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

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

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

Recommendation 13: It is recommended to ASCOS that the description in D1.3 is updated to reflect the characteristics of the FHA. The added value of stages 4 and 5 would be increased if the approach is not focussed on mitigation of failure conditions or hazards, but also on achieving a certain performance level by the intended function and its design.
Recommendation 14: It is recommended to ASCOS to define 'hazard' in guidance material using the wide definition of hazard, i.e. "any condition, event, or circumstance, which could introduce an accident" (refer to the ICAO Safety Management Manual).

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

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

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

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

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

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

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

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

- Stage 1 (Definition of the change)
  The tool can be used to derive the current safety performance in areas that are relevant for the change. As a result the applicant is made aware of the actual safety performance in the TAS in the domain(s) of interest. These data may be used to define the current risk level as a basis for safety target setting as part of the argument structure that defines the applicable safety criteria in stage 2. It may also be used to assess the potential safety impact of the change in the TAS.
- Stage 2 (Define the certification argument) and stage 3 (Development of certification plan)
  In the development of Claim 5, "The service(s) introduced by change X will continue to be demonstrated as acceptably safe in operational service", the tool and supporting SPI framework can be used to define the SPIs that need to be monitored to ensure continuous monitoring and feedback on the safety performance of the approved "change" or certification case.
- Stage 4 (Specification) and stage 5 (Design)

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

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

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

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

- How exactly can the safety risk assessment tool assist in identifying Design Safety Requirements, specifically considering that the events and faults in the risk model are generally at a different level than the logical elements at which the Design Safety Requirements need to be identified?

- It is unclear to what level the ESDs and Fault Trees need to be decomposed to assess how the various stakeholders work together to satisfy the high level safety requirements.

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

- Stage 1 (Definition of the change)
  The tool can be used to derive the current risk picture for the TAS, including different domains and stakeholders. As a result the applicant is made aware of the actual risks or safety performance in the TAS in the domain(s) of interest. These data can be used to assess the potential safety impact of the change in the TAS and to define the current risk level as a basis for safety target setting as part of the argument structure that defines the applicable safety criteria in stage 2. The ASCOS guidance material should explain how the tool for safety risk assessment can be used as part of stage 1 and explain its value and difference compared with the tool for continuous safety monitoring.
- Stage 2 (Define the certification argument)
  The tool can be used to derive and allocate safety objective/requirements as explained in section 4.3.3. The ASCOS guidance material should include a process to ensure that the tool reflects correctly the operational environment and scenarios if it is to be used by multiple stakeholders for safety objective allocation. In addition, guidance material should explain what process to follow for the allocation of safety requirements to human factors (events related to human performance).
- Stage 4 (Specification)
  When the topic of certification is a technical system, stage 4 includes a FHA where the hazards are 'driven by' the functional design. In these cases the tool cannot properly provide a functional hazard identification and assessment.
- Stage 5 (Design)
  The tool can support stage 5 when a PSSA is conducted. The ASCOS risk model and tool can be used as an overall safety assessment model/tool for the TAS, integrating 'local', case specific risk models from different domains or stakeholders (provided that these models use similar modelling techniques). Although the Fault Trees are not yet developed to the level of detail that is immediately useful for application in a certification case, the tool is flexible so that the safety practitioner can update, modify and expand the risk model (ESDs and Fault Trees) as required.

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

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

(stage 5). In stage 1 the first step would be to identify all relevant AoCs and to determine which AoCs should be considered for the subject of certification in the short term and which AoCs may become relevant for the subject of certification in the long term. During the specification and design, and possibly in the safety assessment prior to a change, only the AoCs of significant importance could be considered. 'Significant importance' could be determined for example by the degree of the effect of the AoC on the certification case or the time horizon in which the AoC may impact the certification case. An AoC that will occur in the short term needs to be addressed more urgently in the specification and design stages than a long term AoC. Addressing long term AoCs can be undertaken by Safety Management Systems (SMS) and continuous safety monitoring processes in due course.

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

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

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

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

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

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

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

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

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

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

References

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

Appendix A ASCOS certification approach

Appendix A.1 Overview of approach

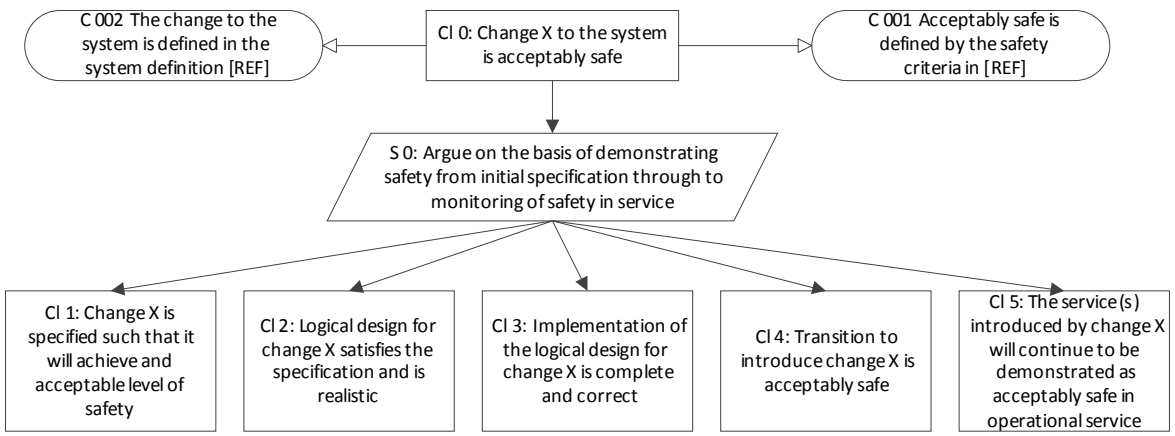
The new ASCOS approach is to use a logical argument for the certification of any changes to the Total Aviation System (TAS), and support the top level claim that the change is acceptably safe. The argument is then broken down into supporting claims, each addressing a smaller portion of the top level claim.

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

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

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

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



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

Appendix A.2 Stages of the approach

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

1. Define the change – Ensure the proposed change to the TAS is fully understood.
2. Define the certification argument (architecture) – development of initial certification argument; top level claim and context.
3. Develop and agree certification plan – Present the certification philosophy to the acceptance authority (ies) and obtain agreement to proposed approach.
4. Specification – Demonstration that claim 1 is met by the change, namely that the change is specified to achieve an acceptable level of safety.
5. Design – Show the logical design for the change satisfies the specification derived within claim 1 thus satisfying claim 2.
6. Refinement of argument – This is a continuous process through all stages of the approach.
7. Implementation – Demonstration that claim 3 is met by the completion and correctness of the physical implementation of the logical design for the change.
8. Transfer into operation: transition safety assessment – Show that the transition to introduce the change is acceptably safe.
9. Define arrangements for continuous safety monitoring.
10. Obtain initial operational certification – Presentation of evidence to authorities in order to introduce change into service.
11. Ongoing monitoring and maintenance of certification

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

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

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

Stage 1 – Define the change

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

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

- Definition of the overall goal of the change;
- Identification of the change to be made, including:
    - Which organisation is proposing the change;
    - Which organisations are affected/involved in the change, and what their role is;
    - The functional and operational concept of the change;
    - Definition of the timescales for actual implementation;
    - Identification of which elements of the system are affected by the change (e.g. process, products, roles, domains);
- Identification of which requirements (safety and non-safety) need to be fulfilled by the change;
- Creation of a high level architecture, and identification of assurance contracts;
- Identification and consideration of any expected TAS Areas of Change (AoC)[4];
- Determining what existing regulations, certification specifications, standards, AMCs or other relevant guidance material are applicable to the change;

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

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

Stage 2 – Define the certification argument (architecture):

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

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

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

Stage 3 – Develop and agree certification plan:

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

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

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

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

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

Appendix A.4 Benefits of the approach

The approach has the following benefits:

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

Appendix A.5 Ownership of the argument

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