Definition and evaluation of innovative certification approaches

U. Dees (NLR), P. van der Geest (NLR), A. Simpson (EBENI), S. Bull (EBENI), P. Blagden (CAAi), T. Longhurst (CAA), A. Eaton (CAA), G. Temme (CertiFlyer), B. Pauly (TR6)

This study identifies, consolidates, and evaluates potential new options for certification process adaptations in the total aviation system. The most promising candidate process adaptation options are selected, and recommendations for further elaboration in follow-up ASCOS activities are given.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	B. Pauly (TR6)

Grant Agreement No.	314299
Document Identification	D1.2
Status	Approved
Version	1.4
Date of Issue	15-09-2015
Classification	Public

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	U.G. Dees et al.	15-07-2013	All	Version for approval by PMT
1.1	L.J.P. Speijker	02-08-2013	-	Incorporated PMT comments
1.2	L.J.P. Speijker	20-08-2013	1, 4, 5	Incorporated SESAR JU comments
1.3	L.J.P. Speijker	20-08-2013	2.3, 3.3	Incorporated EASA comments
1.4	L.J.P. Speijker	15-09-2015		Made publicly available

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
CAAi	S. Long	13-07-2013
CertiFlyer	M. Heiligers	15-07-2013
Ebeni	J. Denness	13-07-2013
TUD	R. Curran, H. Udluft, P.C. Roling	13-07-2013
Institute of Aviation	K. Piwek, A. Iwaniuk	13-07-2013
NLR	A. Roelen, J. Scholte, L.J.P. Speijker	02-08-2013
Avanssa	N. Aghdassi	02-08-2013
APSYS	V. Bonvino, J.P. Heckmann	02-08-2013
ISDEFE	I. Etxebarria, M.M. Sanchez	02-08-2013
Organisation Responsible for Approval	Name of person approving the document	Date
TR6	B. Pauly	15-07-2013
NLR	U.G. Dees	15-07-2013
NLR	L.J.P. Speijker	22-08-2013

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Document Distribution

Organisation	Names
European Commission	M. Kyriakopoulos, S. Grand-Perret
NLR	L. Speijker, A. Rutten, U. Dees, P. van der Geest, M.A. Piers, A. Roelen
Thales Air Systems GmbH	G. Schichtel, J.-M. Kraus
Thales Air Systems SA	B. Pauly
EADS APSYS	V. Bonvino, J.P. Heckmann, M. Feuvrier
Civil Aviation Authority UK	S. Long, A. Eaton, T. Longhurst
ISDEFE	M. Martin Sanchez, I. Etxebarria
CertiFlyer	G. Temme, M. Heiligers
Avanssa	N. Aghdassi
Ebeni	A. Simpson, J. Denness, S. Bull
Deep Blue	L. Save
JRC	W. Post, R. Menzel
JPM	J. P. Magny
TU Delft	R. Curran, H. Udluft, P.C. Roling
Institute of Aviation	K. Piwek, A. Iwaniuk
CAO	P. Michalak
EASA	K. Engelstad, J. Vincent, R. Priego, M. van Hijum, R. Powel, E. Isambert, P. Mattei, C. Audard, M. Masson, C. Gandolfi, S. Haya Leiva, H. Pruis, A. Florin, E. Duvivier, S. Fabbrini, P. Pantazopoulou, J.B. Marciacq, D. Haddon, B. Jolly, E. Radev, J. Penny, M. Kompare, M. Romano
FAA	J. Lapointe, T. Tessitore
SESAR JU	P. Mana
Eurocontrol	E. Perrin
CAA Netherlands	R. van de Boom, R. van de Leijgraaf
IATA	D. Reisinger
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
SAE S-18	J. Dalton

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Acronyms

Acronym	Definition
ADR	Air Data Reference
AIM	Accident Incident Model
AMC	Acceptable Means of Compliance
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AOC	Air Operator Certificate
ASCOS	Aviation Safety and Certification of new Operations and Systems
ATM	Air Traffic Management
ATS	Air Traffic Services
CAA	Civil Aviation Authority (Competent Authority)
CAP	CAA Publication
CATS	Causal model for Air Transport Safety
CBA	Cost Benefit Analysis
CENELEC	European Committee for Electrotechnical Standardization
CMM	Capability Maturity Model
CMMI	Capability Maturity Model integration
COTS	Commercial Off The Shelve
CS	Community Specification; Certification Standards
DoC	Declaration of Conformity
DOD	Department of Defence
DSU	Declaration of Suitability for Use
EASA	European Aviation Safety Agency
EATMP	European Air Traffic Management Programme
EC	European Commission
ETSI	European Telecommunications Standards Institute
ESARR	EUROCONTROL Safety Regulatory Requirement
EU	European Union
FAA	Federal Aviation Authority
FAST	Future Aviation Safety Team

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

GSN	Goal Structuring Notation
HF	Human Factors
ICAO	International Civil Aviation Authority
ICMM	Integrated Capability Maturity Model
i.l.o.	In lieu of
ISO	International Organisation for Standardisation
NSA	National Supervisory Authority
PANS	Procedures for Air Navigation Services
POC	Proof of Concept
R&D	Research and Development
SAM	Safety Assessment Methodology (EUROCONTROL)
SAME	Safety Assessment Made Easier
SARPs	Standards and Recommended Practices (ICAO)
SES	Single European Sky
SESAR	Single European Sky ATM Research
SESAR SRM	Single European Sky ATM Research Safety Reference Material
SMS	Safety Management System
SOPs	Specific Operating Provisions (Operations Specifications)
SOS	System of Systems
SW	Software
SWALs	Software Assurance Levels
TAS	Total Aviation System
TMA	Terminal Manoeuvring Area
TRL	Technology Readiness Levels

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Executive Summary

To ease the efficient and safe introduction of safety enhancement systems and operations, a novel and innovative approach towards certification is felt to be required that:

- Is more flexible with regard to the introduction of new products and operations;
- Is more efficient, in terms of cost and time, than the current certification processes; and
- Considers the impact on safety of all elements of the aviation system and the entire system life-cycle in a complete and integrated way.

In view of this, this study has examined current certification practices and identified potential improvements from the viewpoints of several aviation domains. Next, these potential improvements have been consolidated into eight approaches that can apply to the Total Aviation System, as follows:

1. Integrate all domains within the authority
2. Change between performance based and compliance based
3. Abolish all certification by authorities and transform into voluntary compliance
4. Make more use of competent (certified) entities
5. Certify the applicants instead of their products
6. Use of Proof of Concept approach
7. Enforce existing rules and improve existing processes
8. Cross-domain fertilisation

These eight options have been further reviewed against a set of 15 evaluation criteria, but with an emphasis on safety and cost benefit. Other criteria used include throughput time, stimulation of innovation, required expertise, bureaucracy, interoperability between domains, harmonisation and standardisation, acceptable means of compliance definition, level of difference with current requirements, ability to use retroactively, human factor involvement, new process more performance based or compliance based, possibility to delegate responsibility, and feasibility. The initial review of the impact of these approaches suggests that options 2, 6, 7 and 8 provide the most promise for achieving the aims of ASCOS with regards to enhancing certification approaches.

Different certification process adaptations have been defined, analysed, and evaluated. However, it should be realized that there are other potential options for change that could be defined. For example, focusing more explicitly on the introduction of connections (bridges) between different domains, where such connections are needed, and/or combination of product and organization certification (the latter is now indirectly covered in options 2 and 8). Also, it should be realized that more (or different) evaluation criteria exist and could have been used, such as constraints relating to public responsibility. Also, it should be noted that future advancements in technology could pose new challenges on existing certification. For example, the more automation is used, the less experience is gained by the flight crew which would be needed when manual take-over is necessary. Therefore, use of an additional criterion that explicitly deals with future and emerging risks could be beneficial.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

This report only provides an initial view of the potential for improving the regulatory framework and supporting certification processes. It has deliberately taken a more "blue-sky" approach to looking for improvements. However, moving forward it is recognised that to achieve the aims of ASCOS any future certification adaptations must take the following into account:

- Ensure that there will be a reliable process to ensure that assumptions made in the design and certification safety assessments are valid with respect to operations and maintenance activities;
- Avoid unnecessary change, recognising the good approaches already in place;
- Provide a generic certification framework encompassing the Total Aviation System (TAS);
- Use a common language across all domains based on safety argument concepts (e.g. argument-based as used in OPENCOSS), allowing flexibility to accommodate a variety of approaches across domains;
- Provide rigorous management of interfaces, both between domains and between the TAS and its environment, to ensure that all key safety issues are properly addressed and not lost at interfaces;
- Allow, within each domain, the new certification approach to evolve from the current approach by
    - keeping the existing approach where no change is required
    - learning lessons from other domains where this gives improvement
    - ensuring that bottlenecks and shortcomings are addressed by the proposed approach;
- Promote flexibility within each domain to allow introduction of new technologies or procedures
- Harmonise approaches between domains where this is advantageous or necessary
- Simplify certification processes, where there are:
    - demonstrable benefits and
    - no loss of confidence in the assurance of safety;
- Reinforce existing techniques where they are appropriate but not consistently applied;
- Provide a mechanism for identification and resolution of further bottlenecks and shortcomings;
- Introduce a bridge between regulations for different domains (e.g. between aircraft certification and Air Traffic Management or between product certification, maintenance certification and operational certification) in order to advance throughput time of certification without loss of safety items;
- Take more explicit account of electronic hardware in the proposed approach;
- Consider the fact that less experience is gained by the flight crew when more automation is used;
- Consider the balance between product and organization certification and allow flexibility between the two dependent on criticality, complexity and maturity (of both product and organisation);
- Consider the whole system lifecycle, in particular considering:
    - whether the certification process can usefully be initiated earlier in the lifecycle;
    - how to ensure that certification remains valid throughout in-service life, taking into account changes in the wider system during that lifetime.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Table of Contents

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

List of Figures

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

List of Tables

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

1 Introduction

1.1 Background and scope

The need for improvement of existing certification processes already became clear after the publication of the FAA Commercial Airplane Certification Process Study [1]. According to the conclusions of the report, there is no reliable process to ensure that assumptions made in the design and certification safety assessments are valid with respect to operations and maintenance activities and, furthermore, to ensure that human operators are aware of these assumptions when developing their operations and maintenance procedures. It became clear that aircraft certification standards may not reflect the actual operating environment. Other studies, as well as the findings of various accident investigations, confirm the shortcomings in the existing certification processes as identified in the FAA study [1]. Also, current certification processes may take a long time, or can even turn out to be not reasonably feasible. To ease the efficient and safe introduction of safety enhancement systems and operations, a novel and innovative approach towards certification is required that:

- Is more flexible with regard to the introduction of new products and operations;
- Is more efficient, in terms of cost and time, than the current certification processes; and
- Considers the impact on safety of all elements of the aviation system and the entire system life-cycle in a complete and integrated way.

The aviation system can be regarded as a large system composed of many elements. Safety depends on the elements and on the interfaces between the elements, all of which must be considered during certification because the weakest link in the chain determines aviation safety. ASCOS D1.1 [35] identified several shortcomings and bottlenecks in the certification process. In addition to these, further needs for adaptations of the certification process are emerging from developments in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance.

Currently, certification based on prescriptive regulations is primarily used in aircraft certification. In this case solutions must comply with detailed regulations which prescribe parts of the implementation. These effectively are a collective memory based on past experience, and are a very effective way to gradually improve safety. However they may be less suited for the introduction of new concepts and technologies that might not be fully compliant with existing prescriptive regulations, but which could be just as safe or safer. The determination of a certification basis and demonstrating compliance may then take a long time. In view of the weak spots identified in the existing certification processes as well as the major regulatory and technological changes currently taking place, novel certification approaches are called for to maintain and improve the affordability of certification processes – both in cost and in duration, to reduce the uncertainties involved, and to make a significant step forward in safety. There is therefore a need to define, evaluate, and select new potential improvements to the existing certification processes and – where necessary – develop and provide supporting safety driven design methods and tools to ease the certification of safety enhancements systems.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

The scope of this study includes the total aviation system. Potential certification adaptations in the following domains are addressed and discussed: air operator certification, aircraft/product certification, Air Traffic Management (ATM), and airports. In line with the main objective of the ASCOS project, the main focus is on cost benefits (e.g. moving towards a reduction of the costs of equipment certification) and safety benefits. It is recognized that in the future, certification may – besides safety – also consider additional areas, e.g. security and/or economics. However, the latter issues are outside the scope of ASCOS. It is envisaged to contribute to reaching the ACARE Vision 2020 safety goals. Therefore, time frame (specifying how far ASCOS looks into the future) for actual introduction of proposed certification adaptations is 2015 - 2020. However, preferably the proposed certification adaptations should provide benefits for the time frame up to 2050 as well, keeping in mind the specific goals regarding certification processes as listed in Flightpath 2050 Europe Vision for Aviation.

1.2 Objectives

The main objective is to define and evaluate multiple new approaches to certification. Specific objectives are:

- To identify new certification approaches from the perspectives of the different aviation domains;
- To consolidate a set of new approaches with relevance for all the aviation domains;
- To evaluate the new approaches against a set of evaluation criteria;
- To select the most promising certification adaptations for further elaboration in follow-up tasks;
- To provide recommendations for application of the selected promising certification adaptations.

1.3 Approach

Multiple solutions to improve certification processes may exist, some of which involve approaches in which all safety certification aspects are dealt with in an integrated way from the early design phase of the life cycle towards decommissioning, and which cover the entire aviation system. Other approaches may have a narrower scope, and be targeting specific current certification challenges such as those involved with the treatment of human performance aspects in safety assessments and the differences in the approaches followed in ATM certification and aircraft (operations) certification. An issue that will be addressed is the increasing integration of the certification processes for a) ATM operational concepts and supporting systems and b) aeronautical products and flight operations. The certification concept for both differs significantly and this might be a cause for future un-clarities with potential safety implications.

In view of this, the study approach is as follows:

- The first step is the identification of new approaches to certification from the perspective of the different domains of aviation (e.g. aircraft operations, airworthiness, Air Traffic Management (ATM), and airport).
- Next, the identified approaches are consolidated into a set of new approaches that have relevance for *all* the aviation domains, and hence for the Total Aviation System that ASCOS aims to address.
- Then, this set of new approaches are evaluated against a set of evaluation criteria,
- Finally, the most promising approaches are selected for further elaboration in follow-up tasks in ASCOS.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

1.4 Structure of the document

This document consists of 5 Sections, including this introduction. In Section 2, new approaches are identified from the perspective of different aviation domains. In Section 3, the identified approaches are consolidated into a set of new approaches with relevance for all aviation domains. The evaluation of the new approaches, and the selection of the most promising certification adaptations, is described in Section 4. Finally, in Section 5, conclusions are drawn and recommendations provided.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2 New approaches

2.1 Introduction

In this Section 2, new and – where possible – innovative approaches to certification are identified from the perspective of the following different aviation domains: air operator certification (Section 2.2), aircraft/ product certification (Section 2.3), ATM (Section 2.4) and airports (Section 2.5). It is noted that some cross-fertilisation between these sections took place to stimulate the identification process.

In each of the subsections new approaches are identified using the same numbering. Accordingly, the same new approach may be called Option a in one subsection and Option b in another. Only in the next Section 3, a consolidation of these new approaches takes place.

2.2 Perspective of air operator certification

2.2.1 Introduction

In this paragraph, new and innovative certification approaches will be identified from the perspective of air operator certification. While considering new and innovative approaches, one should keep in mind the reason *why* prospective air operators are certified. The certification process is designed to ensure that prospective certificate holders understand and are capable of fulfilling their duty of providing air transportation with the highest degree of safety possible in the public interest. When satisfactorily completed, the certification process should ensure that the operator is able to comply with the applicable aviation law and regulations. An operator should not expect to be certificated until the Civil Aviation Authority (CAA) is assured that the [State's] aviation law and its Civil Aviation Regulations will be complied with in an appropriate and continuing manner. After a brief description of the current certification practice in paragraph 2.2.2 and the problems encountered today in paragraph 2.2.3 (described in more detail in D1.1), in paragraph 2.2.4 some new approaches will be provided.

2.2.2 Current practice

The way in which prospective air operators are certified differs from state to state. Therefore, to provide a general description of the air operator certification process, reference is made to the certification process the International Civil Aviation Organisation (ICAO) advises its member states to follow. In practice, many member states follow, in more or less detail, this process. Summarized, the Air Operator Certification process consists of 5 consecutive phases, which are presented in Figure 1 and next explained in short.

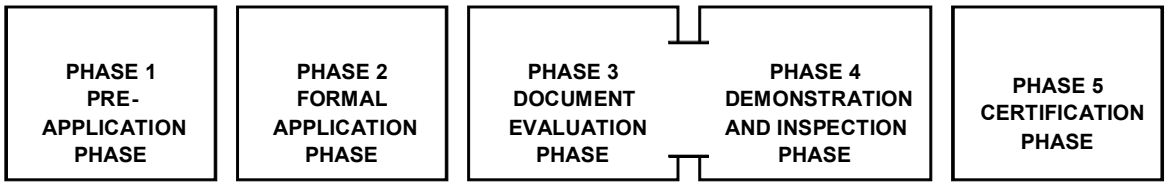

Figure 1 – Air operator certification process

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

(1) Pre-application phase

In the pre-application phase, an applicant seeking an Air Operator Certificate (AOC) makes the initial inquiry for application. Usually a meeting is held between the CAA and the applicant. Information needed to complete the application is provided.

(2) Formal application phase

In the formal application phase, the prospective operator's formal application is (initially cursory) reviewed by the CAA and a formal application meeting is conducted with the prospective operator to discuss its application. The formal application consists of a formal application letter together with necessary attachments like draft specific operating provisions (SOPs), certification job aid & schedule of events, company general manuals (operations manual, maintenance control manual), training and checking manuals, management structure and qualification, statement of compliance, etc. Critical to the success of the entire certification process is a thorough understanding of pertinent regulations and advisory materials. The operator and key management personnel must understand which regulations apply to their intended operation.
The formal application should be submitted at least 90 days before revenue operations are expected to begin.

(3) Document evaluation phase

In the document evaluation phase the CAA performs an in-depth review of the application and all required attachments as mentioned under (2). The in-depth review is necessary to ensure that the applicant's documents and manuals meet all CAA standards and requirements.

(4) Demonstration and inspection phase

In the demonstration and inspection phase, the applicant demonstrates its operation to the CAA in accordance with applicable regulations and as it was defined in the applicant's documents and manuals that the CAA evaluated during the document evaluation phase. Further, the applicant's facilities are inspected and evaluated against the applicant's documents and manuals as well.

(5) Certification phase

The certification phase is the final phase of the certification process. All certification findings are reviewed and when the CAA is convinced that the prospective operator is in compliance and will be able to be in continued compliance, the certificate and specific operating provisions are issued to the operator. The operator now has CAA approval to operate under the conditions that the SOPs dictate.

2.2.3 Bottlenecks in the current practice

There are a few bottlenecks in the current air operator certification practice. The main issue is that it is time consuming and therefore expensive, both for the Authority and applicant. As a result, there is a strong tendency within CAAs to reduce the time spent on certification. Against the background of the process description provided in paragraph 2.2.2, it has been observed that especially the time spent on proper document evaluation and the number of demonstration flights being required has recently reducing.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Apart from the time and costs involved, there are some other bottlenecks as well. It is well known that applicants often do not have the required knowledge about the applicable regulatory requirements. Of course all applicants are able to read the regulations, but when it comes to really understand the reason why compliance is necessary in order to enhance safety, and how to translate the different regulations into the organisation's procedures, there is a battle to win. Are the (prospective) operators to blame, or is the way the regulatory framework is formulated too complicated? Do we need to make one step back, because we went too far in our efforts to assure safe air transport by means of additional and more complex regulations over and over again, or should operators be left with a bit more responsibility in how they want to assure a safe operation? One may tend to regulate more and more, and in more detail, while on the other hand oversight budgets are more and more limited. In the end, the added value of a regulatory structure is limited when there is no oversight, or when the knowledge and experience of the inspectors of the Authorities is lacking as well.

2.2.4 New approaches

In this paragraph some new approaches to air operator certification are provided. We start our description with two extreme approaches, one in which we don't change anything at all, and one in which we simply stop certifying new operators, resulting in a free market entry. The other approaches involve innovations to the current process.

Option a: Do not change anything.

Keep the certification process as it is and follow as much as possible the 5-phase certification approach described by ICAO. The air operator certification process followed today reflects many years of experience and knowledge development, and to come up with something (completely) new and innovative might neglect this knowledge. Moreover, the European Union is not an isolated area; aviation is a worldwide activity. Hence, it is an option to stay as close as reasonably possible to the advisory material developed by ICAO. In the end, all member states of the Union are member states of ICAO as well. However, in actually following the process described by ICAO, there is room for improvement. Because of budget constraints, it seems that in many states shortcuts are made nowadays in order to reduce time and costs involved. Following the ICAO process in more detail could result in a cost increase and a need for more, and possibly better, trained inspectors. The direct safety effect is on short term, like the effect of the opposite situation, hard to measure. However, in the end, safety will benefit from proper certification and supervision on continued compliance.

Option b: No certification at all.

The most extreme option is to refrain from any kind of certification. In the end, it is the responsibility of the (prospective) operator to be in compliance with the applicable regulations.

Option c: Voluntary certification.

It is up to the manufacturer, operator, etc. to participate in a certification process. There is no legal need to be certified. This will be left to the individual organisation. A comparison could be made with International Organisation for Standardisation (ISO) certification: not legally required, but many organisations want to be certified because of commercial reasons. Certification could be done by the competent authority or certified

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

entity, and it is up to the individual customer to choose for a certified company or not. The responsibility is left to the individual company and customer. This option deviates from the basic idea that governments have a certain responsibility to assure safe air transport, and involve requirements regarding communication of involved risks to passengers.

Option d: Extend the use of Certified Entities.

A variation of option a is option d, keep the processes as they are, but extend the use of certified entities. The competent authority can do the certification of those entities. The advantage is that the competent authority becomes more flexible: when there is a need for additional staff because of the amount of applicants in a certain year, the competent authority can make use of the services of a certified entity. In years in which less staff is required, less or no services will be hired. Attention should be paid to the knowledge level of both the competent authority and certified entity staff. Moreover, the costs related to the certification may remain unchanged for the applicant, since the process remains the same, or even rises, because of different involved actors. These elements will be discussed in greater depth in Section 4 when evaluating the different options.

Option e: Strengthen the existing certification process.

Also a variation of option a is option e. Keep the certification process as it is, focus on correct implementation in the different member states, and have a look at possible improvements *within* the process. One could think of a close review of the way demonstration flights should be executed and the minimum amount of that, the possibility of working with model procedures and manuals, more attention for management staff experience and background, and the extension of the availability of acceptable means of compliance. A huge advantage of the availability of acceptable means of compliance is that it provides additional information related to the requirements, it safes time (limits discussions about the interpretation of the requirements) and minimizes subjective assessments of individual inspectors.

Option f: Extend the use of delegated responsibilities.

As a last option, which is also a variation of option a, one could think of extending the responsibilities of individual air operators. Probably more use could be made of operators' own responsibility for safe air transport, and delegate more responsibilities to them like the delegation of instruction and examination of aircraft (and helicopter) type ratings.

2.3 Perspective of aircraft/product certification

Currently an aeronautical product is certified by the European Aviation Authority (EASA) based on Implementing Rule Part 21. More detailed requirements are published in different Certification Standards (CS, e.g. CS 25 [2] deals with transport aircraft, CS 27 deals with transport helicopters etc.). These requirements are further supplemented by "Acceptable Means of Compliance (AMC)", in which possible methods are published to show compliance with the CS. The CS are normally written in a prescriptive way.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Novel technology usually requires new rules when it is considered that the current requirements are insufficient to address this technology. These are called Special Conditions and need to be notified by EASA to Industry via a 3-month public comment period. This is still, however, a quicker process than convening a working group to redraft a CS, which may take several years. If additional AMC material is needed a comment period is not required. More than often this process still leads to a situation where there are no rules available to certify novel technology in time. Delays in the certification process are unavoidable, as the certificating authority needs time to formalize new rules against which the new technology can be evaluated.

This is one example that shows that the current practice needs a change. Another example could be the lack of coordination between domains. Based on personal experience of an aircraft/product certification expert, the problematic division between product certification and operational certification has caused unnecessary delays to get the product on the line with operators. The following will indicate what has been done up to now, what problems remain and what changes could be implemented to resolve these problems.

2.3.1 A changing world

In the last ten years the product certification practice has seen a major change. This is, amongst others, due to the following circumstances:

a) The products have become more integrated with each other and the complete aircraft
b) The products have become more complex by their own and in integrated combinations
c) The products are relying more and more on software
d) The products are required by more than one domain (Product, Operations, ATM etc.)
e) More emphasis on Human Factors due to the realisation that most accidents and incidents have a high HF content
f) Databases are used extensively with certification and operational implications

2.3.2 What has been done up to now?

Due to these changes in the Certification Outlook, the Product Certification community has adapted its working methods in the following way:

a) Establishing of inter-domain policies and regulations (e.g. the Operational Suitability Data, OSD, regulation between product certification and operational evaluation)
a) Stringent software certification requirements and certification of more equipment to higher standards (e.g. FMS software to level B)
b) Introduction of requirements that are focussed on aircraft level safety more than on equipment level safety (e.g. change of CS25.1309 [4])
c) New regulations with respect to Human Factor certification (e.g. CS25.1302 [3])
d) Possible retroactive applications of requirements (CS26 [5])

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.3.3 Did this solve all problems?

Despite all these changes to the certification practice there are still problems and inconsistencies that need attention in order to make the practice more efficient and at the same time enhance safety. The following problems have been identified in more than 30 years certification experience background as systems surveyer, flight test engineer and flight test pilot:

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

2.3.4 Alternatives

With these notions in mind this Section will try to identify in which way improvements could be identified. It is important, though, to realise, from the beginning, that drastic changes to the certification practice will most probably be unsuccessful. This is mainly due to two reasons:

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

Proposals that do not violate the remarks above will clearly have a better “score”. Despite of all arguments used above, it will be the content of this Section to propose changes to the current certification processes which will be rated later during the program on the level of being “promising”. Possible changes are described in the following.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Option a: Integrate all domains within the authority

After a product is certified and a Type Certificate is issued, the Operational Authorities will follow on with the operational certification against EU-OPS requirements [6]. Sometimes these requirements are not in line with the product requirements and a product change is needed, with all the cost involved. The Operational authority will have to familiarize again with the technology, leading to even further delays. Similar obstacles are identified between these domains and the ATM domain.

The aeronautical product should be certified with the whole lifecycle in mind. Standards and requirements must take this lifecycle into account in a balanced manner. It is useless to spend time and money on requirements resulting in overkill when compared to other applicable requirements.

In some cases during the product certification (e.g. for electronic flight bag / Required Navigation Performance standards / steep approach / head up display) more domains in the authority are involved (e.g., aircraft operation, aircraft systems, and ATM. This can lead to an unclear split of responsibility and the applicant may be squeezed between them.

All these are unwanted results of the rather rigid requirement structure that has developed over the years in a process that is harmonized between EASA and the Federal Aviation Authority (FAA). This in itself is a great achievement as it avoids duplication of work by the manufacturer if certification on both sides of the Atlantic is requested. Furthermore, most countries outside the EU and the US accept a Type Certificate issued by one of these two authorities.

The developments in ATM-programs as SESAR will undoubtedly introduce new Avionics. These Avionics will have to comply with Product certification requirements, Operational standards and ATM specifications. This would preferably be managed by an integrated authority. This notion could, among others, mean that the certification/standardization and specification methods need to be harmonized between the different domains.

The integration of all domains could be combined with all following proposed changes.

Option b: Change to "Performance based" i.l.o. "Compliance based"

Performance based refers to a top-level requirement that must be complied with (e.g. the safety level). Compliance based refers to the exact means of how to comply with a requirement. Change to performance based in lieu of compliance based could be done on a voluntary basis by industry instead of using required compliance methods. A performance based requirement structure could accelerate the certification of novel products for which detailed prescriptive requirements are not available. A Proof of Concept (see also change f) can be part of the performance-based method.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Performance based requirements do not necessarily mean the total abolishment of Acceptable Means of Compliance. Certain standardization in how compliance is shown will greatly help the industry to speed up processes. Authority and Industry must work together in the development of AMC material.

Performance based certification can result in the authorities keeping a distance from the development and certification process. This can result in a lesser knowledge of the technology. In the end the authorities must be able to agree the means of compliance used by the applicant, which needs a thorough experience. The authority will have to make sure that the experience of its personnel remains adequate.

Option c: Abolish all certification by Authorities and transform into a voluntary compliance with a certain safety level

Simple systems could be fitted in simple aircraft if it meets the appropriate ETSO (European Technical Standard Order) and provided the manufacturers' installation manual contains sufficient data for non-complex aircraft. If the safety risk of the new equipment is considered minimal with a relatively high safety benefit, this approach could be an acceptable way of working. However, guidance for how these high safety benefits can be predicted, assessed, and measured should made available. In particular, the effect of the loss of the equipment and the effect of misleading information provided by the equipment would need to be assessed and taken into account in the overall assessment. Furthermore, it may be difficult (e.g. for the ETSO manufacturers and/or the aircraft operator) to prove the safety benefits for a given equipment, unless the installation of this equipment is confined to specific products for which the aircraft configuration would be known and controlled as well as confined to specific types of operations, which would significantly decrease the advantage of this option.

The drive to produce a safe product could be generated by the commercial value of safety (an example is the blacklisting of airlines preventing them to operate in Europe if the safety level of the associated civil aviation authority appears to be below standard and) and/or the insurance companies that balance premiums with risk (this is a driver for safer operation in General Aviation). This option will most certainly reduce the cost of Certification activities. The big question is whether the required safety enhancement will be achieved with this approach. For complex systems and/or complex aircraft or new equipment with a high safety risk, this option would most probably not be acceptable. The continued safety of the transport system would be put at risk.

Option d: Make more use of competent (certified) entities to supplement the workforce of the authorities

This can be done under the supervision of the Authority or by delegating the authority to these (certified) entities. The Authorities already put this option in motion. As most Authorities are scaling down their workforce, they have to rely more and more on qualified entities. These can be National Authorities (in the European arena) or commercial and non-commercial bodies. National Authorities are already used extensively by EASA. A tendering process is already started by EASA to contract Qualified Entities. It is not yet clear how much EASA is willing to outsource to these entities. For the short term this is probably a very powerful means to prevent delays in the certification process and to perform the job with enough competence. A risk for the authority is that competence, knowledge and experience will be vested in these entities instead of the Authority. Extensive auditing of the entities needs to be performed.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Option e: Certify the applicants instead of their products

This process is already put in place to a large extend (DOA, POA etc.). The same provisions as under d) above must be taken into account.

Option f: Proof of Concept

First of all it will be important to use a similar definition of what Proof of Concept actually means. Based on descriptions from the different domains covered in ASCOS, this study proposes the following description:

> *A proof of concept (POC) is a demonstration whose purpose it is to verify that certain concepts or theories have the potential for real-world application and will be certifiable. For this purpose a POC uses a prototype (equipment or procedure) that is designed to determine this potential by testing. This prototype may be an innovative, scaled-down version of the system or operation intended to be developed. In order to create such a prototype, tools, skills, knowledge, and design specifications may be required. A PoC can be part of a Performance Based certification method. For this, the result/outcome of Proof of Concept exercises or trials should be the requirements that need to be fulfilled in order to certify the product as well as a more developed specification.*

This definition is based on reviewing descriptions from the different domains that are covered in ASCOS. For example, within the ATM domain the following description is used [7]:

> *The proof of concept is the second stage of concept development (V2), at which basic assumptions should already have been tested and basic design already formulated. At this level, scenarios should focus on more advanced aspects of the concept design, proof of use, non-nominal cases or marginal capabilities. At this stage, there may still need to be a repetition of the type of analysis performed after V1 (establishment of concept principles, but mainly the scenarios here will not be so singularly focused. The outcome of this stage in the validation process should be a mature, stable concept design with an initial proof of concept. Scenarios will be focused on setting the limits of the concept, establishing procedures and phraseology and determining clear requirements to assist in producing a stable environment for the final pre-implementation phase.*

This is an example of a very general description that may be used across domains.

Within the Product Certification domain the following description is used [10]:

> *These Proof of Concept tests shall establish that for evacuation of passengers seated in the overwing area, they can egress the aircraft without unforeseen difficulty or hazard demonstrating that the exits provide a safe and effective means of evacuation. This must be conducted with a double overwing exit configuration, onto a representative wing escape path. The conditions of JAR 25.803 [8] must be applied.*

The latter example however in our view does not represent a PoC, but is an example of a traditional compliance based method, which is typically used in the product certification and airworthiness domain.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4 Perspective of ATM domain

This section identifies new approaches from the perspective of an authority certifying ANSPs (Section 2.4.1), a developer of ATM systems and procedures (Section 0), and an ATM ground system manufacturing company (Section 2.4.3).

2.4.1 ANSP certifying authority

The role of the regulator is to act in *loco parentis* for the public in the context of air transport safety. The regulator is required to apply both European and National law. As with any organisation the regulator should manage itself to ensure it is both effective and efficient. Consequently, where the law makes the role more onerous than necessary the regulator should seek to change it. Current issues in this respect are a) the number and pace of regulations coming from different organisations within Europe (EASA, SES, EUROCONTROL) which are not 'joined up' and b) the current silo mentality, treating individual parts of the air transport system independently of the other parts rather than the treatment of the air transport system as a whole.

Current initiatives

The underpinning principles of the recent changes in European law are:

- The organisation that creates the risk is responsible for it
- The organisation that creates the risk should manage it via the application of an SMS
- Those organisations who are capable of creating significant risk are to be supervised, which takes the form of:
    - Certificating their SMS
    - Supervising the operation of the SMS
    - Approval of change in cases where we believe there is significant risk

Whilst the principles of certification, supervision and the approval of change are very similar across the domains it is observed there are varying levels of maturity in terms understanding and applying the principles.

It is noted that many initiatives are underway to improve the situation, initiatives such as;

- the European Commission Initiative for Better Regulation in the European Union (COM(2006) 689) [9];
- the provision of guidance material by EASA; and
- the EASA's rule making task for the safety assessment of change to address the inconsistencies, the ambiguities and the incompleteness of the legislative requirements with regards to making a change to the aviation system.

Options

The following are extracts from the UK CAA's response to a recent public consultation in view of a simplification, clarification and modernisation of the Single European Sky legislation (SES II +) and alignment of SES and EASA rules. The extracts have been chosen to further illustrate the issues touched on above and to provide suggested ways forward. The text in bold is copied from the questions posed in the consultation. The text in *italics,* provide the CAA's suggested ways forward i.e. the proposed options.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Reference: Improvements in the consistency and focus of new rules through refined institutional arrangements and planning processes.

CAA response: It is important that we have *one clear rulemaking and planning process for ATM and that this process is adhered to* in order to ensure there is sufficient time to develop the best possible regulatory approach and consider the impacts carefully.

Reference: Ensuring policies are decided through a single planning framework and that they all focus on a single agreed objective.

CAA response: These elements are essential if the best use of resources is to be achieved. We need *a co-ordinated, strategic ATM plan, taking into account EASA, EUROCONTROL, SESAR and SES Regulatory issues with all focussed on achieving clear, realistic and agreed goals and prioritising accordingly, including consideration of the ability of ANSPs to implement correctly*.

Reference: Scope for the further reduction of the administrative burden for the small and medium-sized enterprise.

CAA response: There is a multiplicity of regulations, which need time to take effect before we rush to consider new regulation. There is *a need for a strategic pause in order to take stock and ensure that future regulatory activity is performance and/or risk based, drives appropriate behaviour and is correctly focused on the accountable entities that will contribute most to improving performance of the European ATM system*. As part of this exercise where current rules are judged ineffective they should either be modified or removed.

Reference: Ensuring the technical rulemaking is optimally supporting SESAR deployment.

CAA response: The way to achieve confidence and commitment in SESAR is to ensure *that each Operational Improvement has a clear and compelling performance benefit*. It is therefore vital that we *address one of the key gaps between R&D and deployment through the development of robust business cases including CBA*. It is vital now that the aspirational SESAR targets have shifted to SES high-level goals that we consider them for their realism robustly as they could fuel unrealistic expectations of what SES can deliver.

2.4.2 Perspective of ATM systems and procedures

This section surveys the current approach for approval of ATM systems for the provision of Air Traffic Services en-route and at aerodromes; we then draw on this survey to present options for improvement of the certification process across the Total Aviation System (TAS). Note that the term “certification” is used for consistency with the ASCOS project aims; however in different parts of the ATM domain as systems and services are accepted into service in a variety of approaches from licensing through approval to explicit certification, all of which are to be addressed by the certification approach for ASCOS.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.2.1 Introduction

The goal of Air Traffic Management (ATM) is to ensure that aircraft are safely guided in the skies and on the ground. ATM is a complex system involving people, processes, data and equipment interacting in defined ways to deliver this goal. The operational system provides real-time control of aircraft movements through instructions given to pilots by air traffic controllers; these human actors are provided with data by automated information systems; data includes aircraft position and identity, terrain data and weather data. The operational system is supported by further data and processes, including design of the airspace to ensure that routes taken by aircraft maintain safe separation. ATM also involves planning for future developments, which include changes in technology, capacity and safety performance.

There are multiple developments (both on-going and forthcoming) in the ATM environment which drive the need to consider safety from the perspective of TAS, for example:

- target to improve safety performance by a factor of 10
- target to increase airspace capacity by a factor of 3
- target to improve airport management and streamline airport operations
- increasing automation affects the way in which staff (e.g. pilots and ATCOs) discharge their duties and may also affect their on-going competence to manage in failure scenarios
- introduction of new concepts such as
    - self-assured separation i.e. Airborne Separation Assistance Systems (ASAS) changes the focus of responsibility for ensuring separation in a way which must be assessed within the context of the total system
    - free routing, where users can freely plan their routes within a defined airspace
- increased exposure to extreme weather events
- introduction of new technologies (or more widespread adoption of technologies currently only in restricted use)
- continuing need for re-certification and retrospective certification

Many major programmes encounter delays due to their complexity and the way industry is organised. Designers tend to outsource design of significant items to risk sharing partners; thus increasing the number of interfaces across the supply chain.

Even before considering these developments, there is an existing challenge in the complexity of the ATM system. Certification of individual system elements is relatively straightforward; however, the correct and safe interaction of these elements is also critical to the safety of the TAS. These interactions are necessarily complex and it can be in the failure of these interactions where there is the greatest potential for safety not to be adequately addressed. It is therefore critical that an effective certification approach can demonstrate that these interactions are safe – this applies both within the domain and in its external interfaces.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.2.2 Background

2.4.2.2.1 ATM regulatory regime

Whilst in general regulation of aircraft is through type certificates which record compliance with detailed and globally specified specifications (Certification Standards – CSs), within ATM each State is responsible for implementing systems, services, acceptance regimes and regulations in concordance with the ICAO Annexes, Policies, Standards, Recommended Practices and Procedures. In Europe there are also regulations[1], means of compliance and guidance produced as part of the Single European Sky (SES) initiative as detailed and explained on the EASA website. In general the SES regulations are performance-based and usually avoid defining any system or operation specific requirements. The Implementing Rules, for example, mandate in sufficient detail to ensure interoperability of systems between States but do not mandate the specific means by which that interoperability is achieved.

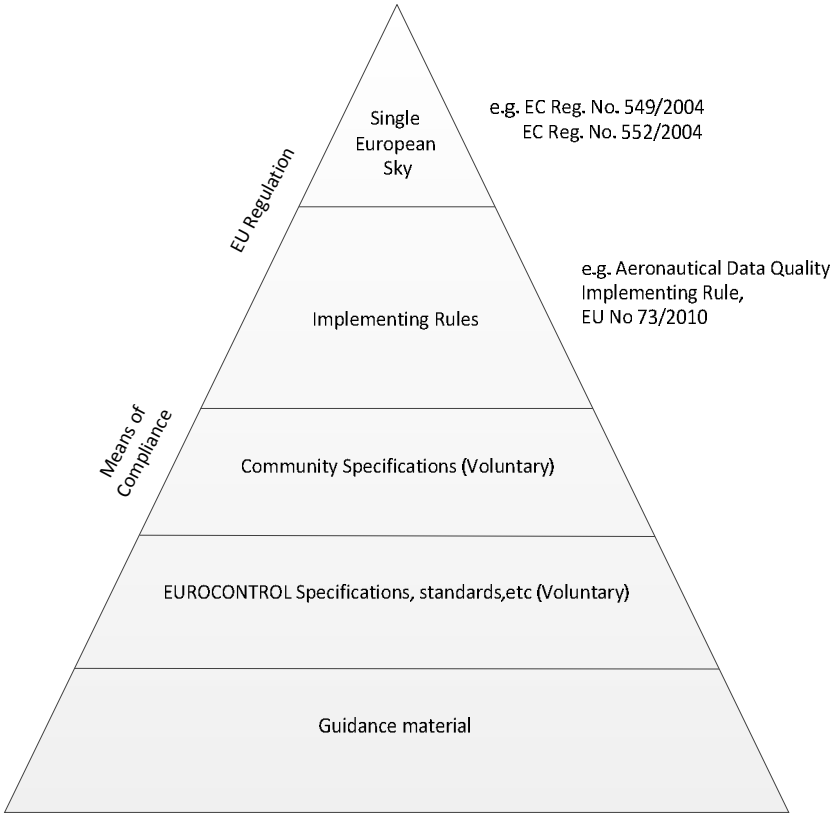

Figure 2 – Hierarchy of SES regulations

The SES regulations include Common Requirements (CRs) for the provision of air navigation services laid down by regulation (2096/2005) of the European Commission (EC) [11]. ANSPs are assessed and licensed against these CRs by the NSA in the State in which they operate. In addition Implementing Rules (IRs) are defined for different aspects of the ATM service provision: these rules are mandatory regulations which must be followed

[1] Note these regulations are enforceable under European Law.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

by ANSPs, covering areas such as surveillance performance and interoperability, initial flight planning, aeronautical data quality, etc.

For each requirement or rule, Means of Compliance are identified or produced, often in the form of Community Specifications. The Means of Compliance are voluntary and States can agree alternative approaches with National ANSPs so long as the regulations are still complied with. Guidance material for many of the regulations has been developed by EUROCONTROL – this guidance is provided to support implementation by ANSPs and NSAs.

Thus approval of a given change to the ATM environment necessarily can involve a wide variety of national, international and European regulations and standards of a disparate nature and detail, all of which may need to be addressed. For this and other reasons the ATM sector in Europe has, to a significant extent, adopted an approach where explicit safety arguments are made for system and service approvals, as discussed in the following section. It should be noted that this approach does not prescribe specific processes either for safety assessment or certification; the approach is sufficiently flexible to accommodate existing processes where appropriate.

2.4.2.2.2 Research into regulatory framework improvements

Previous research (e.g., SESAR Definition Phase [13] and CAATS II [14]) has been undertaken into the current safety regulatory framework for ATM, including its strengths and weaknesses and recommendations for improvement. The strengths identified were:

- successful delivery of effective and acceptably safe ATM despite exceptional traffic growth and technology changes;
- complete and comprehensive regulatory framework providing common standards and procedures which successfully define the roles of the many disparate organisations involved in ATM;
- flexibility in local application.

The weaknesses identified were:

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

These weaknesses are being addressed by the SES initiative. However, any future development of certification schemes within the aviation industry should take these weaknesses into account and consider how they can be further addressed.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.2.3 Safety argument approach to approval

2.4.2.3.1 Implicit and explicit safety arguments

All submissions for safety approval are based on a safety argument of some form. This may be implicit in the procedures to be followed to gain approval, or it may be explicit in the approval submissions, e.g. by constructing a safety case.

An explicit safety argument approach is widely used to assure and justify changes to the ATM system (covering equipment, people and procedures), including the addition of new elements. This approach has also been applied to on-going service provision (so called Unit safety cases), although the approach is not universal.

Key advantages of the explicit argument are its flexibility (e.g. to accommodate new approaches or technologies) and its clarity.

Another common approach, where the safety argument is more implicit, is through application of a prescribed safety assessment such as the EUROCONTROL Safety Assessment Methodology (SAM) [15], which follows distinct stages of FHA/PSSA/SSA[2]. Approaches based on explicit safety arguments can accommodate a wide variety of safety assessment methods and applications, but take a broader view of the evidence required to assure safety.

This explicit safety argument approach is recognised and supported by other research programmes, including CAATS II and SESAR.

It is noted that this is not the only possible approach. However it is presented here as a widely used approach with the greatest scope to provide a framework for certification at the level of the Total Aviation System (TAS) without unnecessarily requiring changes in individual domains.

2.4.2.3.2 Components of a safety argument

A safety argument consists of:

- A set of claims that express why a system or service (made up of equipment, people and procedures) is considered to be acceptably safe;
- Supporting evidence to substantiate each of the claims.

The combined claims and evidence are often presented as a Safety Case, which covers the entirety of certification evidence. The claims being made and thus the types of arguments and evidence provided can vary significantly depending on the focus of the argument; whether it be for example equipment certification or licencing of a service provider.

A key first step in constructing the argument is to clearly define what is meant by “acceptably safe”. An acceptable level of safety is defined in the form of safety acceptance criteria. At the concept level this is usually as a relative and/or absolute risk target. Relative safety criteria are used to show that a change presents no greater risk to safety than was present before implementation[3]. Absolute safety criteria are usually stated as Target Levels of Safety derived from the high level ATM safety targets (ESARR 4), which take into account the potential for the changes to impact the overall safety of the system.

[2] FHA – functional hazard assessment; PSSA – preliminary safety assessment; SSA – system safety assessment

[3] With the exception of changes identified as providing a safety benefit. In this case the risk must (by definition) be reduced significantly.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Additional acceptance criteria will apply to a system or service dependent on the type of system or service and its interfaces to other parts of the TAS. Other criteria may be specific to the lifecycle stage e.g. the transition of the system into operation and on-going safety during operation and service provision. The general nature of certification also changes through the lifecycle from a "product" based argument to a "process" based argument[4]. In the product based argument, the focus is on the certification of the output of a process, e.g. equipment or procedure. In contrast, process based arguments focus on the organisations and processes producing the "product", e.g. day to day air traffic service provision, aeronautical information publication, maintenance, etc. Process based arguments will include for example specifications and justifications for Safety Management Systems employed by an organisation. For example, EC regulation 1035/2011 [12] includes provisions on SMS for ANSPs. Safety arguments can be described textually or graphically and are often set out hierarchically such that any particular claim (the conclusion) is demonstrated if, and only if, all of the next-level claims (premises) are themselves either true (through deductive reasoning), or are highly likely to be true (through inductive reasoning). The arguments can then be further sub-divided until a level is reached at which the supporting evidence for a claim is available and documented. The safety argument is critical as it explains how the acceptable level of safety is (or will be) shown to be achieved. A well-structured argument also drives identification of the evidence needed to support it. It is therefore ideal that the argument is written early in the development process to ensure that production of the required evidence is properly planned.

Supporting evidence is often categorised as direct or backing evidence (as described in the EUROCONTROL Safety Case Development Manual (SCDM)):

- Direct Evidence – evidence that a particular objective has been achieved (i.e. that a higher level Argument or Claim has been satisfied). This is evidence relating directly to observable properties of an output or product (i.e. the output of a process).
- Backing Evidence – evidence that there is sufficient confidence that the Direct evidence can be relied upon (or is "trustworthy"). This is evidence relating to the properties of the processes by which Direct Evidence was obtained, e.g. tools and techniques, human resources applied were qualified/competent and properly deployed.

2.4.2.3.3 Challenges of the safety argument approach

There are three key challenges with the argument based approach which must be addressed.

1. There may be no obvious indication as to how the evidence should be obtained or how rigorous or trustworthy that evidence needs to be. This can often be helped by using prescriptive specifications but this can undermine the benefits gained from performance-based approaches.
2. It is all too easy to create arguments that are false or invalid (or both), or that suffer from what is known as "confirmational bias"[5]. The risk of doing this can be greatly reduced by using formal argument notations, and checking for use of fallacious argument constructions. Good examples of the latter are highlighted in the OPENCOSS deliverable [17] described in section 2.4.2.3.8.

[4] Note that a product based argument may still rely on process or assurance-based arguments and evidence but the focus is still the certification of process outputs.
[5] An implicit bias that can manifest itself if the argument author is too focussed on arguing why the system is safe rather than providing a sound, valid argument supported by adequate evidence and positively seeking out counter evidence.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

3. Safety arguments within ATM often need to address the safety-integrity of system components - software functions or human tasks, in particular, which are difficult to demonstrate through direct evidence. To meet defined target levels of safety it is necessary to specify safety integrity requirements for all components of a system in order to show compliance with a numerical Safety Target. But it is very difficult (if impracticable) to show directly (e.g. by testing alone) that such requirements are satisfied in implementation. As such, and like other domains in aviation and elsewhere it becomes necessary to adopt a more indirect, assurance-based approach which uses the rigour of the development processes to give confidence that the requirements are likely to be met.

The safety case approach does have its critics and one particular example is in the NIMROD review [39] and elsewhere. In this report the Nimrod safety cases are criticised as being out of touch with the system, incomprehensible, insufficiently focussed, lacking in key inputs, not focusing on the true risks. They are also criticised as making an assumption of safety which they then go to every length to demonstrate, rather than starting with an open mind. However, it should be noted that this report levels equally (or more) severe criticisms at the organisations which generate the safety cases. The NIMROD review also recommends that safety cases should be refocused, rather than abolished. The introduction of a structured logical argument for safety provides this focus and guides the safety case to considering all the relevant issues scientifically.

The assurance-based approach defines objectives for how a product is developed. For example, it would consider the design, verification and validation processes, organisational arrangements, etc. It is used in many safety standards including, for example, ARP 4754A [18], ED-153 [20], ED-109 21], RTCA DO-178B [22] and IEC 61508 [23]. Most of these standards focus on hardware and software assurance but it is also the fundamental approach proposed to be adopted as the means of compliance with Article 6.1 of the Aeronautical Data Quality Implementing Rule, currently described in the EUROCONTROL Data Assurance Levels Specification [24]. The recognised key weakness with the assurance-based approach is that it is difficult to demonstrate the correlation between satisfaction of the assurance objectives and the achieved level of safety in the product. Furthermore, there are currently no widely accepted domain standards that address assurance objectives for people and procedures. There are potential weaknesses in the safety argument approach as applied in the ATM sector, including the following.

1. Safety concerns can become compartmentalised, with each organisation responsible for its part of the safety approval but no one entity responsible for ensuring that the arguments fit together, either within the ATM domain or with the sibling domains. In other words, there is no safety case demonstrating that the overall system is acceptably safe. A knock-on effect of this is that it is difficult or impractical to assess properly the full impact of a change on the TAS.
2. Safety arguments can become focussed solely on modelling the (hazardous) failures of a system and demonstrating that the likelihood of occurrence is sufficiently low. This neglects to consider the positive impact of the introduction of improved elements of the ATM system. This is further discussed under Arg. 2 of the Template Safety Argument presented in section 2.4.2.3.4. Approaches such as SAME [25] give significant weight to “success” modelling which models this positive impact.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.2.3.4 EUROCONTROL template safety argument

In general terms all approval processes are argument-driven although often the argument is not explicitly captured. Within the ATM domain methods have been developed to ensure that:

- the argument is logically reasoned;
- it is derived from an adequate definition and understanding of the system and its environment; and
- the criteria for measuring an acceptable level of safety are correctly defined.

Figure 4 shows an example high-level safety argument used in the EUROCONTROL SCDM which is broadly based on the GSN methodology developed by York University. It should be noted that there are many ways to express a safety argument; it is important to choose an approach which can clearly show that the argument is both adequate and valid. Work on the GSN method by York University provides support on structuring arguments in this way [26, 28]. The work of the OPENCOSS project (see section 2.4.2.3.8) [17] may also help in this area. The argument may make use of approved "modules" of argument and evidence for example covering equipment already approved for use, and there are methods (although not yet widely used in ATM) for ensuring the "modules" are integrated correctly. One such method known as Modular Safety Arguments is discussed later in this section.

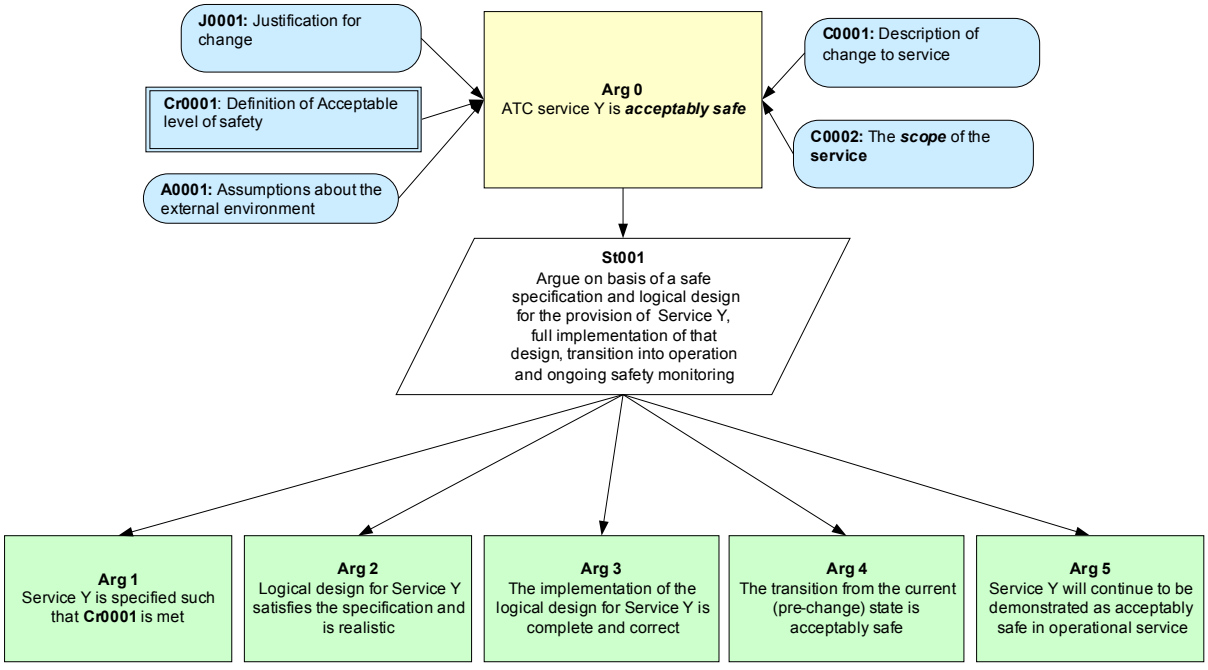

Figure 3 – Template ATM Safety Argument

The top level claim (Arg0) sets out the central claim for the safety argument usually in the form 'System X is acceptably safe' or 'ATC service Y is acceptably safe'. The top level claim is also bound by context to ensure that:

- The system or service at the focus of the argument is clearly defined (especially the interface with the wider SoS context)
- The criteria for determining the acceptability of the system or service are defined. The highest level criteria (for safety) tend to be specified in terms of risk (e.g. target levels of safety), but it should be noted that acceptance criteria may change or extend as the argument is decomposed in order to

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

reflect the certification approach adopted by the regulatory agencies and other factors such as: the lifecycle stage (e.g. design, in-service), the nature of the system components (e.g. procedural, equipment or people) and the significance of any risks to air traffic safety.

- The justification of the system or service is based on sound reasoning including for economic, environmental, operational, or safety benefit.
- Any assumptions made about the environment (including other systems or services) are defined; naturally they must also be reasonable and valid.

2.4.2.3.5 Issues with integration of safety arguments

A number of significant integration issues can arise during the ATM Service or concept "design" stage (and this includes the derivation of regulations[6], standards and certification specifications), including:

- The high level claims within a safety argument are usually made in the context of caveats such as operational limitations, implementation constraints, potential safety issues or non-conformance, some of which may place dependencies or assumptions on parts of the TAS outside the responsibility of the ATM domain.
- The output of an ATM concept design process is a series of design component and interface specifications, which together ensure that the higher-level performance-based specification is achieved. But a design specification may already be defined for specific equipment and procedures such as for Mode S SSR, ILS, etc. These specifications may explicitly or (more usually) implicitly be assumed to be correct as they stand or may need tailoring to local conditions in the environment where the equipment is installed or the procedure is deployed.
- The design specifications need to be realistic or realisable, i.e. the functionality, performance or integrity required are implementable by people, equipment or procedures. For example, in theory an Airborne Collision Avoidance System should be specified to detect and avoid any and all possible aircraft encounter scenarios. In practice this proved to be impracticable and current TCAS II cannot provide a safe RA in all possible multiple aircraft scenarios.
- There can be unintended consequences on other systems if those systems are only considered in the context of the system or service under consideration for approval. For example, the TCAS II display indicates the location of other aircraft in the vicinity but is not intended to be used as a true situational awareness picture. A bulletin was issued by EUROCONTROL to this effect in March 2005 (ACAS II Bulletin No 6 [27]) to ensure that pilots did not solely use the display for this purpose.
- The physical implementation of specifications can have unintended outcomes as a result of the implementation technology or equipment chosen. E.g. the equipment may provide more functionality, which was not considered during the design phase. It is then necessary to demonstrate that these unintended outcomes (e.g. extra functionality) cannot adversely affect the safety of the system. This is a common issue with Commercial-Off-The-Shelf products.

[6] Note much of the SES regulation rule-making for ATM was supported by specific safety argument-based safety assessments to ensure that the provisions (albeit at an abstract level) are complete, correct and implementable.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.2.3.6 System models within ATM

The safety argument-based approach is necessarily based on a clearly defined model of the ATM system, its environment, and its operations, which represents behaviour in both normal and failure conditions. If you do not fully understand how each system works or interacts within the TAS then you are likely to produce an inadequate argument for the safety of that system, or undermine the argument for other systems. Even within the ATM environment these models can quickly become large and complex. For example ACAS II is an ATM concept that encompasses diverse elements including, for example, air traffic service provision procedures, TCAS II airborne equipment, pilot procedures and aircraft operators and maintenance. The efficacy of ACAS is reliant on all of these aspects to some degree in order to ensure the safety of the collision avoidance function, for example the performance of the TCAS equipment, the response time of the pilot, reporting of RAs, etc. Figure 5 shows a logical model capturing some logical elements (related to collision avoidance) and the interactions between them. Note that, whereas a system model may capture only the desired interaction between elements, the safety model must also address undesired/unintended interactions between elements, including those which are not part of the system under consideration.

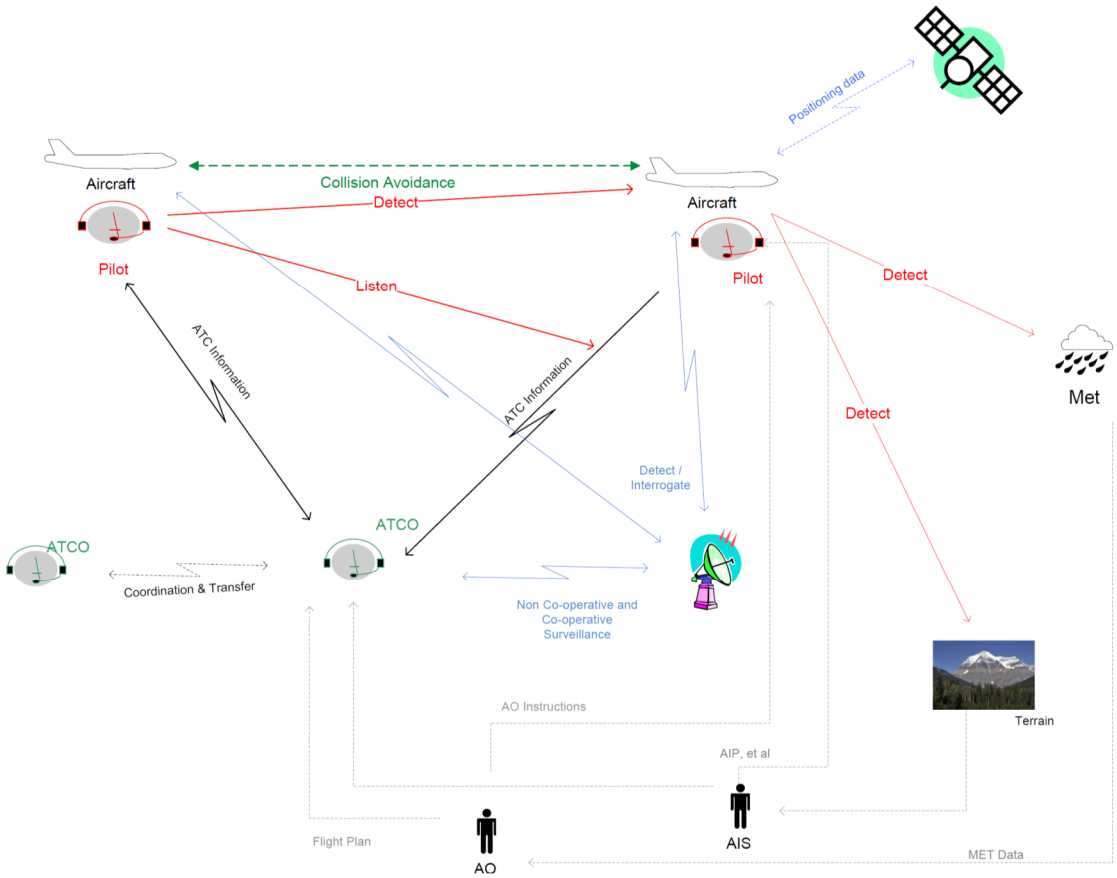

Figure 4 – Logical ATM system diagram

It is critical that the safety argument considers the TAS in sufficient detail. Otherwise, the assumptions made may be invalid; dependencies may be either unrealisable or unenforceable. Dependencies are of particular

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

concern, because they form part of a "contract" between parts of the system; care is needed to ensure that this contract is correctly specified and met.

There is thus a need to ensure from the top down that a "System of Systems" (SoS) approach (see section 2.4.2.3.7) is adopted. This approach not only needs to manage the break-down of the system into manageable elements, but also the subsequent integration back into a total system to assure the interoperability of the elements and address any unintended consequential behaviour.

Development of these system models provides significant benefit in ensuring understanding of the system and therefore informs the whole safety argument development process. Only when we develop such a model of the TAS can we fully assess the efficacy of new approaches and have confidence that the whole scope of safety issues is addressed.

2.4.2.3.7 System of Systems (SoS) concept to consider the aggregation of multiple systems / domains

The ATM System is in itself already a "System of Systems" (SoS), even though it is only part of the TAS. The Safety of Systems of Systems (SoS) is an active academic research topic. Several papers on the subject have been published by the High Integrity Systems Engineering Department at York University, UK [40]. The term is defined as a collection of systems with a number of characteristics; the most relevant characteristics to this discussion are:

- Common overall objectives
- Multiple elements, which are systems in their own right and which are developed independently from the SoS
- Autonomy of the elements of the system
- Geographical dispersion
- Collaboration and communication
- Heterogeneity – elements developed independently from each other using different technologies and different developers.

In particular, elements are often "fully developed" before they enter service in the SoS and thus there is little or no scope for further development to address safety requirements or constraints imposed by other parts of the system.

One of the key challenges is the interfaces between the elements of the SoS; often the elements themselves will have good safety arguments (which are also well supported) but these are dependent on assumptions which the safety case makes about the environment in which the element is used (i.e. about the rest of the SoS). An example is that the safety case for a radar may be dependent on its availability, which may, in turn, depend on it being maintained according to particular procedures. Where a new radar is being introduced into the ATM SoS, the safety of the SoS becomes dependent on successful integration of the new maintenance procedure into the existing maintenance regime.

Multiple papers have been published on the System of Systems approach and these would provide valuable support to developing a TAS approach to certification.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Different elements of the SoS may require or necessitate different approaches to certification and / or approval; approval of the overall SoS must take these differing approaches into account.
Application of the SoS concept assists in understanding the system and its interactions and therefore supports the overall development of a safety argument on which the certification approach can be based.

2.4.2.3.8 Integration and standardisation of safety argument-based approach

The safety argument approach is directed at addressing the issues highlighted above (section 2.4.2.3.5) with regards to assuring that the TAS is acceptably safe as a complete system. In particular, an approach is needed to ensure that the aviation domains interface correctly with each other with respect to the safety arguments (whatever form these take) being made.
Successful integration of approvals across the domains will also depend on clear interfaces with the safety assessment (within each domain and of the total aviation system). Thus, a safety assessment methodology that deals with the total aviation system will need to provide clear outputs, in particular defining the assumptions, dependencies and restrictions to be passed between different components subject to approval.
The OPENCOSS project (Open Platform for EvolutioNary Certification of Safety-critical Systems) is another EU research project; it aims to devise a common certification framework for safety critical embedded systems. This aims to address the problems of certification (and especially recertification) of such systems. In particular, this project is looking to establish:

- a language in which to express safety arguments;
- a compositional approach to certification;
- an evolutionary approach to the management of certification evidence.

This project is currently underway and its outputs should be reviewed as inputs to the development of an integrated aviation certification approach.
One of the approaches considered by the OPENCOSS project is the Modular Safety Case approach (also pioneered at York University, see for example “Managing Complex Safety Cases” [26, 28]) which defines a way in which a safety case for an overall SoS can be broken down into manageable modules, where each module is the safety case (i.e. argument and evidence) for a discrete element of the system. The approach recognises the need for “contracts” between the separate elements of the SoS, allowing development of the safety argument for each element separately in confidence that the argument for that element will support (and be supported by) the rest of the argument. This approach would allow multiple types of radar system or aircraft (for example) to be used within the total system as long as they all comply with the contract for that element of the SoS. This approach also facilitates replacement or upgrade of individual elements of the SoS without the need to redevelop the whole argument.
The modular approach can be applied in a hierarchical fashion, where the “contract” of an aircraft with the rest of the ATM system could be at the aircraft level, but where the contract could be fulfilled by multiple modules which, together, satisfy the contract at the aircraft level.
The modular approach is illustrated in Figure 6, which shows how safety case modules may be overlaid onto the logical model presented in Figure 5.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

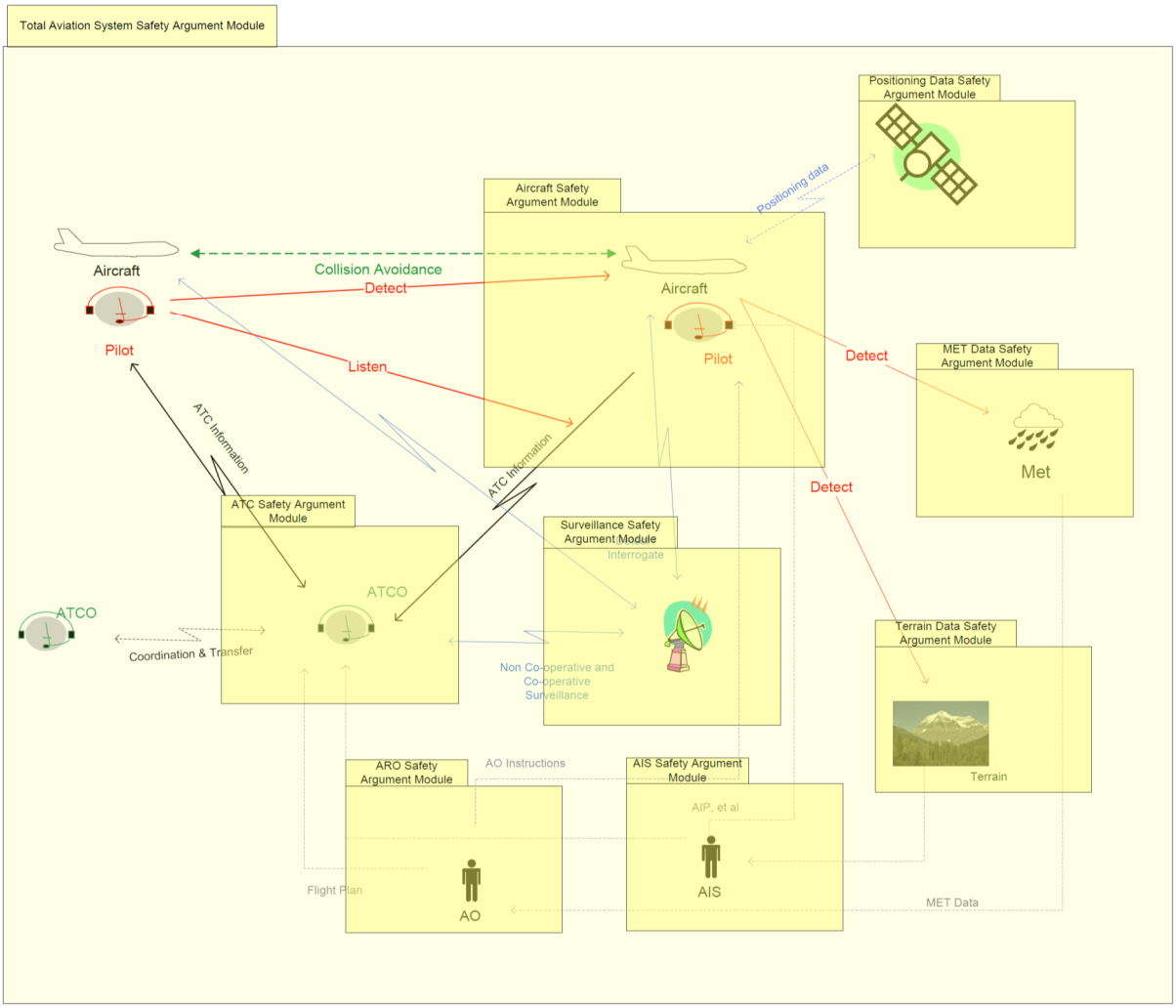

Figure 5 – Decomposition of TAS safety argument into modules

2.4.2.3.9 Aligning approvals to the system lifecycle

Previous work has mapped existing safety assessment methodologies to a generalised development lifecycle. This mapping is documented in CAATSII D13 [14]. However, it is more usual for certification to come at the end of the lifecycle, when the development is complete. This approach inevitably introduces a degree of (non-safety) risk, as the regulator may determine that the development has overlooked a fundamental requirement thus requiring a significant amount of rework and consequent delay. In practice, it is difficult for the regulator to become involved early in the lifecycle because (a) there is nothing concrete to assess and (b) the regulator may have limited resource to support early engagement. This does not mean that regulators are not interested or involved in the earlier development lifecycle.

An example initiative in this area is Virtual Certification. The UK CAA Safety Review Group is currently piloting this on the ASTRAEA project. The aim of the ASTRAEA programme is to enable the routine use of UAS (Unmanned Aircraft Systems) in all classes of airspace without the need for restrictive or specialised conditions

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

of operation. This will be achieved through the coordinated development and demonstration of key technologies and operating procedures required to open up the airspace to UAS. ASTRAEA (Autonomous Systems Technology Related Airborne Evaluation & Assessment) is a UK industry-led consortium focusing on the technologies, systems, facilities, procedures and regulations that will allow autonomous vehicles to operate safely and routinely in civil airspace over the United Kingdom (http://www.astraea.aero). In "Virtual Certification", concepts and designs are submitted before development of the "real" product to gain early comments by the NSA, and to build confidence that the real product will gain approval.

There would be benefit in reviewing the certification process against the lifecycle and determining whether elements of early engagement could be introduced in the new approach without placing unmanageable burden on the NSA.

2.4.2.4 Alternative approaches to certification

This section provides a detailed explanation of the approaches to certification which could be developed from the approaches currently employed within the ATM domain.
It should be noted that these approaches are not mutually exclusive, and in some cases a combination of approaches could be applied.

2.4.2.4.1 Do not change approach but enforce safety argument across the ATM domain

This approach recognises the value brought by making formal safety arguments to document the safety argument for a system: in particular, this provides an explicit argument, supported by evidence, which can be assessed by the appropriate regulatory authority. It also ensures that any assumptions on which the safety argument is based are documented so that they can be communicated to whoever has the power to ensure that they are addressed. (The term "assumptions" is used here in the most general sense – it may include restrictions or conditions on the way in which the system is implemented or used as well as assumptions about the behaviour or properties of other parts of the system.)
A particular focus of this approach would be the introduction of the success case part of the safety argument; safety arguments in the ATM domain have historically concentrated only on the failure case argument.

This approach is a relatively small change as safety cases are widely used in the ATM domain already.

The main benefit of this approach would be to provide uniform safety arguments for all ATM equipment and to improve the documentation of assumptions on which the arguments are based. It would also ensure that the success case part of the argument is given the appropriate weight where previously it may not have been adequately considered. However, this would provide only a limited safety improvement of the Total Aviation System as it would not provide a clear route for ensuring that the assumptions are incorporated into other parts of the system as required.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.2.4.2 Cross fertilisation by applying safety case approach across all domains

This approach requires each domain within the Total Aviation System (TAS) to adopt formal (performance-based) safety arguments (in the form outlined in section 2.4.2.3) for each system and / or product within the domain. The safety argument would take a similar form to the template safety argument described in section 2.4.2.3.4, although the details will need to be tailored for each domain. This approach envisages the domains would still remain separate, in that there would be no explicit linkage between the safety arguments made for the individual systems. This would also include giving appropriate weight to the success case part of the argument, an area which has historically not been considered in sufficient depth.

The key challenges of this approach are:

- lack of familiarity with the approach within the affected domains, leading to resistance and delay in the implementation of the approach;
- development of safety acceptance criteria suitable for each of the domains, such that the criteria are mutually consistent across the domains and also applicable within each domain.

The main benefit of this approach would be to provide uniform safety arguments for equipment and processes across all domains within the TAS, and to improve the documentation of assumptions on which the arguments are based. However, this would provide only a limited safety improvement of the TAS as the safety arguments would still be made in isolation from each other and would not ensure management of the assumptions made between elements, both intra- and inter- domain.

2.4.2.4.3 Integrate all domains into a total aviation system safety argument

Although this approach appears to introduce a huge change, the intention is to limit the impact by introducing an infrastructure (see section 2.4.2.3.8) within which each domain is free to either retain its existing approach or to adopt a different approach dependent on the needs of individual systems.

As discussed in section 2.4.2.3.8, the overall goal of this approach is to demonstrate that the TAS as a whole achieves and maintains an acceptable level of safety, and in particular address the interface issues that can exist between domains. This approach would:

1. recognise that each element of the TAS is a system in its own right, which will have its own development lifecycle;
2. define an overall system model which defines what is required of each element so that it is clear what needs to be achieved (to maintain or improve safety) when an individual element is added, replaced or changed, and so that it is clear what impact this change has on the rest of the TAS.
3. wherever possible, avoid being prescriptive so that it allows flexibility in implementation and in choice of solutions (including new technologies) for individual elements of the system.
4. recognise that system safety is an emergent property which entails more than just arguing that individual elements are safe; it must also show that the elements combine to deliver a system which is acceptably safe;
5. recognise that different elements of the system may be suited to widely different certification approaches.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Any approach to TAS certification must be based on an understanding of the TAS as a system (using the System of Systems paradigm). There is a need to ensure that the interfaces both intra and inter domain are valid, realisable and where necessary enforced. A system model supports the development of a safety argument for the TAS. This safety argument overlays the system model and defines:

- the acceptance argument for the overall TAS
- the certification approach for the overall TAS
- identification of the individual elements (or combination of elements) about which acceptance arguments will be made
- recommended outline acceptance arguments (including certification approaches) for each of the individual elements
- any dependencies / assumptions between the individual acceptance arguments

The safety arguments and certification approach for each element may be completely different as long as the certification ensures that the dependencies (in both the system model and the acceptance model) are met. Arguments for individual elements will draw on a variety of approaches, for example:

- Certification of a surveillance system to be applied at a specific airport based on a performance based safety argument.
- Certification of a product for use on an aeroplane based on compliance with a specification
- Certification of an air traffic control provision to be applied at a specific airport based on the processes to be followed and the competence requirements for the staff undertaking those processes.

Finally, it is necessary to define how the overall acceptance argument is monitored to ensure that it remains valid (and that the system therefore remains acceptably safe) in the face of changes to the elements of the system. The aim of the safety argument, and the definition of dependencies between the elements of the argument, is to make it possible to undertake this monitoring.

The approach described above:

- increases (confidence in) safety, by ensuring that the internal and external interfaces are properly defined and assessed;
- minimises the unnecessary impact between domains, such that each domain can be allowed to work using familiar methods and terminology (which may be specialised for the domain) while also specifying strong interfaces between domains such that the interactions are properly captured and controlled;
- embraces new technology through use of techniques which focus on the levels of safety performance required, rather than how the specific functions need to be performed;
- increases flexibility, supporting changes to discrete parts of the system;
- guides the certification approach for each component to follow the most suitable approach for that component – thus allowing costs to be streamlined.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

It is noted that there would be an initial overhead cost in establishing the safety argument interfaces for the TAS – but it is expected that the on-going cost would be minimal once the "contract" for each part of the system was established. It is further expected that the cost would be small compared to the benefits achieved as described above.

2.4.2.4.4 Apply Proof of Concept (SESAR certification tool) across domains

The SESAR project has a Work Package as part of its development phase (WP16.1.4) which is developing a proof of concept approach for aircraft certification [41, 42]. The idea is to speed up certification by engaging all the relevant authorities in development and testing of a prototype prior to the formal development, validation and certification of the final product. This approach allows early integration of the prototype with representative ground and aircraft systems; it also provides an early opportunity for training of personnel in use of new equipment and procedures. As a result, there is an opportunity to gain increased confidence that eventual deployment of the equipment will be successful.

The proof of concept approach could usefully be applied to any of the domains within the Total Aviation System. This approach is a potentially useful tool to reduce risk in the certification process. It is not linked to any particular certification approach and could usefully be integrated into any new or existing approach.

2.4.2.4.5 Introduce compliance based certification of ATM products

Certification of ATM products is currently largely performance based – high level safety targets are set in the relevant standards (e.g. ESARR 4 [16], with application guidance in EUROCAE ED-125 [19]) and a suitable safety assessment approach is followed to develop safety requirements which will enable the product to meet these targets. A safety argument and safety case is then developed to demonstrate that the product meets the safety requirements.

It would be possible to develop standardised safety requirements for a given ATM product, to form a prescriptive product specification, embodying the safety targets. For equipment types whose use is well-established and which are used within a consistent environment, this would reduce the amount of work needed to develop a new product, as the supplier would simply need to develop to the specification without the need of specialist support to develop a safety argument and safety case. However, it is often difficult to make specifications sufficiently generic to permit any innovation in the product implementation; as such this could restrict the opportunity to innovate in development of new products.

It would also be necessary to establish the concepts of generic type approval and specific application approval (as widely adopted in the rail industry – see CENELEC EN 50129:2003 [29], expected to be superseded by CENELEC EN 50126-4:2012 [30]). This is because ATM products exist within the context of the services provided within their specific ANSP, which are subject to variation between ANSPs. The concept of "individual airworthiness" does already exist for aircraft; this applies the type certification to an individual aircraft. A similar mechanism could be used here, but it would need to include a more in depth consideration of the context of the specific ANSP to ensure that the product was correctly and safely integrated into its environment.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Thus compliance based certification could lead to generic type approval for ATM products, but there would always be a need to confirm the safety of the specific application of the product within the specific ANSP. In order to make this feasible, it would also be necessary for the type approval process to yield sufficient information on the performance and assumed environment of the equipment to allow for safety analysis of the specific application.

2.4.2.4.6 Introduce certification of applicants rather than products

This approach is already adopted within the ATM domain (where ANSPs are licensed to provide an ATM service in accordance with European Commission regulation 1035/2011 [12]), and also for airlines.

The existing certification of products (and systems and procedures) provides a strong mechanism, with external validation, for ensuring that these items meet their safety requirements and therefore deliver the required level of safety. Any shift of focus from products to applicants may reduce the effectiveness of the existing certification process and therefore has the potential to reduce safety.

It is therefore recommended that this approach should only be adopted where the product (or system or procedure) cannot be certified effectively, or where applicant certification is necessary to supplement product certification.

2.4.3 New approaches from the perspective of a ATM ground system manufacturing company

2.4.3.1 Introduction

The general approach for certification of ATM ground systems is that a safety case is developed and approved by Competent Authorities before transfer into operation of an equipment/system. This safety case (ANSP level)[7] is including all parts of an ATM system by addressing risks assessment from human, operational procedures and equipment aspects. Currently there is no “standard” (except some notation like GSN) to develop safety arguments supported by relevant evidence. The Safety Case is performed by considering the specificities of the Operational Environment (e.g. traffic, airspace structure, geography, …). An equipment safety case is provided by the industry in order to be integrated in the global one by the ANSP.

In general there are few ATM regulatory requirements that bear directly upon ground system manufacturers. However, many requirements are passed on from the end users of the systems who themselves must comply with regulatory requirements. Ground system manufacturers must also meet many other standards that are not derived from ATM safety regulation. The ATM ground systems used by ATM service providers also interface with all of the other elements of the ATM system, particularly airborne systems and airport systems. Ground systems manufacturers must therefore be aware of numerous regulations from ICAO, EUROCONTROL, EU and national regulators.

[7] Note that this Safety Case approach towards certification, which is used in the ATM domain, differs from the approach that is usually followed in aircraft system certification.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.3.2 A simplified risk assessment life cycle

The ATM ground system interfaces with ANSPs, Airports and Airborne systems. These interfaces are therefore of particular significance to the ground system manufacturers. To facilitate these interfaces for safety management there are three key phases that need to be addressed. These are:

Allocation of risks: this refers to all the activities related to the right identification and apportionment of risks on the different components of an ATM system (people / procedure/ equipment): what are the relevant safety targets and derived safety objectives/ requirements and how are these objectives/ requirements apportioned to the different components of an ANS System?

Demonstration: the aim is to conclude that the risks are controlled. Because of the different nature of the components of an ATM system the approaches regarding "demonstration" approach can be different (e.g. qualitative versus quantitative). Methods must be harmonised in terms of assessment of the efficiency of mitigation means (e.g. procedures, people, hardware and software are not assessed in a same way). Weaknesses of certain parts of the system can be compensated by miscellaneous mitigation means. For example software failures can be mitigated by operational procedures and in this case, what is the relevant assurance level for an operational procedure in order to demonstrate that the SW failure of a component at a certain assurance level is mitigated? Thus a concept of AMC (Acceptable Means of Compliance) needs to be shared between stakeholders (ANSPs, Industry) whatever the nature of a component of an ATM system (people, procedure, equipment).

Measures: how to measure safety (rationale) and to be sure that safety is globally at a tolerable level and/or is improving? It supposes for example that based on accident/incident models some safety criteria (e.g. acceptable % of failure rate of safety barriers) can be defined and used as reference by safety demonstration. Moreover the concept of assurance levels with related rigour of evidence should be in line with severity and probability classification scheme. Moreover particular attention should be put on "safety a posteriori" (service history) which is a very useful alternative way to assess the safety.

Obviously the three steps are not independent and interactions between each other have to be considered. These three steps can be used as "time" drivers for new or adapted approach of the certification process.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.3.3 Strength & weaknesses of current arrangements

In order to clarify the strengths & weaknesses of the current arrangements, the following points need to be assessed:

- **WHAT** is necessary to cover regarding the *scope and consistency of current applicable regulatory framework*?
- **WHO** are involved and what kind of *interface must be put in place between stakeholders (industry, air services providers, competent authorities)*?
- **WHY** are some improvements needed regarding the existing approach (approach to use in terms of "*compliance based" versus "performance based")?*
- **WHEN** has the new adapted certification process to be operated? This reflects a simplified System Life Cycle including allocation of risks, demonstration that the risks are controlled, measure that the level of safety complies with the defined safety targets.

Based on these considerations **HOW** could some options and/or alternatives be identified in terms of improvement from industry perspective and what are the Pro/ Cons of each possible option?

The following table provides details about the different aspects of this analysis.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHAT is necessary to cover?	**WHEN (according to the simplified life cycle)**		
	Allocation	**Demonstration**	**Measure**
Scope and consistency of the Regulatory Framework			
Scope of the safety assessment: The scope of the safety assessment depends on the considered system boundary. For example the identified hazards and related Mitigation Means differ regarding the part of the ATM system to be considered (equipment, operational procedures and environment, human capabilities,…). The assumptions related to scope (hazards and corresponding set of mitigations) and their interactions are fundamental in the safety assessment and the construction of safety arguments. Moreover a broader approach as used in SESAR is considering safety not only from integrity (failure approach) but also from functionality and performance (success approach). These both approaches contribute to a more efficient risk reduction. This is a reason why a safety case could be difficult to reuse for different operational environments and very often should be considered case by case. What could be the consequence regarding "certification"? ***A new adapted certification process should include the relationship and condition of reuse (assumptions, limitations) of safety case and certification folder.*** Scope of the ANS Life cycle: The safety arguments refer to a set of processes/activities from the definition of a system to its decommissioning. This set of process/activities (not only design and development but also for example maintenance, management,…) are considered as a reference for the CNS/ ATM Life cycle and represent all sources of risks. Thus it facilitates the completeness of hazards identification. ***For completeness of Risks assessment it is necessary to refer to the global life cycle (sources of risks issued from a reference set of processes/ activities). The certification process should cover the whole reference ANS life cycle.***	*	*	

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHAT is necessary to cover?	**WHEN (according to the simplified life cycle)**		
	Allocation	**Demonstration**	**Measure**
Consistency based on Traceability between regulatory frameworks (airborne, airports, ground systems…): Avoid duplication / conflict between European and National Safety regulation: • e.g. SW assurance levels (SWALs vs prescriptive requirements about standards) • Need of a clear separation between the "What" and the "How" Taking into account system boundaries including airborne, airports, ground systems…the set of documents related to these different frameworks (regulation, standards, guidance material) need to be consistent (e.g. traceability between safety requirements coming from different frameworks when explicitly defined should be possible). This traceability is a good support to "allocation" & "demonstration" phases. Example of traceability between regulatory frameworks: number & definition of Assurance levels for software, hardware, procedures consistent with ESARR4 [16], EC 482/2008 [31] ***The certification process should be applicable whatever the domain (airworthiness, ATM, …) by assuming consistency through traceability with related regulatory frameworks (e.g. in terms of severity classification, assurance levels allocation, objectives gradation and use….)***	*	*	

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHO are involved and what kind of interface must be put in place between stakeholders?	**WHEN**		
	Allocation	**Demonstration**	**Measure**
Interface between Industry - Air Service Providers - Competent Authorities			
Safety Management System: is there a need of a formal Safety Management System for the Industry in order to facilitate efficacy of interface between stakeholders and avoid potential safety gaps? Actually the Industry is using Capability Maturity Models to assess the maturity and efficiency of their organizations, for example there is a possibility to develop measures of maturity (e.g. CMMI and iCMM are maturity models broadly used by industry). Moreover the definitions of these models have been extended by DOD and FAA in order to include safety and security aspects. However, these models are not "safety standards" although some Standards refer to these maturity models as a means to provide safety backing evidence mainly regarding processes (e.g. ED153 [20] for the software). These models could be a good support to Measure the efficacy of the Safety Management System (by facilitating the lessons learnt about the definition and use of key indicators) since these maturity models could be a reference for stakeholders. A Safety Management System is including many aspects (organization, procedures, tools, action plans, continuous improvement, reporting…). The point is "how to measure" these different aspects and" how to be sure" that the safety management system is improving? ***The new adapted certification process should reflect the benefit of continuous improvement culture through the Safety Management System whatever the stakeholders***			*
Safety Monitoring: There is a need of transparency between ANSPs and Industry regarding the apportionment of safety objectives into safety requirements and the way to balance their stringency. Considerations must be taken into account, mixing different kind of mitigations including measure point of view (e.g. concept of Assurance levels applicable for procedures and equipment). This supposes: - Lessons learnt and Need of Feedback from ANSPs to Industry about safety measure and monitoring of systems in operation in order to optimise safety levels of components (e.g. confirmation or not about the right allocation of an Assurance level);	*	*	*

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHO are involved and what kind of interface must be put in place between stakeholders?	**WHEN**		
	Allocation	**Demonstration**	**Measure**
- Visibility about the Assurance levels allocated to Procedures in order to converge to the "best solution" regarding "how to balance safety requirements" between the components of an ANS system (compromise cost/ safety); - Harmonised method to balance safety requirements between different components of an ANS system (people, procedures, equipment) in a Total Aviation System context; - Regarding the apportionment of safety objectives into safety requirements and the way to balance their stringency, considerations must be taken into account, mixing different kind of Mitigations including measure point of view (e.g. concept of Assurance levels applicable for procedures and equipment); - Harmonised measures of safety effectiveness of Mitigation Means (people, procedures, equipment): Sometimes an "operational procedure" can mitigate a hazard due to a failure of equipment. As part of the rationale of the demonstration, a measure of influence of mitigation means on failures control (whatever their nature) should be considered (e.g. ability to prevent, detect or recover a failure). Safety occurrences reporting: Safety occurrences reporting can take different forms regarding the stakeholders (ANSPs, Industry). For ANSPs, for example, accidents, incidents with associated severities are reported. For the Industry, safety occurrences rather are addressing failures of equipment functions through a problem reporting process. Globally these data can be used to measure the "safety performance". ***The new adapted certification process should include requirements in terms of transparency and clear responsibilities between stakeholders regarding safety monitoring and safety occurrences reporting.***			
Certification versus Approval: In order to demonstrate the compliance of an equipment with a set of safety objectives / safety requirements, different situations can be encountered. For some equipment, a formal certification is requested (e.g. navaids); for others (e.g. control centres) an approval from an authority is only requested.		*	

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

<u>WHO</u> are involved and what kind of interface must be put in place between stakeholders?	**WHEN**		
	Allocation	**Demonstration**	**Measure**
• The roles of Certification authorities need to be clearly identified and delimited (e.g. value of a "certificate" regarding different countries) • In the context of EC 552/2004 [32] regulation, a declaration of conformity or suitability for use is requested depending the need of demonstration of compliance with a CS (Community Specification) or an AMC (Acceptable Means of Compliance). In practice the need of DoC (Declaration of Conformity) or DSU (Declaration of Suitability for Use) remains unclear. ***The new adapted certification process should provide clear regulatory references and justifications about the criteria to authorise products/ operations to be certified (e.g. delegation arrangements)***			

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHY some improvements are needed?	**WHEN**		
	Allocation	Demonstration	Measure
Compliance versus Performance based approach			
The effort to reduce risks must be proportionate to its level. Risks classification scheme, safety target levels, safety objectives, safety requirements: As input to the safety assessment, a risk classification scheme is used to classify risks and determine risk tolerability. For each severity level, a safety target level is defined. According to safety target levels, safety objectives are defined in terms of qualitative or quantitative statements that define the maximum frequency at which a hazard can be accepted to occur. Then safety requirements can be derived for each component of an ANS system from safety objectives. At each step of the safety assessment a generic problem of "allocation" has to be addressed. Units (e.g. safety objectives, safety requirements): The units used to define safety objectives or safety requirements need to be consistent whatever the level considered (operational, equipment). For example, "per landing" for navaids, "per flight hour" for control centre can be considered. This can be a problem regarding the consistency between the different risks models and the phases of flight. ***The new adapted certification process should include a generic part dedicated to the principle of apportionment of risks and a specific part more dedicated to reflect the specificities of these risks according to phases of flight (e.g. in line with safety occurrence data from risks models like number and diversity of precursors). The required effort for both parts should be proportionate to the level of risks.***	*	*	*
Safety assessment of a Change What are the criteria for a classification of changes? How to use the Accident-Incident models to assess a safety improvement due to a change? What about service history? How to use the service history as a "certification credit"? Could we really "certify" COTS? ***The new adapted certification process should reflect the impact of a change and assumptions about the condition to use the service history.***	*	*	*

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHY some improvements are needed?	**WHEN**		
	Allocation	Demonstration	Measure
Technology aspects What is the safety benefit of a technological innovation? Could we use the concept of "TRL Technology Readiness Levels" for certification purpose? ***The new adapted certification process should clarify the impact of the use of a new technology***	*	*	*
Rigor of evidence: Safety arguments referred in the safety assessment can be qualitative and quantitative regarding their nature (Hardware, Software…). This aspect is impacting the demonstration of compliance and the way to measure this level of compliance (e.g. what kind of assurance level for which severity level?) More generally the rigor of direct and backing evidence supporting the arguments remains a problem due to the fact that the use of objectives metrics is not largely accepted by the community. ***The new adapted certification process should provide requirements regarding the rigor of evidence to support the demonstration with rationale***		*	*
Harmonised measures of safety efficacy of Mitigation Means (people, procedures, equipment): Sometimes an "operational procedure" can mitigate a hazard due to a failure of equipment. As part of the rationale of the demonstration, a measure of influence of mitigation means on failures control (whatever their nature) should be considered (e.g. ability to prevent, detect or recover a failure). ***The new adapted certification process should contain consideration about efficacy of kind of mitigation means in line with safety risks models.***		*	*
Service history arguments • Need to clarify and to improve the Service history measures (link with safety reporting): A large part of safety arguments in a safety assessment is based on confidence coming from a service history (e g legacy systems): "a posteriori" demonstration. The question is "how to measure" the service history considering different exploitation environments and "how to use" this measure for relevance of arguments?		*	*

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

WHY some improvements are needed?	**WHEN**		
	Allocation	Demonstration	Measure
• Need to justify the relevance of the history data for safety purpose • Consistency with risks models ***The new adapted certification process should combine with a sufficient flexibility "safety a priori assessment" and "safety a posteriory assessment" (service history)***			
AMC Acceptable Means of Compliance: The concept of Acceptable Means of Compliance is introduced due to the fact that different kinds of arguments can be used to demonstrate the compliance with a "requirement". The consequence is that there is a need to define clearly what it is intended in terms of "acceptable". AMC (Acceptable Means of Compliance) need to be assessed from process and technical aspects: • According to relevant ANS life cycle and scope of the Safety Assessment • Traceable to other regulatory documents (e.g. ESARR4, EC482, SWALs) for "end to end" demonstration purpose • Based on objectives and related evidence rather than prescriptive solutions • Compatible with open architectures and introduction of new technologies ***The new adapted certification process should include requirements for an AMC depending on the considered context.***		*	

Table 2.1 Assessment of Regulatory Framework (legislative / regulatory, standards, guidance material)

2.4.3.4 Alternatives approaches to certification

This section provides a detailed explanation of the approaches to certification which could be developed from Industry perspective by considering Regulatory framework, Stakeholders interface and Performance issues according to a simplified life cycle phases. It should be noted that these approaches are not mutually exclusive, and in some cases a combination of approaches could be applied.

2.4.3.4.1 Integrate all domains within the Authority (EASA) [option a]

In a context of Total Aviation System approach, the notion of AMC (Acceptable Means of Compliance) must be commonly understood and defined whatever the domain. All along a reference life cycle including maintenance (after a transfer in operation), these characteristics have to evaluated by taking into account the coverage of the Regulatory requirements (by traceability) and the safety benefit of a potential introduction of a novel technology.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.4.3.4.2 Change from compliance based to performance based – or the other way around [option b]

This option supposes a good knowledge of the potential influence to the end effect due to a particular technical choice in terms of specification, design, implementation, processes. This knowledge is based on the use of appropriate risks models with sufficient data regarding the definition and behavior of safety barriers. In a context of Total aviation, the interface between risks models according to the types of accidents/ incidents (e.g. CATS, AIM) need to be consolidated and sometimes detailed. Moreover a good understanding about the use of service history data with justified assumptions should facilitate the performance based approach.

2.4.3.4.3 Proof of concept (integrated process between Authority and manufacturer) [option f]

As part of performance based process, the proof of concept in ATM can be understood as the demonstration that a change of an Operational Concept has a real safety benefit and does not degrade safety barriers. SESAR safety methodology (SRM Safety Reference Material) proposes an approach combining “success” & “failure” based on functionality, performance and integrity aspects. This methodology and the related process could be used as reference with this option. However the fact that even safety criteria seem to be easily identified according to identification of relevant precursors, the notion of emerging risks need to be better investigated. The influence model(s) and interaction on the precursors should be improved in a context of total aviation.

Considering standardisation or AMC aspects, the proof of concept should consolidate and enlarge the validation of standards for some of the elements of concept selected.

Moreover a proof of Concept should be useful to “validate” the benefit of a new technology.

2.4.3.4.4 Make use of qualified entities [option d]

This option is already used in ATM through the EC 552/2004 regulation (Interoperability Regulation) [32]. The interoperability Regulation allows Member States to appoint notified bodies that are entitled to provide conformity assessment services, to manufacturers and/or air navigation service providers in relation to their verification of compliance obligations. The purpose of the certificate is to clearly identify which verification tasks have been accomplished and mentioning reservations, if any. The certificate is not to be confused with the EC declaration to be drawn up by the manufacturer or ANSP. In particular, it is to be noted that the responsibility to assess and declare compliance with the provisions of the interoperability Regulation lies with the ANSP.

2.4.3.4.5 Certify applicants i.l.o. products (Authority could leave more to the level of the organisation) [option e]

This option is already used by industry in order to improve its maturity (e.g. ISO certification, Capability Maturity Model like iCMM from FAA or CMMI from DOD).

For safety the notion of SMS Safety Management System is already defined in ICAO material (e.g. SMS Safety Management Manual) and EASA regulation. At the time being airlines and ANSPs are formally requested to implement a Safety Management System. However for the benefit of interface management between service

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

providers and industry, some recommendations regarding the extension of a SMS for industry could be envisaged and certainly useful for an improvement regarding roles and responsibilities.

Some frameworks exist for safety:

- Extension of CMMI to include processes areas “safety management” & “safety engineering” (maturity level 3)
- Extension of iCMM to include activities for safety & security.

These materials support a certification of organizations according to the definition of levels of maturity (the level 5 supposes that all the processes are measured and optimized through the organization). It could be used as confidence regarding “backing evidence”.

Moreover some SW standards like ED153 from EUROCAE [20] and consistent with EUROCONTROL safety methodology (SAM) [15] proposes a mapping between SWAL objectives and CMMI requirements.

As a conclusion, even Capability Maturity Models are not “safety standards”, this kind of framework should be a good support for providing confidence to support safety arguments (“backing evidence”).

2.4.3.4.6 No changes but improve existing processes [option g]

Processes improvement can be performed according to Capability Models. Safety assessment and certification can be streamlined by considering only safety arguments with their objectives/ requirements focused only on technical/technological aspects of the products regarding the identified risks.

However an improvement should be performed regarding the problem of rigor of evidence to provide in consistency with the severity classification. This rigor of evidence shall be in line with the safety monitoring activities (e.g. analysis of root causes of safety occurrences).

2.4.3.4.7 ‘Cross-domain’ fertilisation [option h]

This option could be envisaged regarding the following aspects:

- Technological benefit for safety,
- Broader safety approach including “success” and “failure” approach.

The safety assessment of a technology could be reused between domains. For example the SW standard DO178C used for airborne systems and having addressed the way to introduce and assess the SW object technology, could be reused with profit for ground systems as guidance material and recommendations.

The broader safety approach “success” and “failure” as used in SESAR could be beneficial for other domains of a total aviation system (not only ATM).

2.4.4 Summary of proposed options from the ATM perspective

In summary, the approaches proposed are presented in the following table, along with the main advantages and disadvantages of each.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

ATM Systems and Procedures

Table 1 – Summary of proposed options from the ATM perspective

Approach	***Main category***	***Key Advantages***	***Key Disadvantages***
Uniform enforcement of safety cases across ATM	Do not change	Uniform, clear understanding of level of safety and assumptions	Limited safety improvement
Application of safety argument approach across all domains	Cross-fertilisation	Uniform, clear understanding of level of safety and assumptions in all domains	Significant cost of adopting new approach across domains
Adoption of safety argument approach for TAS	Integrate all domains	Single cohesive safety argument for TAS Impact on each domain limited	Some cost in developing and maintaining overall model
Adoption of proof of concept across all domains	Proof of concept	Early increased confidence in success of concept	Limited impact on overall certification model
Compliance based certification of ATM products	Performance vs compliance	Easier to bring products to market	Constrains product innovation
Certification of applicants	Certify applicants	Reduced (external) certification burden	Decreased confidence in products

ATM Ground Industry perspective

The proposed options are summarized by presenting main advantages and disadvantages of each.

Table 2 – Summary of proposed options from an industry perspective

Approach	*Main category*
The certification process should be applicable whatever the domain (airworthiness, ATM…) by assuming consistency through traceability with related regulatory frameworks (e.g. in terms of severity classification, assurance levels allocation, objectives gradation and use….)	Option [a] Integrate all domains within the Authority (EASA)
The new adapted certification process should clarify the impact of the use of a new technology	

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Approach	*Main category*
The new adapted certification process should include requirements for an AMC according to the considered domain (ATM, airworthiness…).	
The new adapted certification process should include a generic part dedicated to the principle of apportionment of risks and a specific part more dedicated to reflect the specificities of these risks according to phases of flight (e.g. in line with safety occurrence data from risks models like number and diversity of precursors). The required effort for both parts should be proportionate to the level of risks.	Option [b] From compliance to Performance based
The new adapted certification process should reflect the impact of a change and assumptions about the condition to use the service history.	
The new adapted certification process should clarify the impact of the use of a new technology	
The new adapted certification process should contain consideration about efficacy criteria of kind of mitigation means based on safety risks models justifications.	
The new adapted certification process should include requirements in terms of transparency and clear responsibilities between stakeholders regarding safety monitoring and safety occurrences reporting.	Option [d] Qualified entities
The new adapted certification process should provide clear regulatory references and justifications about the criteria to authorize products/ operations to be certified (e.g. delegation arrangements)	
The new adapted certification process should reflect the benefit of continuous improvement culture through the Safety Management System whatever the stakeholders	Option [e] Certify applicants
A new adapted certification process should include the relationship and condition of reuse (assumptions, limitations) of safety case and certification folder.	Option [f] Proof of Concept
The new adapted certification process should include a generic part dedicated to the principle of apportionment of risks and a specific part more dedicated to reflect the specificities of these risks according to phases of flight (e.g. in line with safety occurrence data from risks models like number and diversity of precursors). The required effort for both parts should be proportionate to the level of risks.	
The new adapted certification process should reflect the impact of a change and assumptions about the condition to use the service history.	
The new adapted certification process should clarify the impact of the use of a new technology	

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Approach	*Main category*
The new adapted certification process should include requirements for an AMC according to the considered domain (ATM, airworthiness…).	
For completeness of Risks assessment it is necessary to refer to the global life cycle (sources of risks issued from a reference set of processes/ activities). The certification process should cover the whole reference ANS life cycle.	Option [g] Improve existing processes
The new adapted certification process should provide requirements and rationale regarding the rigor of evidence to support the demonstration	
The new adapted certification process should refer to "safety a priori assessment" (classical safety analysis) and "safety a posteriori assessment" (service history) with a sufficient flexibility and comparison criteria.	
A new adapted certification process should include the relationship and condition of reuse (assumptions, limitations) of safety case and certification folder.	Option [h] "Cross-domain" fertilization
The new adapted certification process should clarify the impact of the use of a new technology	

Main category	Key advantages	Key disadvantages
Option [a] Integrate all domains within the Authority (EASA)	From AMC point of view the integration of all domains within the authority should be a good condition for development of consistent means to reduce risks	
Option [b] From compliance to Performance based	The use of appropriate risks models (based on historical data) for a total aviation context is a prerequisite to develop a relevant performance based approach (right balance between performance and compliance based)	
Option [d] Qualified entities		The use of qualified entities for verification tasks impose an additional level of stakeholders and is a potential handicap regarding development of safety culture of the involved industry supplier.
Option [e] Certify applicants	The development of a continuous improvement action plan in order to	Risks of no improvement about recognised AMC definition

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Main category	Key advantages	Key disadvantages
	demonstrate a safety maturity is a good prerequisite to delegate the responsibility of self -"certification/ approval"	
Option [f] Proof of Concept	Proof of Concept should facilitate in early steps of the life cycle an assessment of changes by focusing efforts on most important risks areas and by including benefit of technological enablers . Thus AMC characteristics should be highlighted as well.	
Option [g] Improve existing processes	Rigour of evidence more in line with safety monitoring (root causes analysis of safety occurrences	
Option [h] "Cross-domain" fertilization	The success and failure approaches are applicable whatever the domain (total aviation context)	

Key issues to be addressed independent of the approach adopted

The discussion and analysis above has identified a number of key issues which need to be addressed whatever certification approach is adopted.

- Interfaces between components to be approved are a key area and any scheme adopted must ensure that any assumptions, dependencies or restrictions are properly captured and managed.
- The success case (considering the positive impact of introduction of elements into the system) must be properly considered in the approvals approach.
- Existing approaches suffer from a number of weaknesses in terms of fragmentation, confusion over accountability, complexity and duplication of regulations, lack of transparency and lack of harmonisation. Any new approach proposed should aim to make significant improvements in these areas.
- The certification approach should be clearly linked to the appropriate lifecycle phases, and the possibilities of early engagement should be considered.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

2.5 Perspective of an airport

Airport operations cover a multitude of activities and disciplines that relate to or can impact the safety of flight such as:

- Emergency and other Facilities, e.g. rescue and fire fighting, snow clearance, de-icing, bird control, etc.
- Management of ground movements, e.g. vehicles and 3rd parties
- Management of infrastructure including, runway lighting, safeguarding of approach and departure surfaces, clearance of movement areas, etc.
- Aerodrome Maintenance including upkeep of signs and markings, repair of movement areas, etc.

Aerodromes are normally certified through a process of licencing. In principle a licence is granted if the NSA is satisfied of the following fundamentals.

- The applicant (aerodrome owner/operator) is competent based on previous experience of operation, available equipment and arrangements for organisation, staffing, maintenance, etc. of the aerodrome and its services.
- The aerodrome is safe for use by aircraft taking account of the physical environment of the aerodrome and its surroundings including buildings and terrain.
- All necessary information, procedures and instructions are documented and available to enable operating staff to perform their duties, i.e. the Aerodrome Manual.

Other specific acceptance criteria may be applied such as aerodrome perimeter security, rescue and fire-fighting equipment specifications, etc. or the NSA may impose additional criteria if the applicant is new or untried.

The licencing process includes both general performance based requirements and regulations as well as prescriptive specifications. For example within the UK the licencing process is defined within CAP 138 [38] and covers all of the aspects mentioned above as well as prescriptive specifications on a wide range of aspects such as:

- Aerodrome Safety Management Systems
- Low visibility procedures
- Fire fighting equipment, fire stations, etc.

The approval process also requires the production of a safety case similar to that described for the ATM domain. For example, the UK CAA provides guidance on conducting safety assessments and producing safety cases for aerodrome operators and ANSPs in CAP 760 [33]. EASA is currently finalising draft implementing rules for Authority, Organisation and Operations requirements for Aerodromes currently issued as NPA 2011-20 [34]. A new EU regulation is expected by the end of 2013. It is expected that this will promulgate current good practices (including safety assessment and safety case production) across all of Europe. As these changes are already in progress, there will be little appetite or opportunity for further changes in the airport domain at this level, although there may be opportunity to influence the detailed implementation.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

The airport domain therefore has a maturing approach to licensing of applicants (airport operators) rather than any specific products used at the airport. The key approaches to learning from this for the overall aviation system are:

- **Option a: No change from current EASA approach, but adopted good practices from other domains and/or States, and ensure enforcement**: this is underway already in the adoption by the EU of common approaches on licensing of airports; this could be enhanced by ensuring that the lower level good practices guidance is applied across all States; the guidance may require adaptation to fit the current practices in other states. There is also the opportunity for education and training as the other states adopt the new regulations.
- **Option b: Cross-fertilisation**: other domains could review the processes currently used by the airport domain and consider the extent to which they could learn from and adopt the licensing approach used by the airport domain, for parts of the system which are amenable to licensing. Likewise, the airport domain could benefit from good practices in the other domains.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

3 Summary of the new approaches

In the previous Section, new and innovative approaches were suggested from the perspective of several different domains. This Section provides a summary that can be made of these new and innovative approaches to certification, taking all suggestions into account. Also, it provides cross-reference between the options identified in the previous Section and the consolidated approaches presented here.

3.1 Integrate all domains within the Authority

When integrating the different domains in the Authority, certification projects with more than one domain involved (e.g. product certification, operations, ATM) will benefit from a more joined approach. Conflicting requirements between for instance certification and operations can be identified on time and shared solutions developed. Moreover, given a closer cooperation between different aviation domains the probability that conflicting requirements are developed will probably decrease.

3.2 Change between “Performance based” and “Compliance based”

This option comes down to enforcing more compliance-based processes by means of performance-based elements, and more performance-based processes by means of compliance-based elements.

This could be done on a voluntary basis by industry instead of using required compliance methods.
A performance based requirement structure could accelerate the certification of novel products for which detailed prescriptive requirements are not available. A Proof of Concept (see also change f) can be part of the performance based method. Performance based requirements do not mean the total abolishment of Acceptable Means of Compliance. Certain standardization in how compliance is shown will greatly help the industry to speed up processes. Authority and Industry must work together in the development of AMC material. Performance based certification can result in the authorities keeping a distance from the development and certification process. This can result in a lesser knowledge of the technology. In the end the authorities must be able to agree the means of compliance used by the applicant, which needs a thorough experience. The authority will have to make sure that the experience of its personnel is adequate.

Also, a more compliance based approach may be followed where currently a performance based approach is followed.

3.3 Abolish all certification by Authorities and transform into a voluntary compliance

Simple systems could be fitted in simple aircraft if it meets the appropriate ETSO (European Technical Standard Order) and provided the manufacturers’ installation manual contains sufficient data for non-complex aircraft. If the safety risk of the new equipment is considered minimal with a relatively high safety benefit, this

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

approach could be an acceptable way of working. However, guidance for how these high safety benefits can be predicted, assessed, and measured should made available. In particular, the effect of the loss of the equipment and the effect of misleading information provided by the equipment would need to be assessed and taken into account in the overall assessment. Furthermore, it may be difficult (e.g. for the ETSO manufacturers and/or the aircraft operator) to prove the safety benefits for a given equipment, unless the installation of this equipment is confined to specific products for which the aircraft configuration would be known and controlled as well as confined to specific types of operations, which would significantly decrease the advantage of this option.

The drive to produce a safe product might be generated by the commercial value of safety and/or the insurance companies that balance premiums with risk.
This option will most certainly reduce the cost of certification activities. The big question is whether the required safety enhancement will be achieved with this approach.

3.4 Make more use of competent (certified) entities

This proposes more use of competent (certified) entities to supplement the workforce of the authorities. This can be done under the supervision of the Authority or by delegating the authority to these (certified) entities.
This option is already put in motion by the Authorities. As most Authorities are scaling down their workforce, they have to rely more and more on Qualified entities. These can be National Authorities (in the European arena) or commercial and non-commercial bodies. National Authorities are already used extensively by EASA. A tendering process is already started by EASA to contract Qualified Entities. It is not yet clear how much EASA is willing to outsource to these entities. For the short term this is probably a very powerful means to prevent delays in the certification process and to perform the job with enough competence. A risk for the authority is that competence, knowledge and experience will be vested in these entities instead of the Authority. Extensive auditing of the entities needs to be performed.

3.5 Certify the applicants instead of their products

This process is already put in place to a large extend (DOA, POA etc.). The same provisions as under 5) above must be taken into account.

3.6 Proof of Concept

First of all it will be important to use a similar definition of what Proof of Concept actually means.

The following definition is here proposed (cf. Section 2.3.4): A proof of concept (POC) is a demonstration whose purpose it is to verify that certain concepts or theories have the potential for real-world application and will be certifiable. For this purpose a POC uses a prototype (equipment or procedure) that is designed to determine this potential by testing. This prototype may be an innovative, scaled-down version of the system or

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

operation intended to be developed. In order to create such a prototype, tools, skills, knowledge, and design specifications may be required. A PoC can be part of a Performance Based certification method. For this, the result/outcome of Proof of Concept exercises or trials should be the requirements that need to be fulfilled in order to certify the product as well as a more developed specification. A PoC could be profitly combined with a Performance based certification process.

3.7 Enforce existing rules / improve existing processes

In this option we keep the certification process as it is, focus on correct implementation in the different member states, and have a look at possible improvements *within* the process.

3.8 Cross-domain fertilisation

Also in this option no major changes or innovations are made, but the best practices in certification in each of the different domains are used to improve weaker areas in the other domains.

3.9 Consolidation of the identified options

For completeness the following Table 3 provides a mapping of the options identified in the different subsections of Section 2 onto these 8 Options.

Table 3 – Consolidation of the identified options

	Integrate all domains in authority	Performance <-> Compliance	Voluntary compliance	Use competent (certified) entities	Certify applicants instead of products	Proof of Concept	Enforcement & improvements	Cross-domain fertilization
2.2 Air operator			b, c	d	F		a, e	
2.3 Aircraft & Products	a	b	c	d	e	f		
2.4 ATM & ANSP	c	e			f	d	a	b
2.4 Ground equipment	a	b	c	d	e	f	g	h
2.5 Airport							a	b

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

4 Evaluation and selection of the most promising approaches

4.1 Introduction

In the previous Section several new approaches have been identified that could be applied to certification processes. Within ASCOS only the most promising of those approaches are likely to be further elaborated in detail [36]. Therefore there is a need to down select from the entire list of potential approaches those that are considered most promising for further detailed analysis and evaluation. For such down select it is necessary to define criteria that can be used to value the pros and cons of each of the identified approaches in an objective and transparent way. At this stage in the ASCOS project, the evaluation is not intended to be exhaustive, and is based on the views of the experts involved. Further evaluation of chosen adaptations will be addressed in later deliverables of ASCOS WP1. The evaluation criteria addresses the essential characteristics of the certification process, and at the same time estimates the impact that new processes have on each of the criteria, based on the high level description of the new processes, as provided in the previous Section.

Sections 4.2 and 4.3 describe the evaluation criteria and the evaluation process followed. Next, Section 4.4 describes the actual evaluation and selection.

4.2 Evaluation criteria

Before presenting and discussing selected evaluation criteria it is important first to define what the objectives of the considered certification processes are, in order to have a common understanding of what is intended to be achieved. For the purpose of the present study the general objective of certification processes is: to ensure acceptable safety of new systems, equipment, operations or procedures, when put in operation, and to ensure continued safety of these items during their operational life.

Clearly, any new certification process will have to perform such that this objective is being achieved.

Secondly, it has to be assessed how the costs are defined that have to be incurred in order to achieve the defined objectives. As with any evaluation, the basis is formed by an assessment of the costs relative to the intended benefits. In this context the term “costs” has a wider meaning than the direct financial costs. It can be any item that influences the efficiency or effectiveness of the process, like throughput time or the required quality of the involved personnel. Each of such items could eventually translate to a direct financial cost, but beforehand the relation is mostly difficult to estimate. For instance, a new method could lead to a shorter throughput time of the certification process, while achieving the same objectives at the same direct costs. Although in such case no difference would exist in benefits and direct costs, the reduced throughput time could lead to earlier approval and introduction of the item under certification, resulting in earlier achievement of reduced operational costs or improved operational safety. Therefore, reduced throughput time would have to be assessed as a positive attribute of the new process.

Based on such considerations the evaluation criteria are subdivided into primary criteria that are directly related to direct costs and benefits of the certification process, and secondary criteria that are related to indirect safety or cost attributes. The primary criteria are related to the traditional cost/benefit analysis and the secondary criteria are related to cost or safety attributes of elements that are characteristic for the proposed approach.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Therefore, the primary criteria are:

1. Cost benefits

The evaluation criterion "Cost benefits" relates to the direct costs of the certification process. This includes the costs of all involved processes and activities, both to the applicant and the certifying authority. The way of attributing costs to either party is not of importance here. Eventually all costs are burdened to the customer or the tax-payer. The assignment of costs to either party is considered a policy decision, and therefore is not considered an attribute of the certification process itself.

When addressing costs of certification processes a clear distinction has to be made between development costs and certification costs. Sometimes this distinction can be somewhat arbitrary. For instance an aircraft manufacturer, trying to certify a new aircraft model will inevitably have to conduct a flight test program. One could argue that the complete flight test program is performed to eventually achieve the certification of the aircraft and that therefore all associated costs are "certification" costs. However, one could also argue that the flight test program is part of the development programme, and that only a dedicated part of flight test program is directed to certification and as such directly involves the certifying authority, either by witnessing the flight test or approving flight test results. In the context of the present study the latter position will be taken to assess costs, by estimating the costs of the pure certification related costs. Any other cost will be regarded as development cost that will be incurred by the applicant, independent of the certification approach.

The baseline for the cost estimate is the present situation. In many cases these costs are currently perceived as high, but it is unclear how high they in fact are. Therefore, in assessing costs it will be necessary to use a relative comparison, looking only to the changes in the process, and the assumed impact these changes will have on the direct certification costs.

2. Safety benefits

The assumed safety benefit is an interesting one. Any new certification approach will be required to satisfy the defined safety objectives. Without changing the safety objectives it is unlikely that a new certification approach will achieve another safety level than the current process. It could be envisioned that a new approach will achieve higher safety at equal cost. Of course this would have to be assessed as a positive characteristic. On the other hand, a new approach will never result in a lower safety level as the baseline process, as this would disqualify this approach, due to not reaching the required safety targets. Therefore in terms of safety a new approach can only result into a neutral or positive safety effect. Otherwise, it should be regarded as an invalid approach.

The proposed secondary criteria are:

3. Reducing throughput time

The throughput time is a very important attribute of a certification process. The general perception is that current certification processes are quite lengthy. Therefore, reduction of throughput time should be regarded as a positive attribute. To some extent throughput time affects the direct certification costs (time is money). It also determines the time duration in which new innovative systems or operations can reach the market, and can become effective. This may in turn relate to safety improvements that are becoming effective sooner, or to cost reductions that are realized earlier. Therefore reduction of throughput time may affect both safety and

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

costs. However, it should be noticed that overall benefits are only realized over a limited timeframe, namely the reduction in throughput time, and therefore the associated benefits are limited by definition.

4. Stimulation of innovation

An important characteristic of a certification process is its capability to accommodate innovations. Current certification processes are largely based on showing compliance with existing regulations. These regulations are mostly based on requirements that apply to existing system or operations, taking into account past experience (lessons learned). By definition such processes are not very flexible in allowing innovative systems or operations that may employ completely new technologies, for which no experience and thus no appropriate regulations do exist. As such current certification processes are considered to be conservative, which from a safety viewpoint is understandable. However, this conservatism may also impede or delay introduction of new safety features or cost efficiencies. Thus, while conservatism should not be regarded as a negative attribute by definition, it is clear that any new process that stimulates innovation and provides mechanisms that allow innovations to find faster implementation in practice should be favoured. Therefore, any barrier for innovation that can be removed from the process, while still ensuring safety, should be regarded as a positive characteristic of a new approach.

5. Reducing required expertise

Current certification processes are in general very complex processes. The current regulatory framework is an extensive system of rules, regulations, recommended practices, means of compliance, etc., that may even be different from country to country, or from continent to continent. Dealing with such a framework requires not only technical expertise but also an historic notion of the background of applicable regulatory requirements in order to be able to properly interpret the meaning of these requirements and to consistently assess compliance or non-compliance. This all requires not only substantial expertise, but also extensive experience before certification personnel is sufficiently qualified to perform certification activities. Due these requirements on certification staffing, qualified certification personnel is not easy to find, or require substantial training and education before they can be actually employed. Clearly, extensive costs can be involved to find or train these personnel. These training costs have to be amortized in the certification cost. Based on these considerations it can be expected, that any new certification approach that simplifies the process and/or would require a lesser level of expertise and experience, may potentially lead to cost reduction in the certification process. However, it should be noted that this cannot go at the expense of reduced safety. In assessing the required expertise, one should also not forget that high levels of required expertise may inherently also lead to high levels of efficiency that to some extent might offset the associated high costs. Therefore, in using the required expertise as a criterion to evaluate the certification process one should be aware that there is probably some optimum in the required level of expertise, that should preferably be readily available, but on the other hand of a sufficient level to be credible.

6. Reducing bureaucracy (for the Applicant, for the Certifying Authority);

Certification processes involve always some form of bureaucracy. This is inherent to formalized processes with hierarchical approval structures. Therefore, certification processes without some form of bureaucracy are

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

unthinkable. Nevertheless, the term bureaucracy often has a negative association, as it may relate to unnecessary regulations, inefficient approval processes or unduly complex administrative processes. Inevitably, bureaucracy will lead to some costs, either for the applicant or for the certifying authority. Therefore, any new certification process, that would streamline the involved bureaucratic processes, for instance by simplifying regulatory structures and/or approval processes, should be given credit. As the baseline certification process, and the associated bureaucracy, is well known, any new method should be evaluated with respect to relative changes it would bring in this area.

7. Interoperability with other domains

In the current practice, the certification and approval processes in the different domains (such as aircraft certification, operations, ATM and airports) differ (significantly) from each other. In some areas certification is mainly compliance based (as for instance in aircraft certification), while in other areas the approval process is largely performance based (as in ATM where the overall target for ATM contribution to accidents is specified in ESARR4, and contributions of sub-systems can only contribute to fractions of this overall target). While it could be envisioned that specific approaches are optimal for a specific domain, it is most likely sub-optimal if total aviation safety is regarded. The main issue here is that when each domain uses its own methodology problems may arise at the interfaces between the various domains. It may become unclear how for instance an aircraft system that is certified against a given aircraft certification requirement might affect the ATM contribution in aircraft accidents. A good example is the TCAS system that was certified as an airborne safety net to prevent mid-air collisions. However, during the TCAS development it was never fully realised to what kind of inter-operational problems such system could lead with existing ATM procedures. This was one of the main causes of the Überlingen accident. Therefore, a positive attribute of a new certification approach would be when it would improve interoperability among the various domains, for instance by harmonizing the methodologies in the various domains, or specifically addressing the interfaces between the various domains.

8. Early stakeholder involvement

Certification processes involve inherently a large number of stakeholders, such as manufacturers, airlines, ANSPs, airports, EASA, FAA, etc. It is not likely that any new process could have an impact on the amount of involved stakeholders itself. However, it could have an effect on the actual involvement of stakeholders or on the communication and information exchange among stakeholders. To some extent this relates to interoperability, as discussed under point 7. However, it also relates to the efficiency of the whole process. When stakeholders are involved early in the process and efficient communication among stakeholders is promoted (“speaking the same language”) this should be considered as a positive attribute of a new process.

9. Harmonisation and standardisation

For about 40 years a lot of effort has been put in international harmonisation of rules, standards and methods that are used for certification. In particular the harmonisation between Europe and the United States has got significant attention. Also ICAO and organisations like RTCA and EUROCAE play an important role in the world-wide harmonisation and standardisation of the regulatory framework and the associated means of compliance. Although the current regulatory framework may not be perfect, and full international

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

harmonisation has not been accomplished, it must be realized that the current state of affairs has been achieved at the cost of significant efforts and time. Any new certification process or method has the danger of de-harmonization, in case it would not be widely accepted. However, the new process could also promote harmonisation by streamlining existing processes. If this would lead to world-wide efficiency improvements, regardless of local situations, this also could lead to world-wide acceptance and harmonisation. Based on these considerations, a new certification process should be evaluated with respect to its potential to improve harmonisation. Clearly, any perceived de-harmonization would have to be seen as a negative characteristic.

10. Acceptable Means of Compliance definition

A regulatory framework does not only set the standards, but will also need to specify certain guidelines (best practices) and acceptable means to show compliance with the certification requirements. These means of compliance are preferably clear to understand (in terms of objectives and activities to be performed) and not susceptible to subjective interpretation. Implicitly, a new certification process will have to take into account how suitable AMCs can be defined. When a new certification process would lend itself to easily define AMCs this would have to be regarded as a positive attribute. As an example, performance based regulations require usually that it is demonstrated that a given target level safety is achieved, but leave the way how this is demonstrated largely open. This may seem to be a good property of such regulations because it provides the applicant more freedom to incorporate innovations and tailor evidence. However, such process would lend itself less for a clear description of the acceptable means of compliance, and therefore results could be susceptible to interpretation (e.g. the impact of assumptions on the end result). Also, it would a priori not clear whether provided evidence, intended to show achievement of the target level of safety, is acceptable for the certifying authority. This would therefore impose a risk to the applicant, whether certification can succeed or not. Therefore, the suitability of a new process to accompany its requirements with a clear set of AMCs should be used an evaluation criterion.

11. Level of difference with current requirements

Clearly any change in the certification process will have some level of difference with current requirements. At one end of the spectrum, the changes could be minimal, reflecting an evolutionary approach. At the other end of the spectrum the complete process could be redefined; the revolutionary approach. It is a priori difficult to say which approach is inherently better. By penalizing revolutionary approaches too much, the opportunity to incorporate real innovations could possibly be very limited. On the other hand it is unrealistic to assume that current certification processes, that incorporate the collective wisdom and past experience, would need to be completely re-designed. It should be noted that the significant safety improvements that have materialized in aviation have been achieved by virtue of a well-founded, slowly evolving, regulatory framework. Based on this experience, it can be assumed that an evolutionary approach in general will be favourable. Consequently, it should be rated positively when the level of difference with current requirements remains limited.

12. Ability to use retroactively

An important aspect of a new certification approach is to what extent it can be applied retroactively. Current aircraft designs may continue to be in operation for 40 years or more (f.i. the Boeing 737). During their lifetime

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

such designs are improved and upgraded on a continuous basis. Because, also the regulatory framework evolves during the lifecycle of such designs, the question may arise to what extent new standards should be applied to design upgrades and to what extent grandfather rights do apply. Often this is subject to a negotiation process between applicant and regulatory authority. The outcome of such negotiation process is sometimes considered as subjective or not transparent. Therefore, if a new certification process would be more suited to be used retroactively it is beneficial in defining a consistent certification baseline for design changes. This capability should therefore be rated as positive.

13. Promote human factor involvement

The main source for aviation safety risk is still human error. Reducing the possibility for human error will have an immediate positive impact on safety, and is inherently linked to the criterion 'safety benefits'. It is therefore important, and maybe even critical, to address human factors aspects as criterion as well. Although human factor aspects are increasingly incorporated in the present regulatory framework, it is still not considered to be fully adequate to further improve aviation safety. In case a new certification process would promote the incorporation of human factor aspects this would therefore be considered a positive attribute of the approach.

14. Possibility to delegate responsibilities to the Applicant

It is difficult to state that delegation of more responsibilities to the applicant is always a good development. There are positive aspects, namely that certification burden at the certifying authority is reduced, and that it potentially adds flexibility to the certification process. On the other hand, it leads to new responsibilities for the certifying authority, because the delegated responsibility has to be supervised and quality controlled. Also, it can be questioned whether delegation of responsibilities doesn't lead to erosion of knowledge and expertise at the certifying authority, and with that of the inherent certifying capabilities. Therefore, it is difficult to rate a new approach on its capability to delegate responsibilities. However, a general trend is visible that certifying authorities have a positive attitude towards further delegation of responsibilities. This is evident from increased attention on safety management systems, while direct supervision and inspections are reduced. Whether this is a favourable development or not is not a priori clear. However, if a new approach would be in line with the general trend to delegate responsibilities, this would have to be regarded as a positive attribute.

15. Feasibility

Feasibility: the outcome of the evaluation of all criteria.

4.3 Method of evaluation and selection

The evaluation is performed in a qualitative way, by using the terms of "very positive (++), positive (+), neutral (+/-), negative (-), very negative (--)" or a more applicable description depending of the specific evaluation criterion. A weighting scale of the different criteria could be developed, but at this very moment it is not used. The same counts for relative scaling. A score per criterion for each new approach provides an overview of how the different new approaches score on all different criteria. Most probably use of the ASCOS consortium partners will be sufficient to draw initial conclusions. A more thorough exercise (e.g. as part of ASCOS WP5) could involve ASCOS User Group members. This would allow validation of the scoring results and conclusions.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

In the following assessment of options quantitative values are used:

++ very positive → +2
+ positive --> +1
+/- neutral --> 0
- negative --> -1
-- very negative --> -2

A distinction is being made between the primary evaluation criteria and secondary evaluation criteria.

4.4 Evaluation of certification process adaptations

The scoring process is performed on the basis of the viewpoints of the following types of organisations, each represented by one of the ASCOS consortium partners (*in brackets*) involved in this study:

- Operations (NLR)
- Manufacturer (TR6)
- Certifying authority (CAAi)
- Aircraft/product certification (CertiFlyer)
- ATM systems and procedures (Ebeni)
- Airport (Ebeni)

The different scores are subsequently added. The results of the evaluation of the new certification approaches are presented below. First an overview is given of the 8 approaches that are evaluated. Next, the scores of these 8 options against the evaluation criteria discussed in paragraph 4.2 are presented.

Table 4 – Consolidated options for certification process adaptations

Option	
1	Integrate all domains within the Authority
2	Change between “Performance based” and “Compliance based”
3	Abolish all certification by Authorities and transform into a voluntary compliance
4	Make more use of competent (certified) entities
5	Certify the applicants instead of their products
6	Proof of Concept
7	Enforce existing rules & improve existing processes
8	Cross-domain fertilisation

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Primary evaluation criteria:

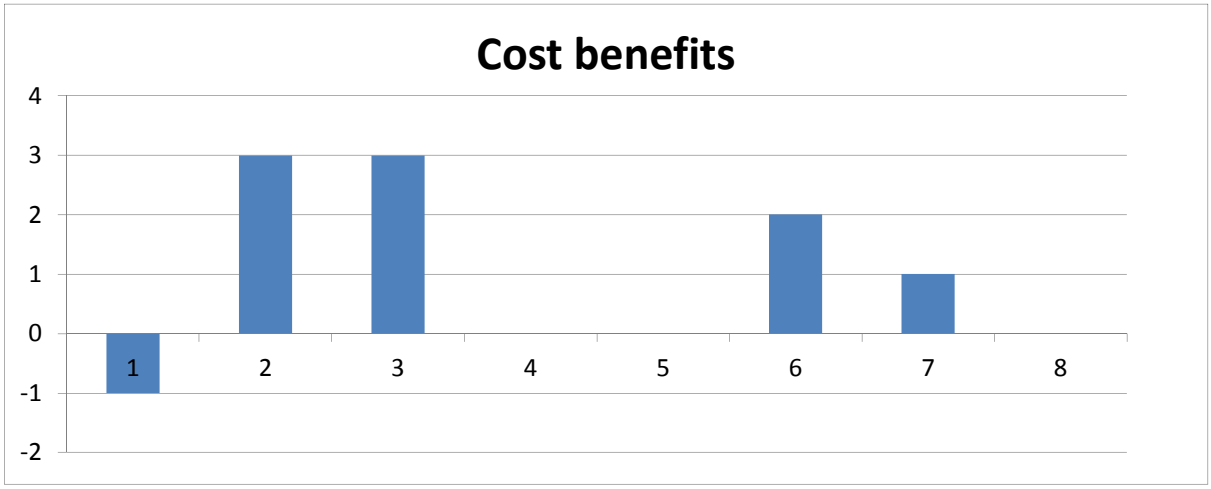

Figure 6 – Evaluation of options against criterion costs

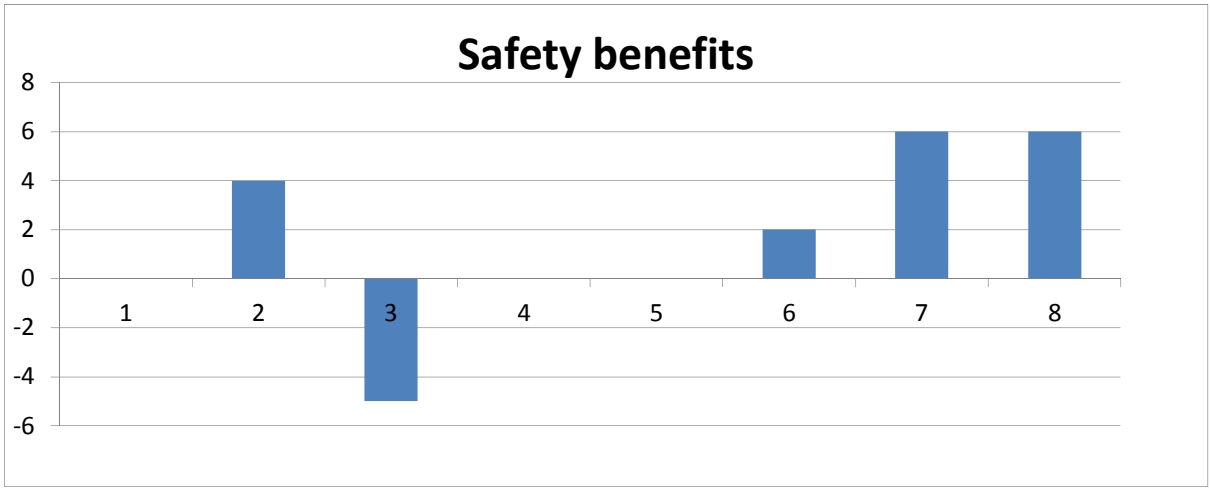

Figure 7 – Evaluation of options against criterion safety benefits

Secondary evaluation criteria:

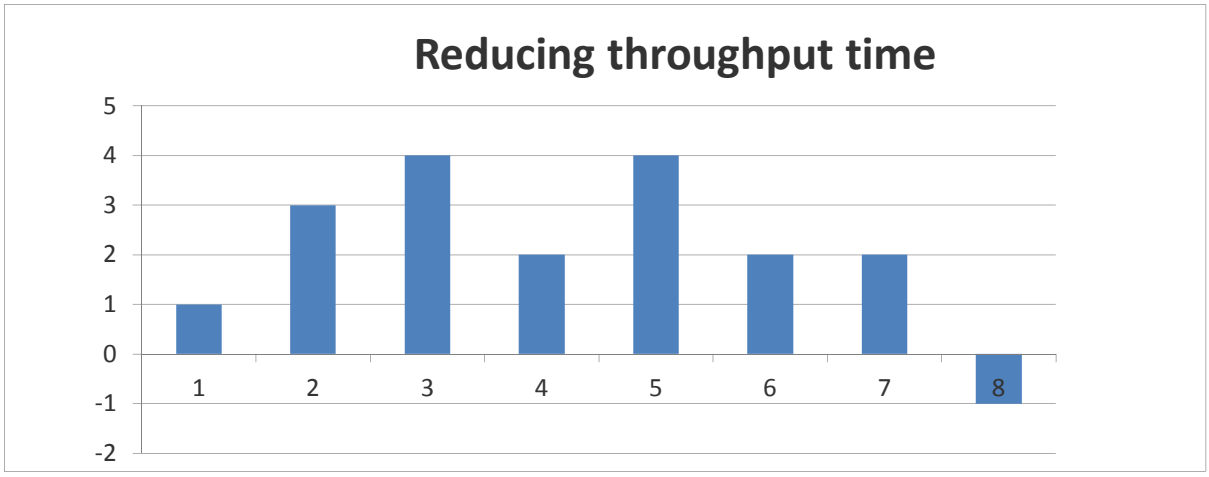

Figure 8 – Evaluation of options against criterion throughput time

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

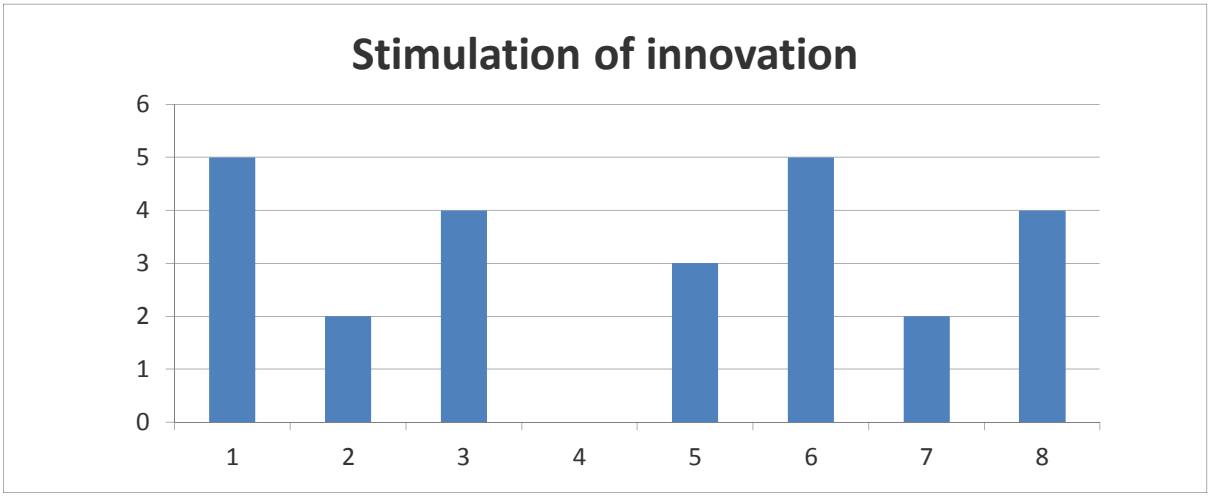

Figure 9 – Evaluation of options against criterion stimulation of innovation

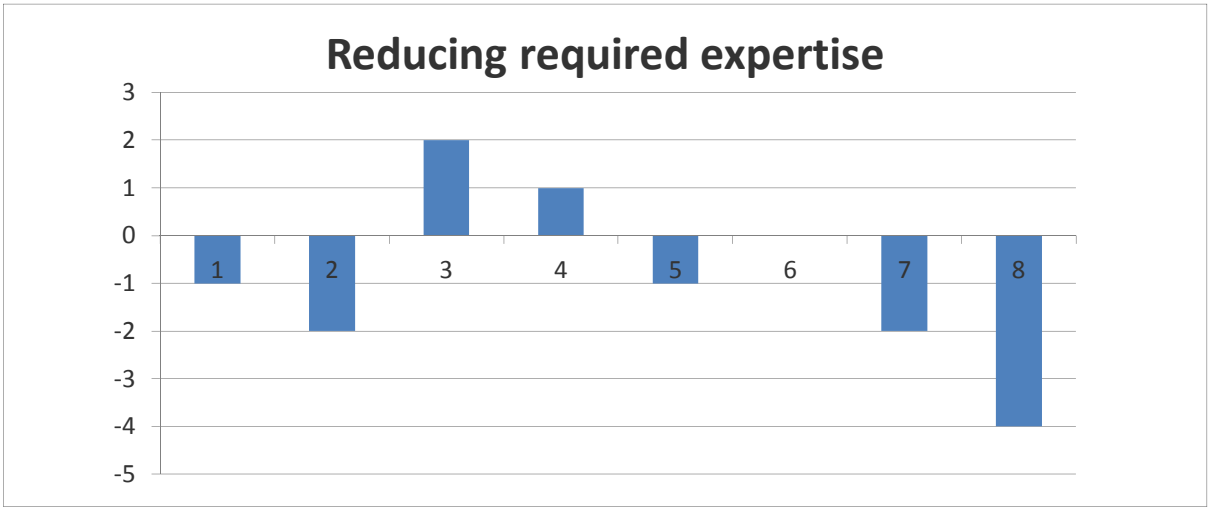

Figure 10 – Evaluation of options against criterion required expertise

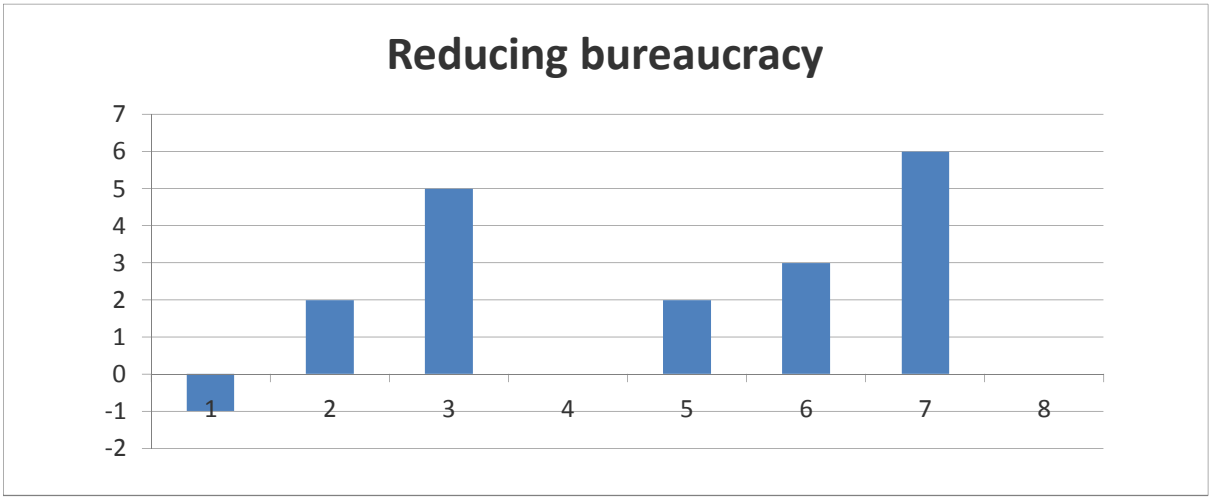

Figure 11 – Evaluation of options against criterion bureaucracy

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

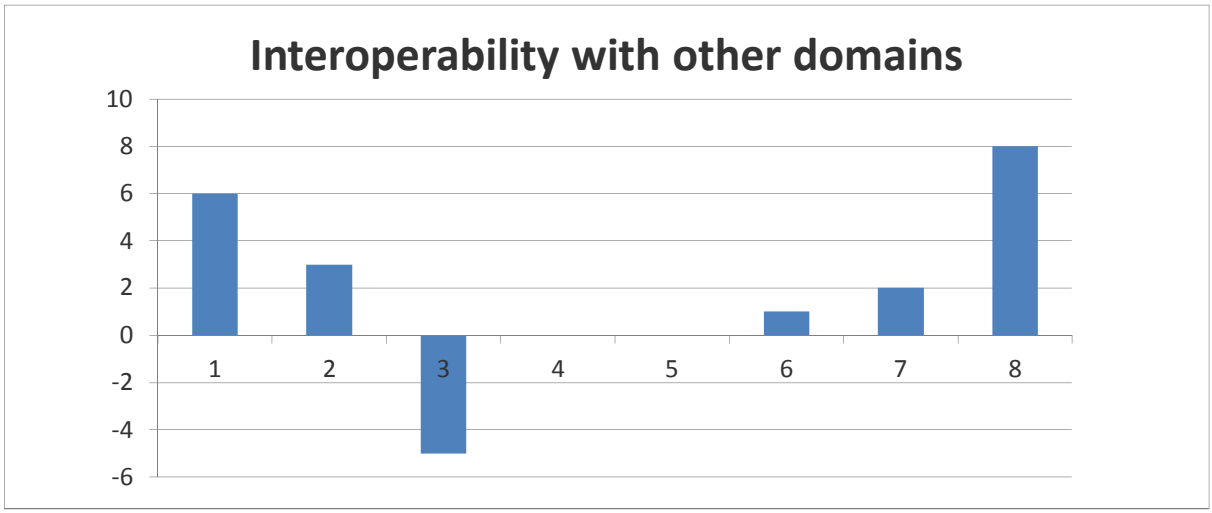

Figure 12 – Evaluation of options against criterion interoperability with other domains

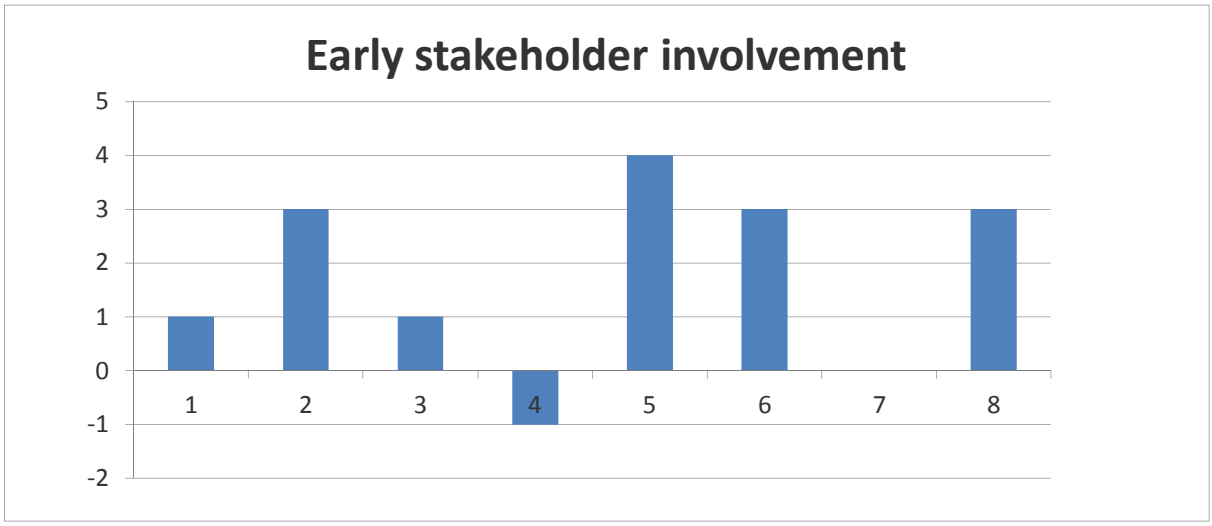

Figure 13 – Evaluation of options against criterion stakeholder involvement

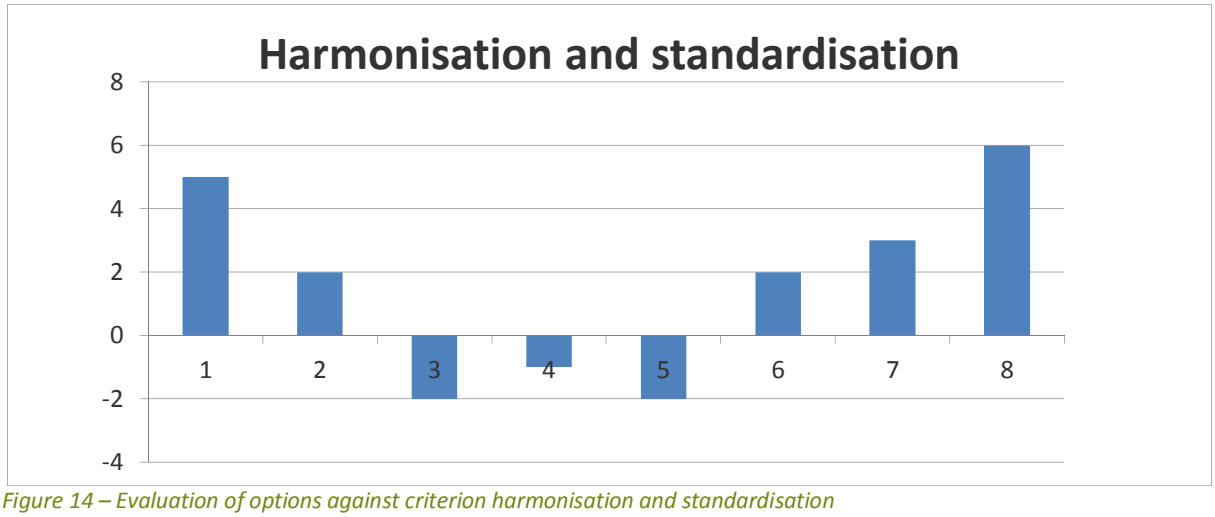

Figure 14 – Evaluation of options against criterion harmonisation and standardisation

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

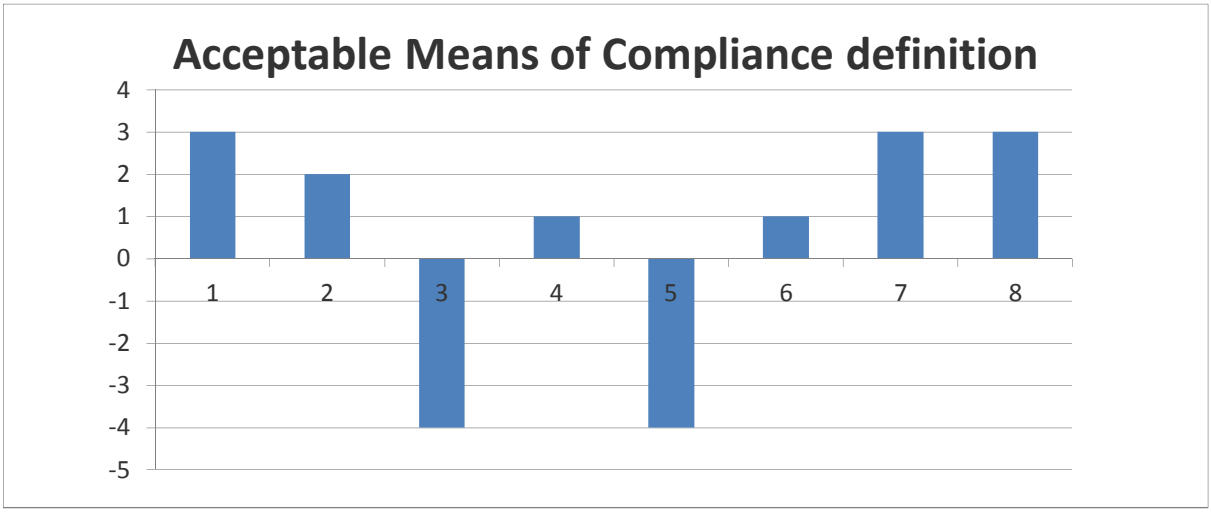

Figure 15 – Evaluation of options against criterion AMC definition

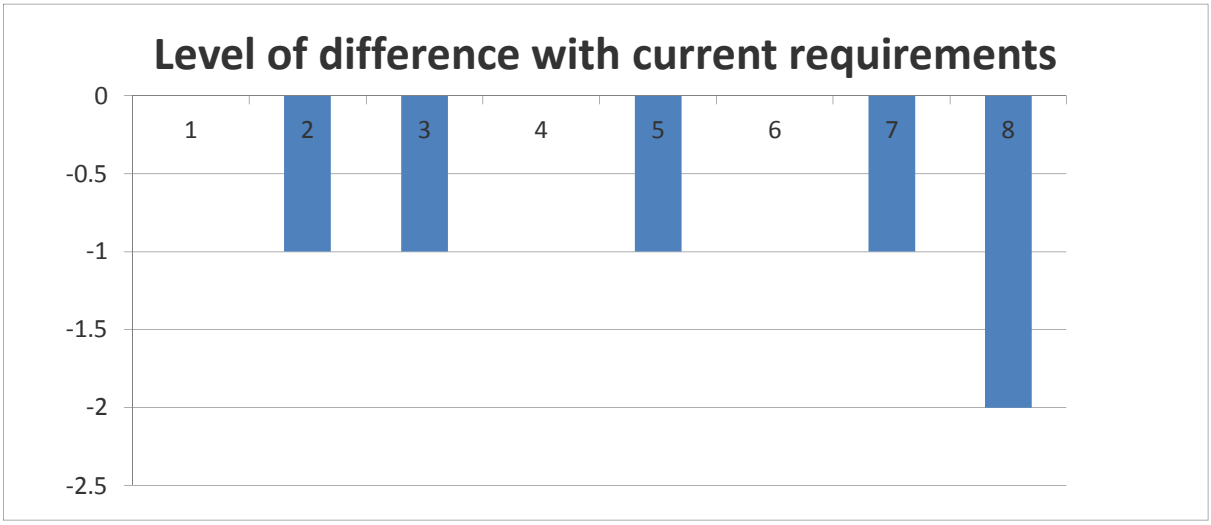

Figure 16 – Evaluation of options against criterion level of difference with current requirements

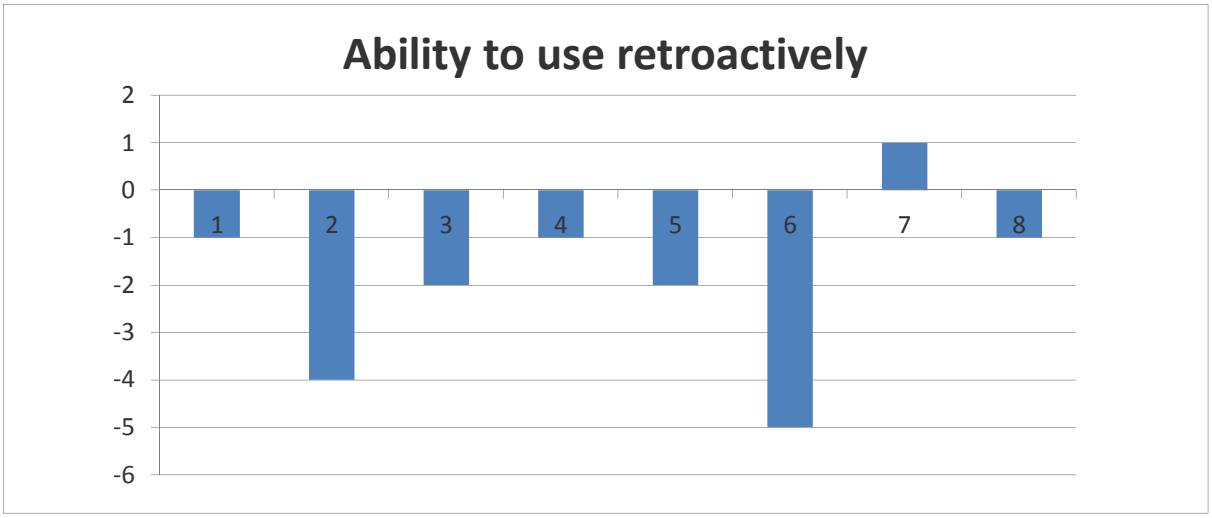

Figure 17 – Evaluation of options against criterion ability to use retroactively

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

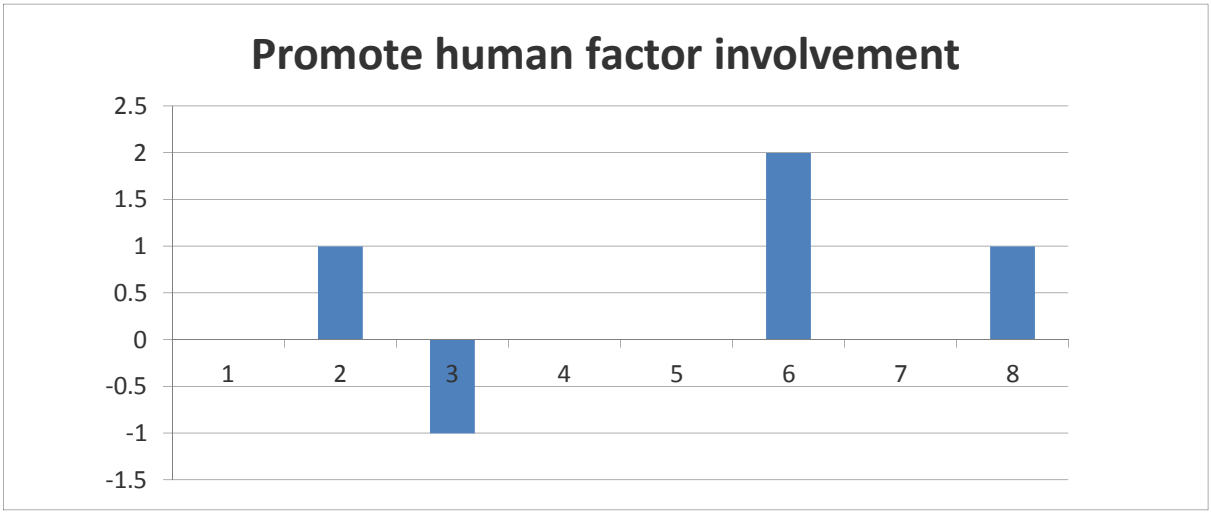

Figure 18 – Evaluation of options against criterion human factor involvement

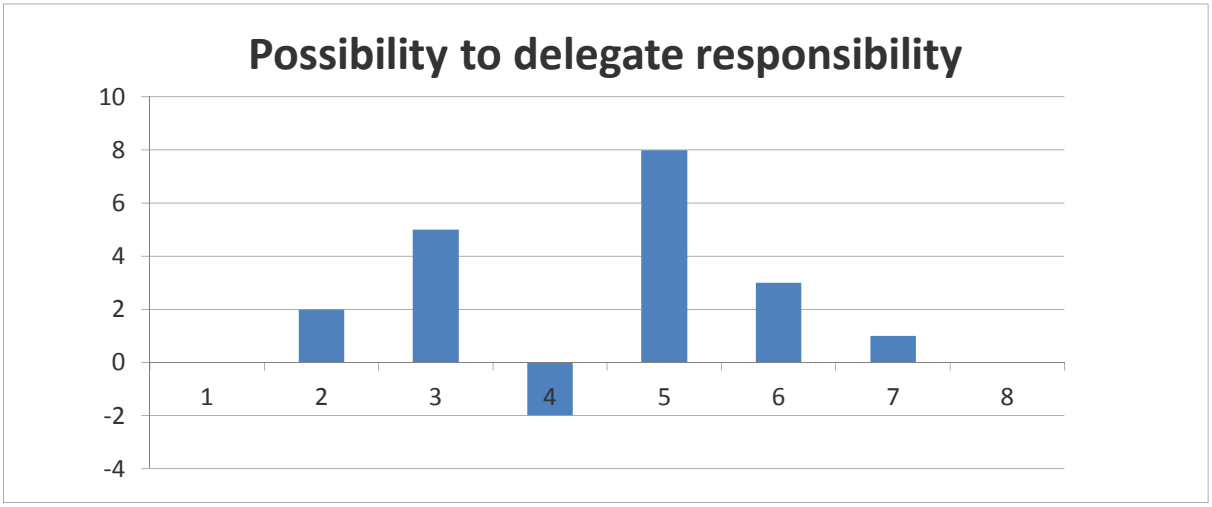

Figure 19 – Evaluation of options against criterion possibility to delegate responsibility

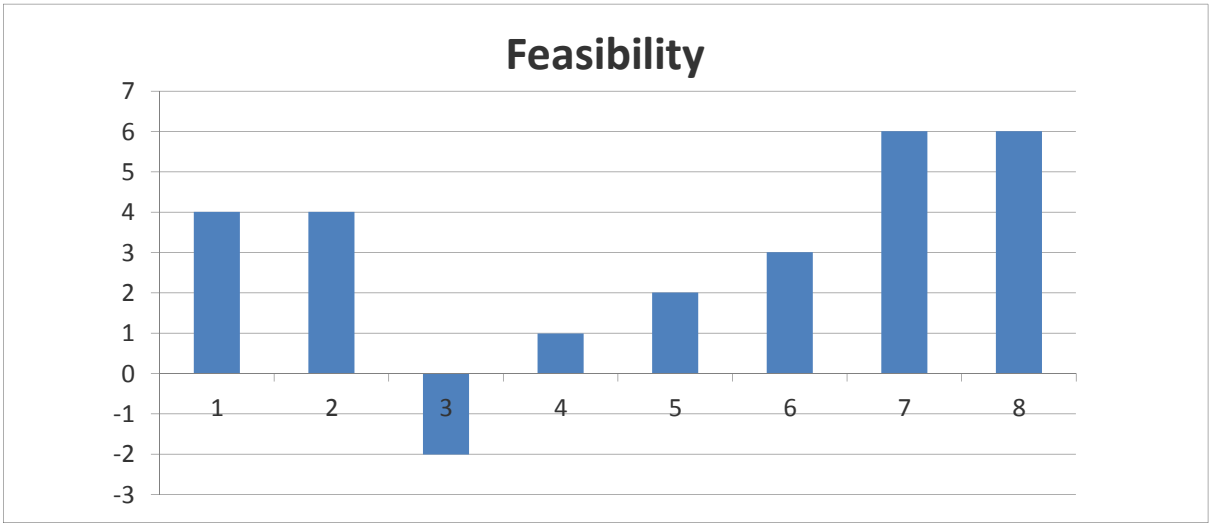

Figure 20 – Evaluation of options against criterion feasibility

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

4.5 Selection of the most promising certification process adaptations

From a safety benefit perspective, option 7 and 8 score best, followed by option 2. From a cost perspective, option 2 and 3 score best, followed by option 6. When both primary evaluation criteria (costs and safety benefits) are taken into account, options 2 and 7 are the most promising options, followed by options 6 and 8. When also considering the secondary evaluation criteria, these four options remain the most promising ones. Accordingly, the options here selected as most promising ones are:

- Option 2: Change between performance based and compliance based;
- Option 7: Enforce existing rules and improve existing processes;
- Option 6: Proof of concept approach;
- Option 8: Cross-domain fertilisation.

It is recommended to further develop the newly proposed certification approach on the basis of the selected most promising options. Specific guidelines to be considered and taken into account within the follow-up ASCOS activities regarding certification process adaptations are [37]:

- Avoid unnecessary change, recognising the good approaches already in place;
- Provide a generic certification framework encompassing the Total Aviation System (TAS);
- Use a common language across all domains based on safety argument concepts (e.g. argument-based as used in OPENCOSS), allowing flexibility to accommodate a variety of approaches across domains;
- Provide rigorous management of interfaces, both between domains and between the TAS and its environment, to ensure that all key safety issues are properly addressed and not lost at interfaces;
- Allow, within each domain, the new certification approach to evolve from the current approach by
    - keeping the existing approach where no change is required
    - learning lessons from other domains where this gives improvement
    - ensuring that bottlenecks and shortcomings are addressed by the proposed approach;
- Promote flexibility within each domain to allow introduction of new technologies or procedures
- Harmonise approaches between domains where this is advantageous or necessary
- Simplify certification processes, where there are:
    - demonstrable benefits and
    - no loss of confidence in the assurance of safety;
- Reinforce existing techniques where they are appropriate but not consistently applied;
- Provide a mechanism for identification and resolution of further bottlenecks and shortcomings;
- Introduce a bridge between the regulations for aircraft certification and Air Traffic Management;
- Take into account the electronic hardware more explicitly in the proposed approach;
- Consider the fact that less experience is gained by the flight crew when more automation is used.

Based on the outcome of ASCOS D.1.1 [35], this study has identified several applicable options in order to address the problem of shortcomings and bottlenecks regarding current certification processes, including the implementation of current safety regulatory framework in a context of Total Aviation System. Appendix A summarizes how the consolidated eight options address (part of) these shortcoming and bottlenecks.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

5 Conclusions and recommendations

5.1 Conclusions

To ease the efficient and safe introduction of safety enhancement systems and operations, a novel and innovative approach towards certification is felt to be required that:

- Is more flexible with regard to the introduction of new products and operations;
- Is more efficient, in terms of cost and time, than the current certification processes; and
- Considers the impact on safety of all elements of the aviation system and the entire system life-cycle in a complete and integrated way.

In view of this, this study has identified potential improvements to the existing certification processes from the viewpoints of several aviation domains. Next, these potential improvements have been consolidated into eight approaches that apply to the Total Aviation System, as follows:

1. Integrate all domains within the authority
2. Change between performance based and compliance based
3. Abolish all certification by authorities and transform into voluntary compliance
4. Make more use of competent (certified) entities
5. Certify the applicants instead of their products
6. Use of Proof of Concept approach
7. Enforce existing rules and improve existing processes
8. Cross-domain fertilisation

These eight options have been reviewed against a set of 15 evaluation criteria, the most important ones being safety benefits and costs. Secondary criteria used are throughput time, stimulation of innovation, required expertise, bureaucracy, interoperability between domains, harmonisation and standardisation, acceptable means of compliance definition, level of difference with current requirements, ability to use retroactively, human factor involvement, possibility to delegate responsibilities to the applicant, and feasibility. The initial review of the impact of these approaches suggests that the following options provide the most promise for achieving the aims of ASCOS with regards to enhancing certification approaches:

- *2. Change between performance-based and compliance-based or vice versa.* This option considers replacing compliance-based processes with performance-based elements and/or performance-based processes with compliance-based elements.
- *6. Proof of concept approach.* This option is based on a demonstration whose purpose it is to verify that certain concepts or theories have the potential for real-world application and will be certifiable.
- *7. Enforce existing rules and improve existing processes.* In this option, regulation and rules remain as is, but we focus on full and correct implementation in the different member states, and have a look at possible improvements *within* the certification process.
- *8. Cross-domain fertilisation*. In this option no major changes or innovations are made, but the best practices in certification in each of the different domains are used to improve weaker areas in the other domains.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

5.2 Recommendations

Different certification process adaptations have been defined, analysed, and evaluated. However, it should be realized that there are more options for change that could have been addressed. For example, focusing more explicitly on the introduction of connections (bridges) between different domains, where such connections are needed, and/or combination of product and organization certification (the latter is now indirectly covered in options 2 and 8). Also, it should be realized that other evaluation criteria exist and could have been used, such as constraints relating to public responsibility and ability to cope with future changes in the aviation system. The more automation is used, the less experience is gained by the flight crew when manual take over is necessary. This could impact the certification process of future automation technologies. Therefore, the use of one or more additional criteria that explicitly deals with future and emerging risks would have been beneficial.

It is recommended to further develop the newly proposed certification approach on the basis of the selected most promising options. It should be noted that these options are not mutually exclusive and the proposed adaptations to the certification process may comprise a blend of these options. This report only provides an initial view of the potential for improving the regulatory framework and supporting certification processes. It has deliberately taken a more "blue-sky" approach to looking for improvements. However, moving forward it is recognised that to achieve the aims of ASCOS any future certification adaptations must take the following into account [37]:

- Avoid unnecessary change, recognising the good approaches already in place;
- Provide a generic certification framework encompassing the Total Aviation System (TAS);
- Use a common language across all domains based on safety argument concepts (e.g. argument-based as used in OPENCOSS), allowing flexibility to accommodate a variety of approaches across domains;
- Provide rigorous management of interfaces, both between domains and between the TAS and its environment, to ensure that all key safety issues are properly addressed and not lost at interfaces;
- Allow, within each domain, the new certification approach to evolve from the current approach by
    - keeping the existing approach where no change is required
    - learning lessons from other domains where this gives improvement
    - ensuring that bottlenecks and shortcomings are addressed by the proposed approach;
- Promote flexibility within each domain to allow introduction of new technologies or procedures
- Harmonise approaches between domains where this is advantageous or necessary
- Simplify certification processes, where there are:
    - demonstrable benefits and
    - no loss of confidence in the assurance of safety;
- Reinforce existing techniques where they are appropriate but not consistently applied;
- Provide a mechanism for identification and resolution of further bottlenecks and shortcomings;
- Introduce a bridge between the regulations in different domains where needed, in particular between aircraft certification and Air Traffic Management;
- Take into account the electronic hardware more explicitly in the proposed approach;
- Consider the fact that less experience is gained by the flight crew when more automation is used.

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

References

#	Authors(s), Title, Year
[1]	FAA; Commercial Airplane Certification Process (CPS) Study: an evaluation of selected aircraft certification, operations, and maintenance processes, March 2002
[2]	EASA; CS25 – Certification Specifications for Large Aeroplanes (including Book–1 - Airworthiness codes and Book–2 - Acceptable Means of Compliance)
[3]	EASA; CS25.1302 – Installed systems and equipment for use by the flight crew
[4]	EASA; CS25.1309 – Equipment, systems and installations
[5]	EASA; CS–6 - Additional Airworthiness Specifications for Operations (expected to be issued on the basis of EASA Notice of Proposed Amendment (NPA) No 2009-01 – Operational Suitability Certificate and Safety Directives, R.F00802, 16 Jan 2009)
[6]	Commission Regulation (EC) No 859/2008 of 20 August 2008 amending Council Regulation (EEC) No 3922/91 as regards common technical requirements and administrative procedures applicable to commercial transportation by aeroplane (also referred to as 'EU-OPS requirements')
[7]	FAA/EUROCONTROL Action Plan 5; Validation and Verification Strategies: Operational Concept Validation Strategy Document, Edition 2.0, 27 March 2007
[8]	JAA; JAR25.803 – Joint Aviation Requirements for Large Aeroplanes – Emergency Evacuation.
[9]	European Commission; Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the Regions - A strategic review of Better Regulation in the European Union, COM (2006) 689 final, 14/11/2006
[10]	EASA; Type Certificate Data Sheet No. IM.A.120 for Boeing 737, Issue 09, 12 July 2012
[11]	Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services
[12]	Commission Regulation (EC) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 & 691/2010
[13]	SESAR; Definition Phase - ATM Safety Regulation: Synopsis of the current regulatory framework, WP1.6.1/D1, DLT-O507-161-00-02, 11-07-2006
[14]	CAATS II; Good practices for Safety Assessment in R&D projects (D13), 30/10/2009
[15]	EUROCONTROL; EATMP Air Navigation Safety Assessment Methodology, Edition 2.0, 4 April 2004
[16]	EUROCONTROL; ATM Safety Regulatory Requirement 4 "Risk assessment and mitigation in ATM"
[17]	Open Platform for EvolutioNary Certification Of Safety-critical Systems (OPENCOSS): Baseline for the Compositional Certification Approach (D5.1), Julʸ 5th, 2012
[18]	SAE; Guidelines for Development of Civil Aircraft and Systems, ARP4754, Revision A, 21-12-2010 (= revised updated version of the EUROCAE ED79A)
[19]	EUROCAE; Process for Specifying Risk Classification Scheme and Deriving Safety Objectives in ATM, ED-125, March 2010
[20]	EUROCAE; Guidelines for ANS Software Safety Assurance, ED-153, August 2009

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

[21]	EUROCAE; Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, ED-109A, January 2012
[22]	RTCA; Software Considerations in Airborne Systems and Equipment Certification, DO-178B, 12/1/1992
[23]	International Electrotechnical Commission (IEC); Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems, IEC 61508, Edition 2.0, April 2010
[24]	EUROCONTROL; Specification for Data Assurance Levels, Edition 1.0, 15/03/2012, EUROCONTROL-SPEC-148, ISBN: 978-2-87497-029-0
[25]	EUROCONTROL; Safety Assessment Made Easi–r - Part 1 Safety Principles and an Introduction to Safety Assessment, Edition 1.0, 15 January 2010
[26]	T. Kelly, R. Weaver; The Goal Structuring Notation – A Safety Argument Notation, Department of Computer Science and Department of Management Studies, University of York, York, YO10 5DD UK
[27]	EUROCONTROL; ACAS Bulletin No.–6 - Incorrect use of the TCAS traffic display, March 2005
[28]	T. Kelly; Managing Complex Safety Case, [1]1th Safety-Critical Systems Symposium, (pp. –9 - 115), 2003
[29]	CENELEC; Railway applicatio–s - Communication, signalling and processing syste–s - Safety related electronic systems for signalling, EN 50129:2003
[30]	CENELEC; Railway applicatio–s - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAM–) - Part 4: Functional Safe–y - Electrical/Electronic/Programmable electronic systems, prEN 50126-4:2012
[31]	Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005
[32]	Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation)
[33]	Civil Aviation Authority UK; Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases: For Aerodrome Operators and Air Traffic Service Providers, CAP760, 10 December 2010
[34]	EASA; Notice of Proposed Amendment (NPA) No 2011-20 – Authority, Organisation and Operations Requirements for Aerodromes, 13 December 2011
[35]	ASCOS D1.1; Analysis of existing regulations and certification processes
[36]	ASCOS D1.3; Development of selected new certification approach
[37]	B. Pauly; ASCOS WP1 Certification Process – Intermediate results, ASCOS EASA Workshop, 19 April 2013, Cologne
[38]	Civil Aviation Authority UK; CAP 138
[39]	C. Haddon-Cave, C; An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, HMSO UK, 2009
[40]	G. Despotou, R. Alexander, T. Kelly; Addressing Challenges of Hazard Analysis in Systems of Systems, in 3rd Annual IEEE Systems Conference, 2009

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

[41]	J. Monso, B. Rabiller; SESAR Proof of Concept supporting document, SESAR P16.01.04, deliverable D4
[42]	J. Monso, B. Rabiller; Guidance material to execute proof of concept, SESAR P16.01.04, deliverable D6

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

Appendix A Summary of options addressing shortcomings and bottlenecks

The Table below provides potential options to be considered for a new adapted certification process by taking into account different points of views (e.g. authorities, industry…). The columns ("shortcoming"; "bottleneck") provide information (marked with a "*") regarding what kind of problems this option is preferably addressing. The column "Rationale" indicates from "process" and/or "stakeholders" points of views the reason why the corresponding option is addressing "shortcoming" and/ or "bottleneck". Based on the outcome of ASCOS D.1.1, this study has identified several applicable options in order to address the problem of "shortcomings" and "bottlenecks" regarding implementation of current safety regulatory framework in a context of Total Aviation System. The following definitions have been used regarding "shortcoming" and "bottleneck":

- Shortcoming: 'a fault or failure to meet a certain standard, typically in a person's character, a plan or a system'. In the context of the analysis the term shortcoming is used to describe the situation where the regulation is fully implemented but proves to be inadequate.
- Bottleneck: 'a phenomenon where the performance or capacity of an entire system is limited by a single or limited number of components or resources'. In the context of the analysis the term bottleneck is used to describe the situation where the regulation is not implemented at the expected level.

Table 5 – Summary of options addressing shortcomings and bottlenecks

N°	short-coming	Bottle-neck	Identified options	Rationale	Domains
1	*		Integrate all domains within the authority	Stakeholders Closer cooperation between different aviation domains The probability that conflicting requirements are developed will probably decrease.	ATM industry (option a) ATM Authority *(coordinated strategic ATM plan taking into account EASA, Eurocontrol, SESAR and SES regulatory issues)* Aircraft/ product certification (option a) ATM System & Procedures
2		*	Change between performance based and compliance based	Process A performance based requirement structure could accelerate the certification of novel products for which detailed prescriptive requirements are not available.	ATM industry (option b) ATM Authority *(Strategic regulatory pause)* Aircraft/ product certification (option b) ATM System & Procedures

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium

N°	short-coming	Bottle-neck	Identified options	Rationale	Domains
3		*	Abolish all certification by authorities and transform into voluntary compliance	Stakeholders/ Process This option will most certainly reduce the cost of Certification activities	Air operator (option s 2&3) Aircraft/ product certification (option c)
4		*	Make more use of competent (certified) entities	Stakeholders/ Process For the short term this is probably a very powerful means to prevent delays in the certification process and to perform the job with enough competence.	Air operator (option 4) ATM industry (option d) Aircraft/ product certification (option d)
5		*	Certify the applicants instead of their products	Stakeholders/ Process Decrease of number of certifications	ATM industry (option e) Aircraft/ product certification (option e) ATM System & Procedures
6	*	*	Use of Proof of Concept approach	Process A Proof of Concept can be part of a Performance based Certification method Could accelerate the ability of products to be certified	ATM industry (option f) Aircraft/ product certification (option f) ATM System & Procedures
7	*	*	Enforce existing rules and improve existing processes	Process Expected Benefit to reduce shortcoming & bottleneck	Air operator (options 1 & 5 &6) ATM industry (option g) ATM Authority *(one clear rulemaking and planning process for ATM)* *(Strategic regulatory pause rulemaking)* ATM System & Procedures Airport
8	*	*	Cross-domain fertilisation	Process Expected Benefit to reduce shortcoming & bottleneck by taking into account experience and lessons learnt	ATM industry (option h) ATM System & Procedures Airport

This report is not to be reproduced, modified, adapted, published, nor disclosed to any third party, without permission of the ASCOS Consortium