WP1 Certification Processes Final Report

Bernard Pauly, Fateh Kaakai (TR6)

This final report reflects the approach followed in WP1 dedicated to adapt the certification process. It describes the different steps regarding the identification of potential shortcomings and bottlenecks induced by the regulatory framework in the scope of Total Aviation (D1.1). Then some alternatives have been identified and assessed (D1.2) in order to propose some arrangements in the certification of products and operations (D1.3). Finally the feedback from Certification case studies (WP4) and Users Group (WP5, WP6) are considered for the final adaptation of the process (D1.5). During the analysis inputs from WP2 and WP3 were also considered to refine the process adaptation.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	B. Pauly (Thales Air Systems)

Grant Agreement No.	314299
Document Identification	D1.6
Status	Version for approval by PMT
Version	1.0
Date of Issue	23-09-2015
Classification	Restricted

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	B. Pauly, F. Kaakai	22-09-2015	All	Version for approval by PMT

Review and Approval of the Document

Organisation	Name of person reviewing the document	Date
JPM	J.P. Magny	17/09/2015
NLR	A.L.C. Roelen	17/09/2015
TU DELFT	H. Udluft	17/09/2015
THALES	B. Pauly	17/09/2015
CAAi	T. Longhurst	17/09/2015
Deep Blue	L. Save	17/09/2015
ILOT	B. Dziugiel, A. Iwaniuk	17/09/2015
APSYS	J.P. Heckmann, J.F. Delaigue, S. Bravo Munoz	17/09/2015
Ebeni	A. Simpson, J. Denness, S. Bull	17/09/2015
Organisation	Name of person approving the document	Date
Thales Air Systems	Fateh KAAKAI	23/09/2015

Document Distribution

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

Acronyms

Abbreviations	*Description*
AARS	Automated Aircraft Recovery System
AAT	Aeronautics and Air Transport
ACARE	Advisory Council for Aviation Research and Innovation in Europe
ACAS	Airborne Collision Avoidance System
ADM	Aerodrome Design Manual
ADR	Air Data Reference
ADRM	Aerodrome
AIM	Accident Incident Model
AIP	Aeronautical Information Publication
AIS	Aeronautical Information Services
AltMoC	Alternative Means of Compliance
AMAN	Abrupt Manoeuvre
AMC	Acceptable Means of Compliance
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AOC	Air Operator Certificate
AoC	Area of Change
ARC	Abnormal runway contact
ASCOS	Aviation Safety and Certification of new Operations and Systems
ASM	Airspace Management
A-SMGCS	Advanced Surface Movement Guidance and Control Systems
ATCO	Air Traffic COntroller
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATM/CNS	Air Traffic Management/ Communication Navigation Surveillance
ATS	Air Traffic Services
AUR	Airspace Usage Requirements
BIRD	Collision/ near collision with Birds
CAA	Civil Aviation Authority
CABIN	Cabin safety event
CAP	CAA Publication
CAST	Commercial Aviation Safety Team
CATS	Causal model for Air Transport Safety
CBA	Cost Benefit Analysis
CENELEC	European Committee for Electrotechnical Standardization
CFIT	Controlled Flight into or toward terrain

Abbreviations	*Description*
CLR	Deviation of ATC Clearance
CMA	Continuous Monitoring Approach
CMM	Capability Maturity Model
CMMI	Capability Maturity Model integration
CNS	Communication, Navigation, and Surveillance
CofA	Certificate of Airworthiness
COL	Collision with a vehicle, person or aircraft, while aircraft is on the ground.
COTS	Commercial Off The Shelve
CRD	Comment Response Document
CS	Community Specification; Certification Standards
CSM	Continuous Safety Monitoring; Common Safety Method
CTOL	Collision with obstacle(s) during take-off and landing
DoC	Declaration of Conformity
DOD	Department of Defence
DSU	Declaration of Suitability for Use
EASA	European Aviation Safety Agency
EASP	European Aviation Safety Plan
EATMP	European Air Traffic Management Programme
EC	European Commission
ECAST	European Commercial Aviation Safety Team
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems
ECR	European Central Repository
EFB	Electronic Flight Bag
EGAST	European General Aviation Safety Team
EHEST	European Helicopter Safety Team
e-learning	Electronic learning
ELS	E-Learning Support
E-OCVM	European Operational Concept Validation Methodology
ESA	European Space Agency
ESARR	EUROCONTROL Safety Regulatory Requirement
ESASI	European Society of Air Safety Investigators
ESD	Event Sequence Diagram
ESSI	European Strategic Safety Initiative
ETSI	European Telecommunications Standards Institute
ETSO	European Technical Standard Order
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
EUROCONTROL	European Organisation for the Safety of Air Navigation
EVAC	Evacuation

Abbreviations	*Description*
EVAIR	EUROCONTROL Voluntary ATM Incident Reporting system
EXTL	External load related occurrence
FAA	Federal Aviation Administration
FAST	Future Aviation Safety Team
FMS	Flight Management System
F-NI	Fire/smoke (non-impact)
FP7	7th Framework Programme
F-POST	Fire/smoke (post-impact)
FTA	Fault Tree Analysis
FUEL	Fuel related
GCOL	Ground collision
GM	Guidance Material
GSN	Goal Structuring Notation
GTOW	Glider towing related event
HF	Human Factors
i.l.o.	In lieu of
IATA	International Air Transport Association
IBIS	ICAO Bird Strike Information System
ICAO	International Civil Aviation Organization
ICE	Icing
ICMM	Integrated Capability Maturity Model
IMA	Integrated Modular Avionics
IORS	EASA Internal Occurrence Reporting System
IR	Implementing Rule
IRP	EUROCONTROL Integrated Risk Picture
IS	Inadequate Separation
ISO	International Organization for Standardization
JARUS	Joint Authorities For Rulemaking of Unmanned Systems
LALT	Low altitude operation
LOC-G	Loss of control ground
LOC-I	Loss Of Control - Inflight
LOLI	Loss of lighting conditions en-route
LURS	Light Unmanned Rotorcraft Systems
MAC	Airprox/ TCAS alert/ loss of separation/ near mid-air collision/ mid-air collision
MCC	Means of Compliance Checklist
MOOC	Massive Open Online Courses
NAA	National Aviation Authority
NPA	Notice of Proposed Amendment
NSA	National Supervisory Authority

Abbreviations	*Description*
OMG	Object Management Group
OPENCOSS	Open Platform for Evolutionary Certification of Safety-Critical Systems
OTHR	Other
PANS	Procedures for Air Navigation Services
PANS-RAC	Procedures for Air Navigation Services-Rules of the Air and Air Traffic Services
POC	Proof of Concept
R&D	Research and Development
RAMP	Ground handling
RE	Runway excursion
RF	Radio Frequency
RI	Runway Incursion is an occurrence involving the incorrect presence of an aircraft, vehicle, or person on the protected area of a surface designated for the landing and take-off of an aircraft
RI-A	Runway incursion animal
RI-VAP	Runway incursion –vehicle, aircraft or person
RNP	Required Navigation Performance
RPAS	Remotely Piloted Aircraft System
RTCA	Radio Technical Commission for Aeronautics
RVSM	Reduced Vertical Separation Minima
SACM	Structured Assurance Case Metamodel
SAM	Safety Assessment Methodology (EUROCONTROL)
SAME	Safety Assessment Made Easier
SAM-E	Safety Assessment Made Easier
SARPs	Standards and Recommended Practices (ICAO)
SCDM	Safety Case Development Manual
SCF-NP	System/ component failure or malfunction (non-powerplant)
SCF-PP	System/ component failure or malfunction (powerplant)
SEC	Security related
SEooC	Safety Element out of Context
SERA	Standardised European Rules of the Air
SES	Single European Sky
SESAR	Single European Sky ATM Research
SMI	Separation Minima Infringement
SMM	Safety Management Manual
SMS	Safety Management System
SOIR	Simultaneous Operations on Parallel or Near-Parallel Instrument Runways
SOPs	Specific Operating Provisions (Operations Specifications)
SOS	System of Systems
SPI	Safety Performance Indicator

Abbreviations	*Description*
SRAC	Safety Related Application Condition
SRC	EUROCONTROL Safety Regulation Commission
SRG	Safety Regulation Group
SRM	(SESAR) Safety Reference Material; Safety Risk Model
SW	Software
SWALs	Software Assurance Levels
TAS	Total Aviation System
TC	Type Certificate
TESG	TAS Engineering and Safety Group
TMA	Terminal Manoeuvring Area
TRL	Technology Readiness Levels
TURB	Turbulence encounter
UAP	Unauthorised penetration of Airspace
UAV	Unmanned Aerial Vehicle
UIMC	Unintended flight in Instrument Meteorological Conditions (IMC).
UNK	Unknown or undetermined
URL	Uniform Resource Locator (web address)
USOS	Undershoot/ overshoot
WP	Work Package
WSTRW	Windshear or thunderstorm

This page is intentionally left blank

Executive Summary

Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance, suggest the need for the adaptation of existing certification processes within the frame of the Total Aviation System (TAS) which encompasses all stakeholders involved in aviation: products, operators, crews, and aerodromes, ATM, ANS, on the ground or in the air.

The European Commission (EC) Project "Aviation Safety and Certification of new Operations and Systems" (ASCOS) contributes to the removal of certification obstacles and supports implementation of technologies to reach the EU ACARE Vision 2020 and Flight Path 2050 goals.

The Work Package 1- Certification Process Work Package (WP1) aims at adapting approval/certification processes by addressing issues where no improvement has been observed during the past years. These adaptations intend to deliver as far as possible (i) efficiency in terms of cost and time, (ii) ability to analyse and demonstrate acceptable safety for new concepts and technologies, and (iii) ability to analyse and consider the entire aviation system rather than sub-elements in isolation.

Identification shortcomings and bottlenecks in existing regulation and certification/approval processes

A key step in an improved certification process is firstly to understand as much as possible how the current regulation could influence at the end the operational safety occurrences in a context of Total Aviation System (TAS). It is noted that current EASA initiatives also aim to address these shortcomings, and this shared interest proves the relevance of this subject. For this purpose an analysis has been performed in D1.1 in order to identify potential shortcomings (situation where the regulation is fully implemented but proves to be inadequate) and bottlenecks (situation where the regulation is not implemented at the expected level) in the current European certification processes and more generally the regulatory framework.

The main conclusions are related to potential issues concerning overlaps between regulatory requirements, lack of clear accountability for regulated entities, inappropriate actual requirements due to technological changes and emerging risks in the following domains: Human factor, Aerodromes (runway conditions), CNS/ATM (interoperability), Interfaces between maintenance/operations/certification, re-use of safety cases. On top of shortcomings and bottlenecks precisely identified in D1.1, it has been recommended to continue this study to address some issues listed in the general conclusion of this report.

Overview of the ASCOS Method

On the basis of Key Principles (identified in D1.2) influencing the reduction of shortcomings and bottlenecks, and of findings gathered from WP4 (ASCOS Certification Case studies), WP5 (ASCOS Validation results), and feedbacks from ASCOS Users Group (WP6), a consolidated new approval method called the *ASCOS Method* (fully described in D1.5) has been built. The ASCOS Method responds to the pressures in the aviation industry which are driving innovation and increased integration between domains and therefore making it imperative to streamline approval processes. The ASCOS Method integrates with the lifecycle of a change, from concept to building a safety argument supporting the application for approval. The proposed method considers the full

impact of the change, and recognizes and manages the interaction between domains. The method is also flexible to embrace innovation while encompassing existing established processes wherever appropriate.

Concept of approval path and Definition of an acceptable level of safety

Central to the ASCOS Method is the development of an approval path for the proposed change. This path should follow existing approaches wherever possible, adapting and extending these approaches only where necessary to accommodate parts of the change which are not covered by existing regulations, or where significant efficiencies can be gained. The approval path should be justified by a safety argument which demonstrates that the change will achieve the *acceptable level of safety* required by the approver of the change, and this is the purpose of the next point.

The ASCOS Method focuses on demonstrating that the change delivers an acceptable level of safety across the TAS. A change which decreases safety (i.e. increases safety risk) in one domain is usually difficult or impractical to justify, even when it significantly increases safety in other domains. To trade off safety between domains, it would be necessary to provide a robust quantification across all domains which demonstrates a significant overall positive impact on safety. As a result, each module of the safety argument will need to demonstrate that the change achieves the acceptable level of safety applicable in the domain for which the module is making the safety argument. The building of safety arguments shall be modular and iterative until the development is complete and approval is gained. It has been recommended in D1.5 that further research should be undertaken to develop the existing models to a level of maturity where such trade-offs between domains could be made.

Modularisation of the argument and Concept of an argument architect

The ASCOS Method addresses the issue of interfaces within the TAS by introducing the concept of dividing the argument into modules aligned to domains of the TAS and organisational responsibilities. Assurance contracts are established between modules to define and manage dependencies between modules.

The ASCOS Method introduces the role of an argument architect, with the role of designing and maintaining the safety argument, which includes ensuring that the argument modules are correctly bounded and interfaced to other modules throughout the development. ASCOS proposes (D3.6) that any complex development should be co-ordinated by a TAS Engineering and Safety Group (TESG) that would therefore play the role of argument architect for changes involving multiple organisations.

Clarification of the key roles and Application of the ASCOS Method

Another main significant example of the ASCOS Method added value is the development and clarification of the roles of different stakeholders across the certification process steps highlighting the complexity of the TAS aspects in the control of risks

Finally, further opportunities for improvement and refinement of the ASCOS Method have been identified. However, the greatest opportunity for improvement will come from application of the ASCOS Method. The ASCOS Consortium commends this ASCOS Method to EASA for adoption as a means of establishing approval for changes to the TAS within Europe.

Table of Contents

List of Figures

List of Tables

1 Overview of ASCOS and of Certification Process Work Package (WP1)

1.1 The ASCOS Project

Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance, suggest the need for the adaptation of existing certification processes. The European Commission (EC) Project 'Aviation Safety and Certification of new Operations and Systems' (ASCOS) contributes to the removal of certification obstacles and supports implementation of technologies to reach the EU ACARE Vision 2020 [1] and Flight Path 2050 [2] goals.

ASCOS is delivered by a consortium of organisations involved in the European aviation industry and supported by a wide ranging User Group providing input and review.

The main objective of the ASCOS project is to develop novel certification process adaptations and supporting safety driven design methods and tools to ease the certification of changes to the aviation system (in particular safety enhancement systems and operations), thereby increasing safety. The project will follow a total system approach, dealing with all aviation system elements (including the human element) in an integrated way over the complete life-cycle. ASCOS is also tasked with ensuring that any proposed approach is cost-effective and efficient.

The ASCOS Project was structured into six main work packages:

- WP1: Certification Process – Development of safety based certification process adaptations based on analysis of existing certification and rulemaking process and evaluation of different possible new approaches
- WP2: Continuous Safety Monitoring – Development of a methodology and supporting tools for multi-stakeholder continuous safety monitoring, using a baseline risk picture for all parts of the total aviation system
- WP3: Safety Risk Management – Development of a total aviation system safety assessment methodology, with supporting safety based design systems and tools, for handling of current, emerging and future risks
- WP4: Certification Case Studies – Application of the new certification approach and supporting safety based design systems and tools in the selected example case studies
- WP5: Validation – Validation of the new certification approach and the supporting methods and tools
- WP6: Dissemination and Exploitation – Dissemination to ensure that results are correctly understood and exploited to the maximum extent

The project is also supported by a seventh work package for project management.

1.2 Overview of the Certification Process Work Package (WP1)

The aim of the certification process work package (WP1) is to develop safety based certification process adaptations based on analysis of existing certification and rulemaking process and evaluation of different possible new approaches. It is structured into five sub-work packages:

- D1.1: Analysis existing regulations and certification processes
- D1.2: Definition and evaluation of innovative certification approaches
- D1.3: Outline proposed certification approach
- D1.4: E-learning environment to support certification processes
- D1.5: Consolidated New Approval Method

Proposed certification adaptations within WP1 are based on the assessment of issues where no improvement has been observed during the past years. These adaptations aim at delivering as far as possible:

- Efficiency in terms of cost and time
- Ability to analyse and demonstrate acceptable safety for new concepts and technologies
- Ability to analyse and consider the entire aviation system rather than sub-elements in isolation

The scope of WP1 is the Total Aviation System (TAS) which encompasses all stakeholders involved in aviation: products, operators, crews, and aerodromes, ATM, ANS, on the ground or in the air. Therefore, it means that all the categories of accidents / incidents shall be considered.

For this purpose, in D1.1 [8], the different reports from EASA, EUROCONTROL (SRC) were examined. Some tendencies were highlighted. The following point was to propose a framework to objectively define what are the shortcomings and bottlenecks potentially induced by the current Regulation in the deployed certification processes. This framework is based on the following criteria:

- the severity of the safety occurrences
- the tendencies in terms of improvement (or not) during the past years,
- the identification of the main precursors of the safety issues
- the number of Aviation domains embedding the precursors
- the flight phases in order to consolidate assumptions in terms of tendencies (cross reference with annual reports of international bodies).

After identification of findings related to shortcomings and bottlenecks, some additional criteria have been identified in D1.2 [9] to support the brainstorming phase in order to identify potential alternatives in terms of

certification / approval processes adaptation. The main ideas were to consider both the benefits of actual practices but also to keep a certain degree of flexibility able to streamline the processes when it is acceptable.

In D1.3 [10], the above principles and findings have been applied and organized to implement a new process for certification of a change within the frame of the whole Total Aviation System. This new process has been deployed by the Certification Case Studies of WP4 representing a large diversity of case studies regarding the TAS domains [16].

In parallel of the studies, a framework of an e-learning environment has been developed to support the dissemination of ASCOS results and facilitate the appropriation of the approaches by the public [11].

Finally in D1.5, an assessment of the feedback from WP4 [16] and of the validation results provided by WP5 [17] with the support of ASCOS User Group has been performed in order to refine the initial certification process proposed in D1.3 and to issue the final ASCOS Consolidated New Approval Method [12].

2 The considered Regulation and Certification/ approval processes

In ASCOS project, the regulatory issues are considered from the scope covered by the different TAS domains but also from the roles of involved stakeholders in the TAS in the chain of activities included in the certification or more generally in the approval processes.

EP & EC (European Parliament and European Commission): In compliance with ICAO Regulatory Material (Annexes, Rules, Recommended Practices….), the harmonisation of the European TAS Regulatory Framework is developed under the legal authority of the EP & EC

Single European Sky (SES) In 2004 a dedicated Regulatory Framework was approved by these authorities in order to support the creation of the SES (Single European Sky: SES package I)

EASA: In addition to face the challenges due to the Total Aviation System issues, the EC has extended the responsibility of EASA (2008) to cover all the Aviation domains (including ATM and ADR)

TAS Regulatory Framework: In this context, the TAS Regulatory Framework in Europe needs to consider the applicable Regulation (EASA and SES). Their improvement and harmonisation is currently in progress and managed by EASA in consultation with all the aviation stakeholders.

2.1 The scope of TAS (Total Aviation System)

The total system approach is based on the fact that Products (aircraft, airborne and ground equipment), Airspace users (Flight Operators, crews, maintenance personnel), Aerodromes, CNS/ ATM services providers Suppliers ,on the ground or in the air are part of a single network.

The aim of the "total system approach" is to eliminate the risk of safety gaps or overlaps, and seeks to avoid conflicting requirements and confused responsibilities. Regulations are interpreted and applied in a standardised manner and best practices are provided.

It supports increased interoperability of products and services. The “total system approach” also streamlines the certification processes and reduces the burden on regulated persons and organisations.

- Airworthiness may be defined as the fitness of an aircraft for flight in all the environments and circumstances for which it has been designed and to which it may therefore be exposed. An Airworthy aeroplane is one which is fit to fly. This includes the design and construction (in accordance with specific certification codes.

- Continuing airworthiness: The set of processes by which an aircraft, engine, propeller or part complies with the applicable airworthiness requirements and remains in a condition for safe operation throughout its operating life (source ICAO Annex 8). The ultimate responsibility for Continued Airworthiness is assigned in ICAO Annex 8 to the State of Design but the program to achieve it is a matter for the State of Registry.

- Flight Operations: All provisions to prepare and operate a flight in safe conditions. For example: Standard Operating Procedures (SOP) for each phase of flight, the specifications for the operational flight plan, Instructions on the use of normal checklists and the timing of their use, Emergency evacuation procedures, Departure and approach briefings, Instructions and training requirements for the avoidance of controlled flight into terrain and policy for the use of the ground proximity warning system (GPWS), Route and destination familiarization, Instructions on the clarification and acceptance of ATC clearances, particularly where terrain clearance is involved, etc….

- Aerodrome: A defined area on land or water (including any buildings, installations and equipment) intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft (source ICAO annex 6).

- ANS: Air Navigation Services means Air Traffic Services, Communication, Navigation and Surveillance services, Meteorological services for air navigation and Aeronautical Information Services:

    1. ATS Air Traffic Services means the various Flight Information Services, Alerting services, Air Traffic advisory services and ATC services (area, approach and aerodrome control services)

    2. AIS Aeronautical Information Service means a service established within the defined area of coverage responsible for the provision of aeronautical information and data necessary for the safety, regularity, and efficiency of air navigation

    3. ATC services means services provided for the purpose of:

        - preventing collisions: between aircraft, and in the manoeuvring area between aircraft and obstructions and

        - expediting and maintaining an orderly flow of air traffic.

    4. ATM: Air Traffic Management means the aggregation of the airborne and ground-based functions (Air Traffic Services, Airspace Management and Air Traffic Flow Management) required to ensure the safe and efficient movement of aircraft during all phases of operations

        - AM Airspace Management means a planning function with the primary objective of maximising the utilisation of available airspace by dynamic time-sharing and, at times, the segregation of airspace among various categories of airspace users on the basis of short-term needs.

        - ATFM Air Traffic Flow Management means a function established with the objective of contributing to a safe, orderly and expeditious flow of air traffic by ensuring that ATC capacity is utilized to the maximum extent possible, and that the traffic volume

is compatible with the capacities declared by the appropriate air traffic service providers.

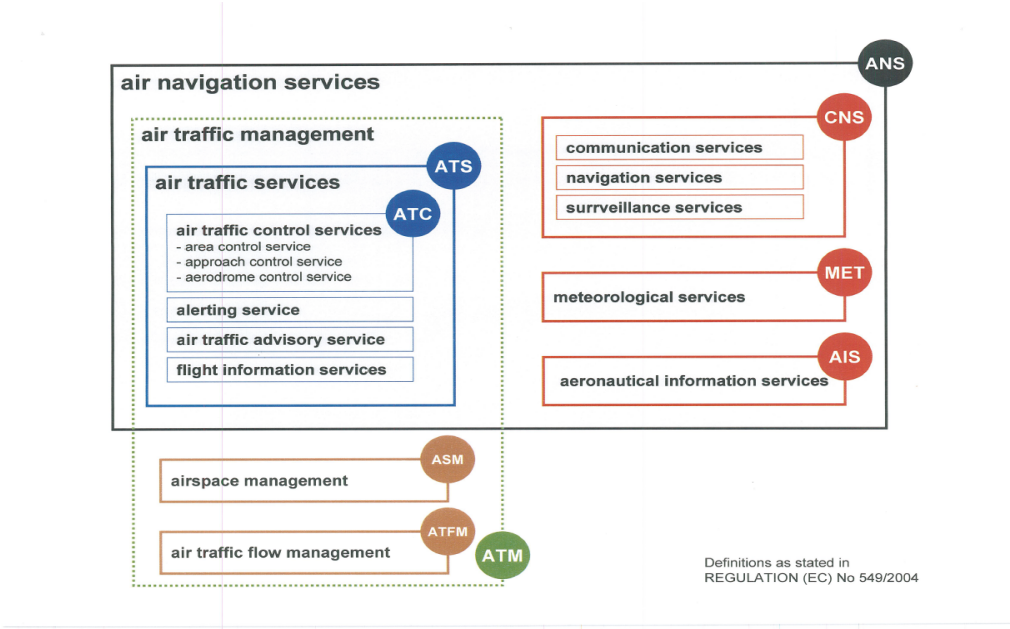

Figure 1 - ANS-ATM Scope

2.2 The stakeholders of the TAS

According to the TAS scope, the set of involved stakeholders are the following:

- Airspace users

The airspace users include airlines, pilots, aircraft operators and passengers

- Air Navigation Service providers

Air navigation service providers (ANSPs) are responsible for organising and managing the flow of traffic in the air and on the ground in a dedicated airspace

- Airports

Airports operators are particularly responsible for managing departures and arrivals of aircraft and all the movements of aircraft and vehicles on the ground

- National and international aviation regulators

Regulators are responsible to put in place appropriate regulations and to assume the fact that these regulations are respected

- Aeronautics industry

The aeronautics industry includes manufacturers of aircraft, avionics (aviation electronics) and air traffic management infrastructure (radio antennas and satellites for instance, control centers supporting all the operational services like Flight data management, surveillance, communication air-ground and ground-ground…..).

- International aviation organisations

ICAO (world wide scope) and ECAC (Europe scope) have an important role to provide the status of evolution of aviation safety issues and to define and monitor agreed improvement actions plans in the different areas and avoid duplication of efforts (EASA, EUROCONTROL, EUROCAE).

ICAO (International Civil Aviation Organisation) :

A specialised agency of the United Nations was created in 1944 to promote the safe and orderly development of international civil aviation throughout the world. It sets standards and regulations necessary for aviation safety, security, efficiency and regularity, as well as for aviation environmental protection. The Organisation is made up of an Assembly, a Council of limited membership with various subordinate bodies and a Secretariat. The Assembly, composed of representatives from all Contracting States, is the sovereign body of ICAO. It meets every three years, reviewing in detail the work of the Organisation and setting policy for the coming years. It also votes a triennial budget. The Council, the governing body which is elected by the Assembly for a three-year term, is composed of 36 States.. It is in the Council that Standards and Recommended Practices are adopted and incorporated as Annexes to the Convention on International Civil Aviation. The Council is assisted by the Air Navigation Commission (technical matters), the Air Transport Committee (economic matters), the Committee on Joint Support of Air Navigation Services and the Finance Committee. ICAO works in close co-operation with other members of the United Nations family:

- World Meteorological Organisation, the International Telecommunication Union, the Universal Postal Union, the World Health Organisation and the International Maritime Organisation.
- Non-governmental organisations which also participate in ICAO's work include the International Air Transport Association, the Airports Council International, the International Federation of Air Line Pilots' Associations, and the International Council of Aircraft Owner and Pilot Associations.

EASA (European Agency for the Safety of Aviation):

EASA is an Agency of the European Union (based in Cologne- Germany). As a Community Agency, EASA is a body governed by European public law; it is distinct from the Community Institutions (Council, Parliament, Commission, etc.) and has its own legal personality. EASA was set up by a Council and Parliament regulation (Regulation (EC) 1592/2002 repealed by Basic Regulation (EC)

No 216/2008 and amended by Regulation (EC) 1108/2009) and was given specific regulatory and executive tasks in the field of civil aviation safety and environmental protection. Article 1(2) of Basic Regulation , as amended by Regulation (EC) No 1108/2009 of the European Parliament and of the Council of 21 October 2009, excludes from the Agency's scope aircraft involved in the execution of military, customs, police, search and rescue, fire fighting, coastguard or similar activities or services.

The main tasks of the Agency currently include:

- Rulemaking: drafting aviation safety legislation and providing technical advice to the European Commission and to the Member States;
- Inspections, training and standardisation programmes to ensure uniform implementation of European aviation safety legislation in all Member States;
- Safety and environmental type-certification of aircraft, engines and parts;
- Approval of aircraft design organisations world-wide as and of production and maintenance organisations outside the EU;
- Authorisation of third-country (non EU) operators;
- Coordination of the European Community programme SAFA (Safety Assessment of Foreign Aircraft) regarding the safety of foreign aircraft using Community airports;
- Data collection, analysis and research to improve aviation safety.
- From 2008, its role has been extended to ATM/ ADR domains.

EUROCONTROL

EUROCONTROL is an intergovernmental organisation made up of 38 Member States and the European Community.

It has as its primary objective the development of a seamless, pan-European air traffic management (ATM) system. EUROCONTROL was originally founded in 1960 as a civil-military organisation. Its aim was to deal with air traffic control for civil and military users in the upper airspace of its six founding European Member States (Belgium, Germany, France, Luxembourg, the Netherlands and the UK). EUROCONTROL, today, is committed to building, together with its partners, a Single European Sky (SES) that will deliver the ATM performance required for the 21st century and beyond. EUROCONTROL works closely with Member States, air navigation service providers, civil and military airspace users, airports, the aerospace industry, professional organizations and European institutions.

EUROCAE (European Organisation for Civil Aviation Equipment)

EUROCAE is a non-profit making organisation which was formed at Lucerne (Switzerland) in 1963 to provide a European forum for resolving technical problems with electronic equipment for air transport. EUROCAE deals exclusively with aviation standardisation (Airborne and Ground Systems and Equipment) and related documents as required for use in the regulation of aviation equipment and systems. EUROCAE is an association composed of members who are all specialised in one or several technical fields of Aeronautics and many of them are considered to be among world's leaders in their domain.

These members include Equipment and Airframe Manufacturers, Regulators, European and International Civil Aviation Authorities, Air Navigation Service Provider (ANSP), Airlines, Airports and other users. To develop EUROCAE Documents (ED), EUROCAE organises Working Groups (WG) where members provide experts working on voluntary basis.

The regulatory framework is based on different levels of contributions and decisions. The following figure represents the decomposition of these levels according to the nature of Regulatory Material (Irs, AMC, GM, CS…) EASA issues Opinions (Hard Law legally binding) or Decisions (Soft Law) based on consultation of stakeholders, bodies ….(Eurocontrol, Eurocae, SESAR….)

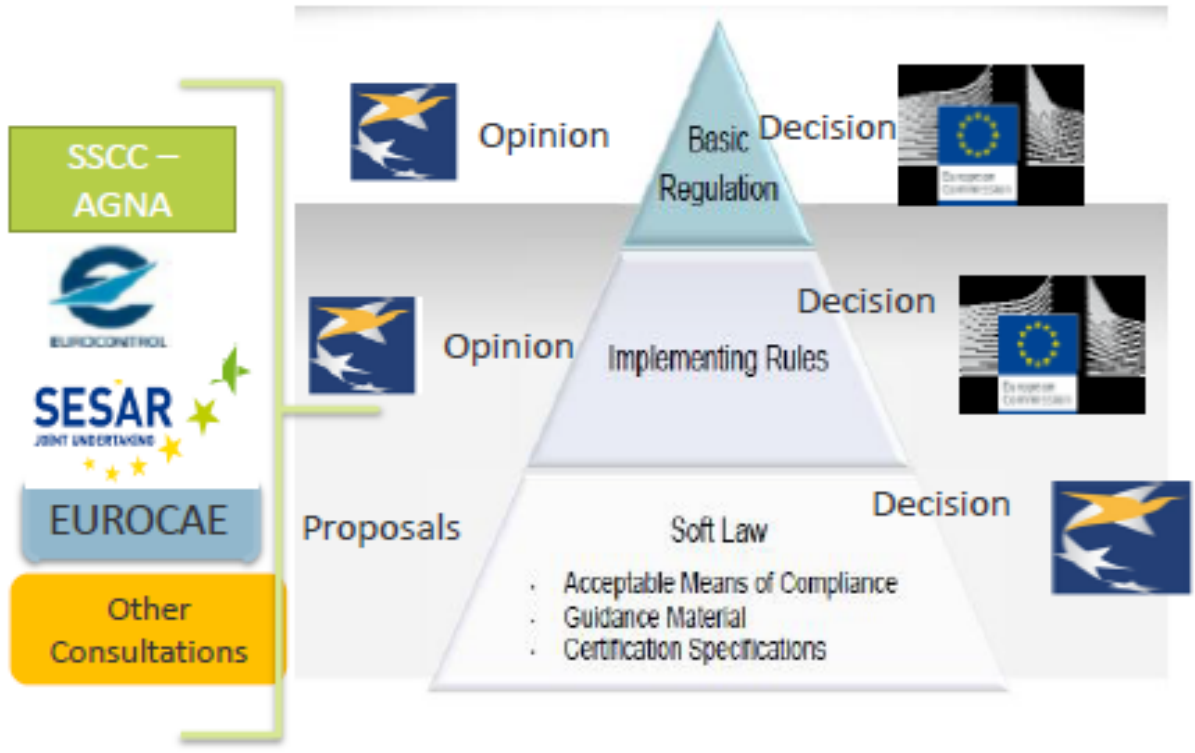

Figure 2 - Structure of the regulatory material

3 Identify potential shortcomings and bottlenecks in existing regulation and processes (D1.1)

3.1 Introduction (WP1.1)

Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance call for the adaptation of existing certification processes. The European Commission (EC) Project 'Aviation Safety and Certification of new Operations and Systems' (ASCOS) contributes to removal of certification obstacles and supports implementation of technologies.

A key step in an improved certification process is firstly to understand as much as possible how the current regulation could influence at the end the operational safety occurrences in a context of Total Aviation System (TAS). Regarding this clarification an analysis is performed in order to identify potential shortcomings and bottlenecks in the current certification processes and more generally the regulatory framework.

The WP1.1 task firstly provides an overview of the existing regulations and certification processes. Next, shortcomings and bottlenecks are identified via two complementary ways [8]:

Firstly, investigates which safety occurrences have relatively high or increasing risk,

Secondly, which areas have a relatively low level of implementation of regulations?

This analysis made use of data from EASA and SRC annual reports [1, 5]. The underlying assumptions were:

Classes of safety occurrences for which the risk is relatively high or increasing may point to shortcomings of the associated regulations and certification processes; some of which may be associated to interactions between regulatory domains;

Areas where the implementation level of regulations is low may point to bottlenecks in the associated regulations and certification processes.

This WP1.1 task describes how these two kinds of considerations (classes of safety occurrences, implementation level) could be combined and exploited in order to better understand what kind of recommendations could be provided. These recommendations should contribute to improve the definition and application of the regulatory framework in line with initiatives as already managed by EASA.

Moreover they should be an input for the different options to be investigated in a new adapted certification process as proposed in ASCOS WP1.

Finally this approach could initiate an assessment framework for certification processes and practices in Aviation.

The amount of effort involved in the certification of new aviation products and services can be an obstacle for the introduction of innovative technologies and operational concepts. The Airbus A400M military transport aircraft for instance, as well as the Eurofighter program, suffered delays and cost exceedances that were partly attributed to irregularities in the certification process (Traufetter, 2013). Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance may require an adaptation of existing certification processes. The European Commission (EC) Project 'Aviation Safety and Certification of new Operations and Systems' (ASCOS) contributes to removal of certification obstacles and supports implementation of technologies to reach the ACARE Vision 2020 (ACARE, 2001) and Flight Path 2050 (European Commission, 2011) goals. ASCOS outlines a new approach to certification that (ASCOS D1.3, 2013):

Is more flexible with regard to the introduction of new operations, systems and products;

Is more efficient, in terms of cost, time and safety, than the current certification processes;

Considers the impact on safety of all elements of the total aviation system and the entire system life-cycle in a complete and integrated way.

The work contributes directly to the high level Flight path 2050 [15] and ACARE Vision 2020 [13, 14] safety goals. By 2020, the target is

- reducing accident rate by 80%, and
- reducing human error and its consequences.

The Figure 3 - Fatal accident rates over the period 1980 until 2010 gives the fatal accident rate for commercial operations with western-built jet aircraft over the period 1980 until 2010. As can be observed, there has been little to no improvement of aviation safety worldwide from about 2004 onwards. Europe, the United States and other 'western' regions show a similar trend.

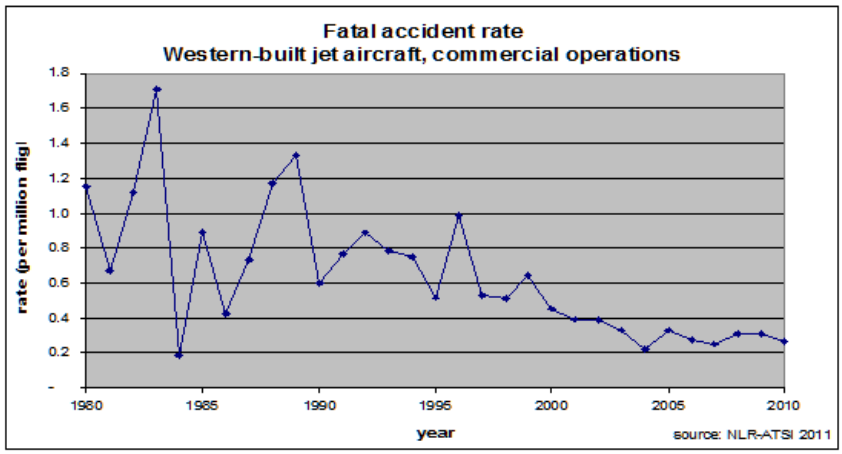

Figure 3 - Fatal accident rates over the period 1980 until 2010

3.2 Needs

Taking in consideration these situations, the needs are to investigate improvement areas and particularly the role of regulation whatever the involved domains of TAS in operational issues. These situations are based on the fact that the regulatory framework seems to be a corner stone and as a consequence there is a strong need to progress in the understanding of relationships between applicable regulatory material and operational safety issues. This topic is not new and the complexity is high due to many interacting factors.

An example of this kind of previous initiative is the study performed during SESAR Definition Phase (2007-2008) and focused on the necessary improvements and changes to be undertaken concerning regulatory framework to support the ATM Master Plan challenges.

After a preliminary status of the current situation, the recommendations of this study [1] were mentioning the following issues and weaknesses:

Fragmentation and variability: *"There is a diversity of approaches between States in the regulations applied and considerable difference in the rigour with which they are enforced"*

Accountability: "The development of new systems and operational concepts that may result in changes in the ATM roles of service providers, airborne systems, users, airports or the military will require clarity in the safety regulatory framework on the allocation of safety responsibilities."

Duplication: "The three layers of ATM safety regulatory organisations in Europe have produced many different regulatory requirements in Europe. In some cases these regulatory requirements cover the same areas and overlap or are even contradictory"

Complexity of Regulation:" The quantity and complexity of ATM safety regulatory material is also a problem. A clear, unambiguous safety regulatory framework is needed so that all participants in the ATM system know what is expected of them"

Transparency: "All future standards and regulations should clearly state their safety objectives, provide details on how safety requirements have been derived and record any assumptions that have been used"

Harmonization of Industry Regulation: "The relationship between different regulatory and legislative requirements is currently unclear. This has led to un-coordinated safety targets, different approaches to safety assessments and different classifications schemes for causal factors in incidents across the air transport industry"

Proportionality and Cost Effectiveness: "The complexity of regulatory requirements, variability in implementation and lack of clarity makes if very difficult to determine the true cost or benefits of safety regulation. The future ATM safety regulatory arrangements should:

Ensure that the costs and benefits of safety regulation are known (this includes a validated approach to monitor the safety performance);

Apply safety regulation in a manner that is proportional to the risk that is managed;

Ensure transparency of costing for safety regulation that are related to the economic system of the aviation system (different models might be possible);

Undertake a cost impact analysis as part of the rationale for all new safety regulations."

3.3 WP1.1 Research approach

Regarding this context, ASCOS aims to break this chain of 'stagnation' of safety improvement through introduction of novel and innovative certification adaptations, which will ease the certification and approval process of safety enhancement systems and operations. Within ASCOS, WP1 aims to develop safety based certification process adaptations. As an important first step, WP1.1 aims to analyse the existing regulations and certification processes, in order to identify shortcomings and bottlenecks in these regulations and certification processes.

The considered scope of this analysis refers to a total aviation context, including the domains Aircraft/airworthiness; Operations and FCL; ATM/ANS; and Aerodromes (ADR). The following Figure 4 - Structure of EASA regulations, including the domains considered illustrates this by showing the structure of EASA's regulations addressing these domains.

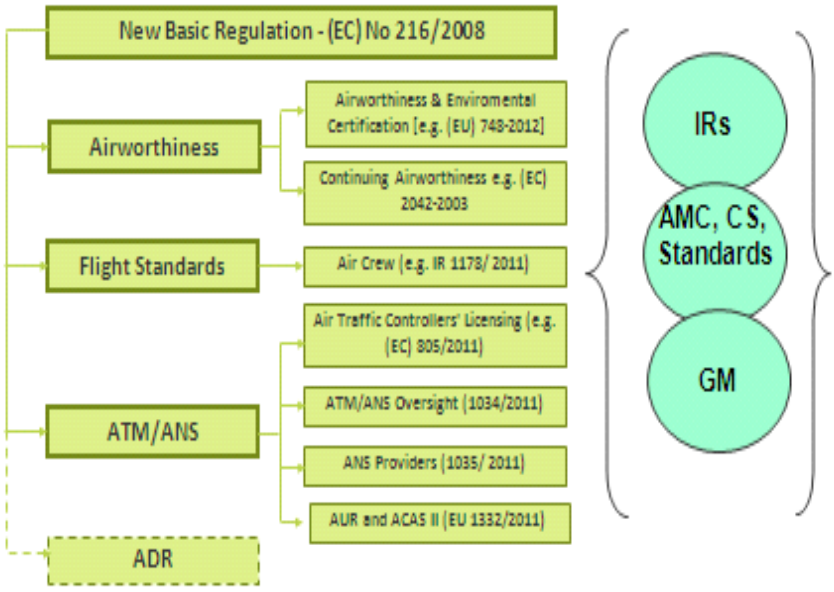

Figure 4 - Structure of EASA regulations, including the domains considered

For each domain (e.g. Airworthiness, Flight Standards….), regulatory framework is structured according to "Hard Law" (IRs Implementing Rules) legally binding and "Soft Laws" (AMC Acceptable Means of Compliance, CS Certification Specifications, or Community Specifications for the Single European Sky, GM Guidance Material) which are highly recommended.

As part of the ASCOS WP1 Certification Process, the objectives of this study are:

- To analyse the existing regulations and certification processes;
- To identify potential shortcomings and bottlenecks in the current certification processes;
- To derive ad-hoc recommendations related to regulatory material for TAS domains (e.g. ADR, ATM/ ANS , Flight Standards…).

Shortcomings and bottlenecks are distinguished as follows:

> A **shortcoming** is '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.
>
> A **bottleneck** is; '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.

As a first step, this study provides a description of existing regulations and certification procedures to be considered in the scope of TAS. This includes a catalogue of existing regulations a catalogue of existing administrative procedures & technical requirements, and a high-level description of the certification-approach in selected domains.

Next, the WP1.1 identifies shortcomings and bottlenecks via two complementary ways. Firstly, an analysis is conducted based on reported safety occurrences and secondly on the degree of implementation level of the regulations in the various domains of aviation (TAS scope). This analysis makes use of data from EASA and SRC annual reports [1, 5]. The underlying assumptions are:

Classes of safety occurrences for which the risk is relatively high or increasing may point to ***shortcomings*** of the associated regulations and certification processes; some of which may be associated to interactions between regulatory domains; and

Areas where the ***implementation level of regulations*** is low may point to ***bottlenecks*** in the associated regulations and certification processes.

To complete these initial outcomes, the approach is including a review of existing studies of identified shortcomings and bottlenecks in the certification process and regulations. Finally the study consolidates the identified shortcomings and bottlenecks.

3.4 Analyse the existing regulations and certification processes

3.4.1 Airworthiness & Continued Airworthiness

Aircraft must be designed, constructed, operated and maintained in compliance with an appropriate airworthiness requirements (notion of Certificate of Airworthiness)

- ICAO Annex 8 contains Minimum airworthiness requirements but Authorities in States have to develop their own regulation based on this ICAO Annex.
- In Europe (and US) airworthiness Certification standards are:
    - For aircraft > 5,7 T CS25
    - For aircraft <5,7 T CS23
    - For helicopters > 2,7 T CS29
    - For helicopters < 2,7 T CS27

The Airworthiness scope is including:

- Performance & operating limitations
- System & equipment design/ installation
- Structural design & construction
- Cabin safety
- Engine & propeller design/ installation
- Operating environment & human factors
- Flying qualities

3.4.2 Flight Operators

ICAO in 1948 has adopted SARPs (Standards And Recommended Practices) for the operation of aircraft engaged in international commercial air transport. ICAO Annex 6 cover areas as aircraft operations, performance, communication and navigation equipment, maintenance, flight documents, responsibilities of flight personnel and the security of the aircraft. Regulations based on ICAO Annex 6 are established by National Operational Authorities.

An Operator may operate an aircraft if an AOC (Aircraft Operator Certificate) has been issued by the relevant operational authority. Annex 6 is addressing responsibilities of States in supervising their operators (e.g. flight crew):

- Method to supervise flight operations,
- Operation manual for each type of aircraft,
- Appropriate instruction (duties and responsibilities) and training for all operational staff within the airline
- Minimum performance operating limitations with respect to aircraft in use (mass, elevation, temperature, weather conditions, runway conditions, take-off and landing speeds under normal and abnormal conditions (failure of one or more power-units)

3.4.3 ANS/ ATM

TAS shall consider CNS/ ATM (Communication, Navigation, Surveillance and Air Traffic Management). ATM is including ATS (Air Traffic Services), ASM (Airspace Management) and ATFM (Air Traffic Flow Management). ICAO Annex 11 is covering descriptions of services and related regulatory requirements (Air Traffic Services). Air traffic control service consists of clearances and information issued by air traffic control units to achieve longitudinal, vertical or lateral separation between aircraft.

ICAO Annex 10 is covering Aeronautical Telecommunications (radio navigation aids, digital data communications, voice communications, surveillance radar data, …).

3.4.4 Airports

In 2003 International Civil Aviation Organisation obliged every Member State to certify all international publicly accessible airports.

ICAO Annex 14 (5th edition 2009) – Requirements concerning certification procedures and guidelines were included in ICAO Annex 14 and Doc 9774 titled Manual on certification of aerodromes. The contents of Volume I reflect, to varying extents, the planning and design, as well as operation and maintenance, of aerodromes:

- Aerodrome data (e.g. runway, pavement, visual approach…)
- Physical characteristics (runways, taxiways, aprons, de-icing facilities…),
- Obstacle restriction & removal,
- Visual aids for navigation (markings, lamps….),
- Visual aids for denoting restricted use areas (e.g. closed runways and taxiways…),
- Aerodromes operating services (e.g. emergency, rescue, wildlife strike hazard reduction),
- Aerodrome maintenance

The content of Volume II are including provisions for heliports.

3.5 Identify potential shortcomings and bottlenecks

3.5.1 Safety Occurrences to be considered

This section collects information from CAT (Commercial Air Transport) safety occurrences reporting from EASA [2] and EUROCONTROL SRC [3]. These data are reflecting evolution of the situation during the previous Years up to now. The objective is to identify classes of safety occurrences for which the risk appears to be high or increasing, since this could point to a shortcoming in certification and regulations.

- LOC-I (Loss Of Control In flight)

LOC-I involve the momentary or total loss of control of the aircraft by the crew. This loss might be the result of reduced aircraft performance or because the aircraft was flown outside its capabilities for control.

- CFIT (Controlled Flight Into Terrain)

CFIT accidents involve the aircraft colliding with terrain while it is still under the control of the crew. Such accidents can be the result of loss of situational awareness or of errors of the crew in managing the aircraft systems.

- SCF-PP (System or Component Failure related to Power Plan)

SCF-PP accidents involve the failure of a system or component directly related to operation of an engine SCF-PP.

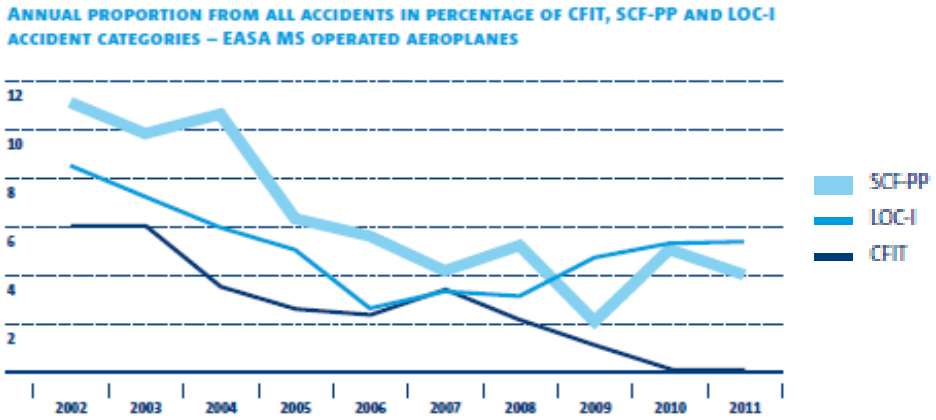

Figure 5 - Source EASA [2] Annual proportion from all accidents in percentage of CFIT, SCF-PP and LOC-I accident categories- EASA MS operated aeroplanes

Figure 5 - Source EASA [2] Annual proportion from all accidents in percentage of CFIT, SCF-PP and LOC-I accident categories- EASA MS operated aeroplanes shows the trend of some of the occurrence categories over

time. The graph is created by calculating the percentage of accidents which have been categorized under the occurrence categories.

From this figure it is evident that CFIT accidents involving EASA MS operated aircraft have an overall decreasing trend over the past decade. This can be attributed to technological improvements and to increased awareness of situations which may lead to such accidents.

A similar trend is also shown for accidents which involve the failure of a system or component directly related to operation of an engine SCF-PP ("System or Component failure related to power plant").

In recent years there has been an increasing trend in the number of accidents involving loss of control in flight (LOC-I).

- RE (Runway Excursion)

The number of severe runway excursions presents an improvement in the recent years. Both accidents and serious incidents involving runway excursions show an overall declining trend. The number of incidents reported shows an increasing trend. The opposite direction of these trends between severe and less severe runway excursions is likely due to improved reporting.

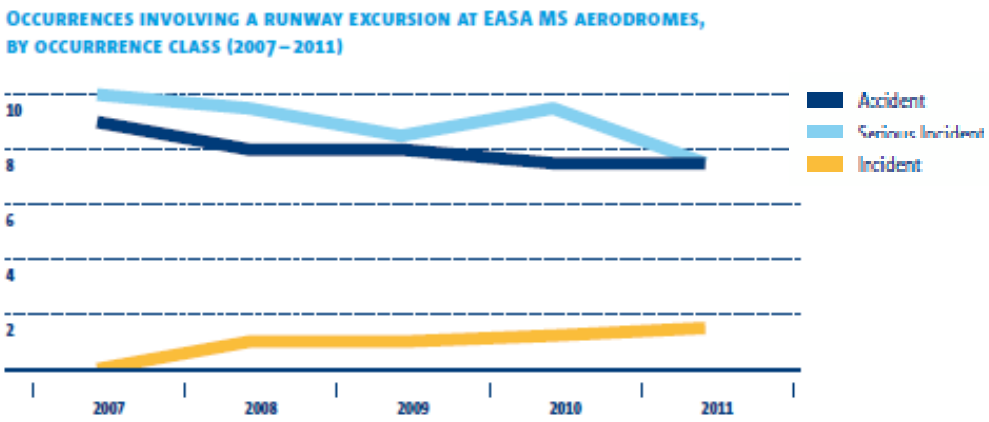

Figure 6 - Source EASA [2] Occurrences (2007-2011) involving a runway excursion at EASA MS aerodrom

Regarding the following incidents categories only a fraction of the related incidents are having an ATM contribution in the chain of events.

- UAP (Unauthorised penetration of airspace)

According to EUROCONTROL SRC [3] concerning the UPA Unauthorized penetration of Airspace (also known as Airspace Infringements) the percentage of serious incidents (severity class A) amounts to 0.3% of the total

number of reported events. This represents a small increase (0.2% in the 2010 data). However, in terms of absolute numbers of occurrences, 2011 shows a considerable increase from 4 to 12 events. The number major airspace infringements decreased, in absolute figures, from 79 in 2010 to 68 in 2011.

However an improvement shall be put in place due to weakness in terms of severity classification. The Figure 5 Classification of ATM incidents (source Eurocontrol SRC [3]) shows the number of ATM-related incidents not severity classified for different categories of incidents. Unfortunately, we see an increase in most areas, especially in Unauthorised Penetrations of Airspace and Separation Minima Infringements.

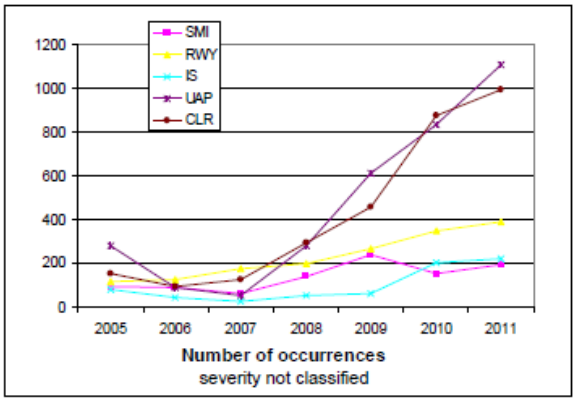

Figure 7 - Classification of ATM incidents (source Eurocontrol SRC [3])

- SMI (Separation Minima Infringement)

According to EUROCONTROL SRC [3] concerning the risk bearing SMI separation minima infringements, compared with the previous year's data, the data reported for 2011 shows a 12.1% increase in absolute numbers and a 5.6% increase when measured against traffic levels:

- Serious incidents (severity class A) increased in absolute numbers from 16 to 35,
- Major incidents (severity class B) increased in absolute numbers from 178 to 217.

- RI (Runway Incursions)

Concerning RI (Runway Incursion in absolute figures, the number of serious runway incursions in 2011 slightly increased (23) compared with the previous year (22), whilst a decrease is shown for major events (from 77 to 62) (source EUROCONTROL SRC [3]).

- IS (Inadequate aircraft Separation)

The Incidents involving "inadequate aircraft separation" are categorised under 'IS'. An improvement is certainly needed - increased number of safety occurrences not classified in terms of severity.

- CLR (aircraft deviation from ATC CLeaRance)

This category includes the Level Busts. Many of these incidents are also categorized as SMI (in the causal chain). An improvement is needed due to an increased number of safety occurrences not classified in terms of severity.

3.5.2 Specific ATM scope

The considered severity classes are the following:

- Severity A serious incidents;
- Severity B major incidents;
- The other classes are severity C (significant), severity D (not determined), severity E (no safety impact).

The category that has the largest proportion of risk bearing incidents (severity A and B) is the SMI (Separation Minima Infringements). This category refers to occurrences in which the defined minimum separation between aircraft has been lost. Many of the incidents that have resulted in a loss of separation and categorized as risk bearing are also categorized as deviation from ATC Clearance or Unauthorized Penetration of Airspace Infringements.

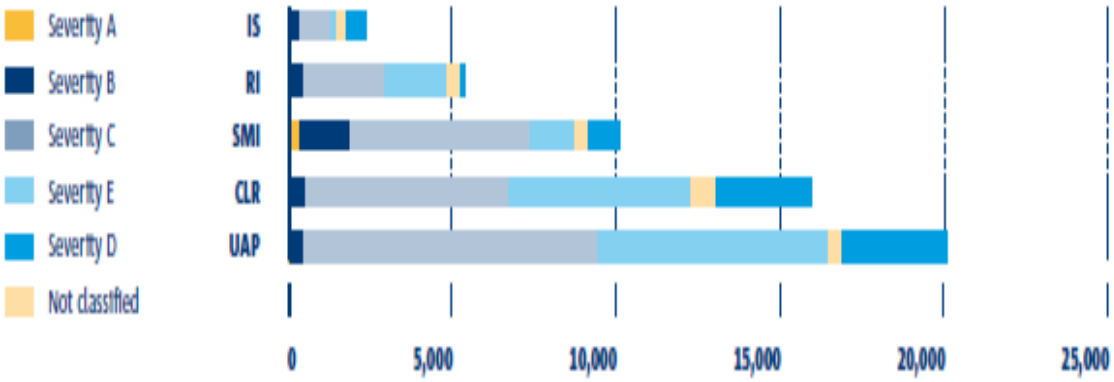

Figure 8 - Number of ATM related incidents by category and severity (2005-2011) [source EASA [2]]

- RI must be considered due to occurrences rates increase in 2010 although 2011 is showing an improvement - Figure 6 Number of ATM related incidents by category and severity (2005-2011) [source EASA [2]].

- SMI refer to occurrences in which defined minimum separation between aircraft, has been lost. With the exception of 2009 and 2010, overall the total number of incidents reported is increasing every year. SMI under **severity A** have a decreasing trend until 2010 followed by an increase in 2011. A similar increase in severity B is

indicated in the preliminary data in 2011 -Figure 6 Number of ATM related incidents by category and severity (2005-2011) [source EASA [2]].

3.5.3 Is Regulation satisfactorily implemented?

Although it is very difficult to assess in a rigorous way the level of implementation of regulatory material in the different TAS domains (airworthiness, Flight operators, airport, CNS/ATM…), it is however possible to distinguish some trends based on miscellaneous published material (see below) highlighting current status and evolution from former years. The following

Figure 9 - Level of implementation of regulatory material in TAS domains summarizes these tendencies.

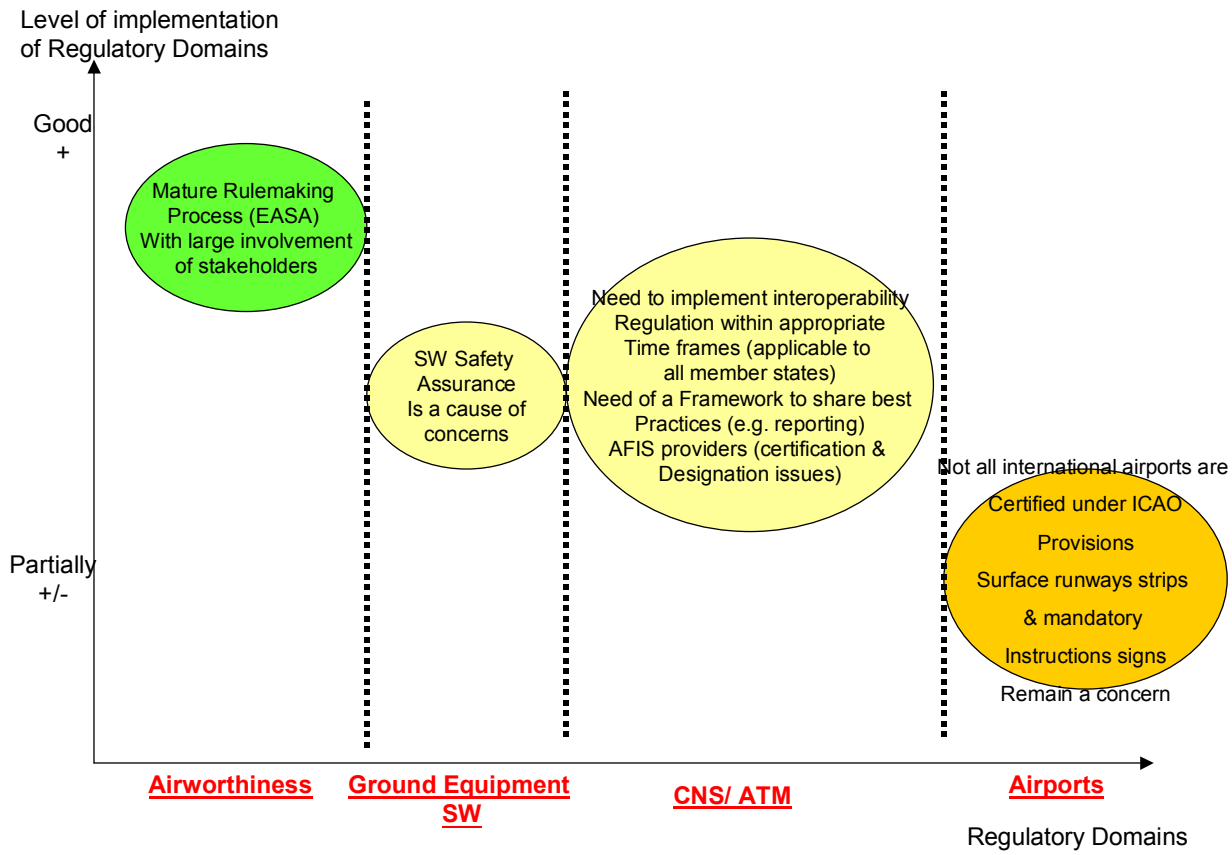

Figure 9 - Level of implementation of regulatory material in TAS domains

- Airworthiness and Continuing Airworthiness:

Basic Regulation (EC) No 1592/2002 of 15 July 2002 with later amendments gave responsibility to the European Aviation Safety Agency for the airworthiness and environmental certification of all aeronautical products, parts, and appliances designed, manufactured, maintained or used by persons under the regulatory oversight of EU Member States. EASA has developed and implemented the Agency's Internal Certification Working Procedures in the following areas: Type Certification, ETSO-Authorisation, Supplemental Type Certification (STCP) and Continuing Airworthiness of Type Design (CAP). Globally there is no major issues regarding the implementation of this regulatory material and the related practices.

- CNS/ATM (to completed)
- Airports

  ICAO provisions

  Not all European international airports are certified under ICAO provisions.

  Amongst other extremely varied level of consistency of national regulations with currently valid ICAO Annex 14 was observed. As for the area of SMS implementation there was also an apparent gap between the current situation and best practices in analysed countries.

  Problems with resources.

  According to EASA Report finding main reason for actual deviation from Annex 14 regulations is insufficient resources and capacities as well as some kind of grandfathered rights for the airport infrastructure. There were also problems with publication of actual deviation in the respective AIP. There were no examples of satisfying solutions anywhere in EU.

  CAA staff problem in many countries.

  Staff shortages, or in other words overworking, lead to common delay in implementation in many countries (especially, if NAAs/CAAs employees are involved in regulatory and legislative processes).

  Not all standards and recommendations are fulfilled among aerodromes surveyed in EASA Report.

  For example at 7 from 56 visited airports Standards and at 34 Recommendation concerning RESA (Runway End Safety Area) were not fulfilled.

- Ground Equipment Software:

Although the maturity of practices has been considerably improved during these recent years through the publication in 2008 of EC482 (Implementing Rule for the CNS/ ATM Software) and the availability of Guidance material and Standards (ED153 in 2009, ED109 in 2002), some remaining issues need to be addressed like:

1. Manufacturers have a tailored approach to cope with various depth of requests and complexity of ANSPs;

2. ED153 and ED109 (the most frequently mentioned) are still at very high level and need application notes based on lessons learnt

3. How should safety requirement issued from the IRs Implementing Rules be considered in the global system/equipment safety assessment? What about the balance between compliance based and performance-based approaches?

4. How can we get a better/common (ANSP/Manufacturer) view of what we really need to do to show compliance with EC482?

5. What should be the content of EC 552 declaration of conformity in relation with safety assessment?

6. COTSs (do we have enough in GM Guidance Material?)

3.5.4 Bottlenecks and shortcomings identification

The purpose is to identify shortcomings and bottlenecks in regulations and certification processes by considering:

- A further analysis of the classes of selected safety occurrences (3.5.1) as described in **step1**,
- The degree of implementation of the regulatory material by considering its implementation level per domain, for which input was collected (3.5.3) as described in **step2**.
- By combining these two "dimensions" and also considering additional aspects like improvements or not during past years of these safety occurrences, number of regulatory domains involved in scenarii, phases of flight related to these scenarii, the notions of shortcoming and bottlenecks of the current regulation and certification process could be highlighted (as described in **step3)**.

Step1 Safety Occurrences scenarii classification

The classification of safety occurrences scenarii is performed according to a ranking of scenarii in 2 levels (high, medium) by combining 2 criterias including the notions of severities and improvements aspects:

- (criteria N° 1) --> consider the severity of safety occurrences: accident, serious incident (severity A),
- (criteria N° 2) --> consider the quantitative evolution of these occurrences (select occurrences categories if there is no improvement for recent years (e.g. number of occurrences absolute or relative).

The ranking of scenarii is performed according to the following rules:

- Importance of scenario High --> if criteria N°1(OK) AND criteria N°2 (OK),
- Importance of scenario Medium --> if criteria N°1 (OK) OR criteria N°2 (OK),

Step2 Identification of Safety scenarii Precursors and related involved TAS domains

For this step of analysis the following approach is followed:

- describe safety occurrences in more details,
- identify potential precursors and related causes according to the previous set of selected scenarios and related safety occurrences, [use some inputs from Accident/Incident models (e.g. CATS, IRP)] in order to highlight involved operations & systems
- consider occurrences figures related to ATM support functions [5] (SRC Annual safety report 2012)
- consider phases of flight related to safety occurrences scenarios (to consolidate identificaton of related TAS domains),
- identify level of contribution of each regulatory domain

The expected outputs should be the list of involved regulatory material consolidated with the related phases of flights, the list of main precursors (and potential causes if possible).

Step3 Initial assessment of regulation influence

The regulation influence is provided through the identification of shortcomings and bottlenecks by taking in consideration for each safety occurrence scenario (CFIT, SMI, ….) the degree of implementation of involved regulatory materials, the number regulatory domains (ATM, Airworthiness, Flights Operations….) and phases of flights:

- Very High Priority (shortcoming & bottleneck) if:

The safety occurrences scenarios induced in the scope of the regulatory domain are high (accident/ incidents severity A), the interaction with the other regulatory domains is very important in the analysis of safety occurrences scenarios.[1] The identified regulatory area is not implemented at the expected level (whatever the reason).

[1] These criteria (safety occurrences scenarios and interaction with other regulatory domains) are combined in order to assess the level of safety risks in the Figure 10 - Regulation influence diagram on safety risks

- High Priority (shortcoming) if:

The safety occurrences scenarios induced in the scope of the regulatory domain are high (accident/ incidents severity A), the interaction with the other regulatory domains is important in the analysis of safety occurrences scenarios. The degree of regulation application is at the expected level.

- Medium Priority (bottleneck) if:

The safety occurrences scenarios induced in the scope of the regulatory domain are medium (not explicitly related to safety occurrences (accident/ incidents severity A). The interaction with the other regulatory domains is less important in the analysis of safety occurrences scenarios. The identified regulatory area is not implemented at the expected level (whatever the reason).

- Satisfactory if:

The safety occurrences scenarios induced in the scope of the regulatory domain are medium (not explicitly related to safety occurrences (accident/ incidents severity A). The degree of regulation application is at the expected level,

Figure 10 - Regulation influence diagram on safety risks

Step4 Additional considerations

Based on similar analysis [7] (FAA Commercial Airplane Certification Process Study (March 2002) or [6] (EASA RIA Process definition) some relevant inputs should be also considered to improve the characterisation of shortcomings or bottlenecks.

Initial Results

The following Figure 11 - Potential influences of Domains Regulatory Frameworks on Safety Scenarii provides an overview of this analysis results considering safety scenarii priorities and regulatory domains according to identified precursors.

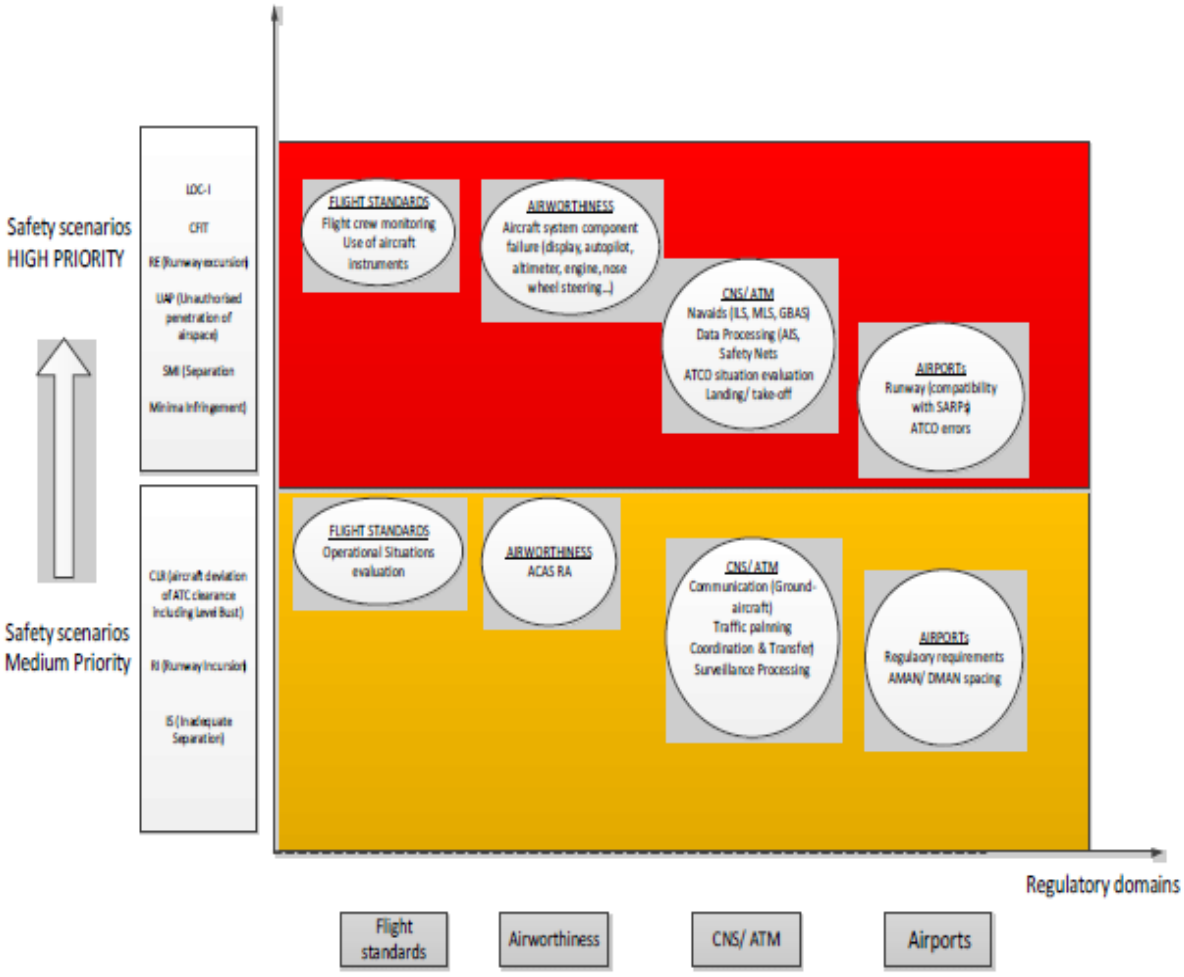

Figure 11 - Potential influences of Domains Regulatory Frameworks on Safety Scenarii

3.5.5 Conclusion and ad-hoc recommendations

An approach was followed that investigated which safety occurrences have relatively high or increasing risk, and which areas have a relatively low level of implementation of regulations. This analysis made use of data from EASA and SRC annual safety reports. The *Figure 12 - Shortcomings and bottlenecks induced by application of regulatory framework* illustrates this approach.

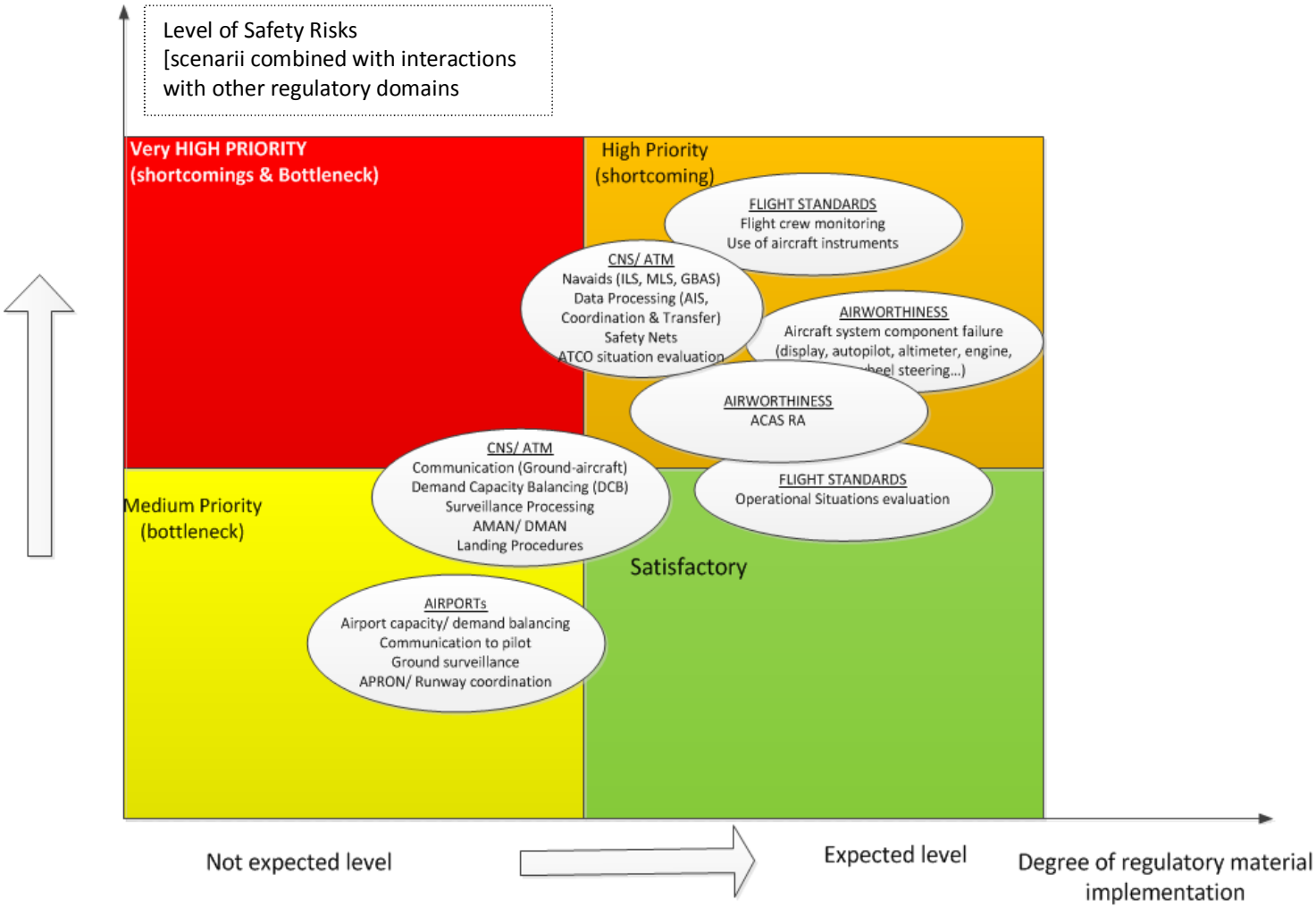

Figure 12 - Shortcomings and bottlenecks induced by application of regulatory framework

The underlying assumptions were:

Classes of safety occurrences for which the risk is relatively high or increasing may point to shortcomings of the associated regulations and certification processes; some of which may be associated to interactions between regulatory domains; and Areas where the implementation level of regulations is low may point to bottlenecks in the associated regulations and certification processes.

The main conclusions regarding shortcomings and bottlenecks in the current regulations and certification processes are:

- In many cases, human errors can be identified as direct cause of the accidents, both when piloting as well as during maintenance works. Elaboration of design techniques in the area of piloting as well as maintenance to better address the avoidance of error-prone solutions is necessary. There is a need for developing adequate regulations addressing the human-machine interface, ergonomics and human limitations aspects, as well as eliminating error-prone solutions. Due to the importance of human factors aspects as source of risks, this aspect must be considered whatever the regulatory domain (airborne and ground).

- Aerodromes: Elaboration of tools ensuring proper and full execution of ICAO Annex 14 SARPs at Aerodromes. Lack of regulatory requirements to provide flight crews with a consistent format of take-off and landing data for all runway conditions. Inadequate regulation for the provision of correct, up-to-date and timely runway condition reports. Currently, no international standard exists for measuring and reporting runway conditions.

- CNS/ATM can be identified as a critical area for safety benefit due to the importance of human factors aspects as source of risks, level of change of operational concepts for the coming years evolving from SESAR, no visible improvement regarding the situation of ATM support functions (e.g. software), and level of implementation of interoperability regulation. Improvements in this field could help significantly in further reducing commercial aviation incidents and accidents. In this context, it should be noted that improving the collection of incidents and accident statistics to better understand the severity of incidents in the CNS/ATM domain may bring additional insight and benefits.

- Existing studies: a review was conducted of existing studies of identified shortcomings and bottlenecks in the certification process and regulations. The main conclusions from this review are as follows: several shortcomings exist in the following certification areas:

  - the aircraft certification process;
  - aviation safety data management;
  - the interfaces between maintenance, operations, certification, major repairs and modifications;
  - the safety oversight process.

- Safety Cases: there are certain risks with the use of safety cases in certification. Various potential shortcomings of the use of safety cases were identified in a military setting, but are of potential interest for the civil domain as well. It should be considered that safety cases

need to be improved due to the current level of maturity of stakeholders regarding this approach.

4 Options to adapt certification and approval processes (D1.2)

The following sections describes the main outcomes of [9].

4.1 What kind of influences regarding D1.1 findings (bottlenecks and shortcoming issues)?

The following *Figure 13 - Principles influencing the reduction of shortcomings and bottlenecks* summarises the factors influencing these identified issues.

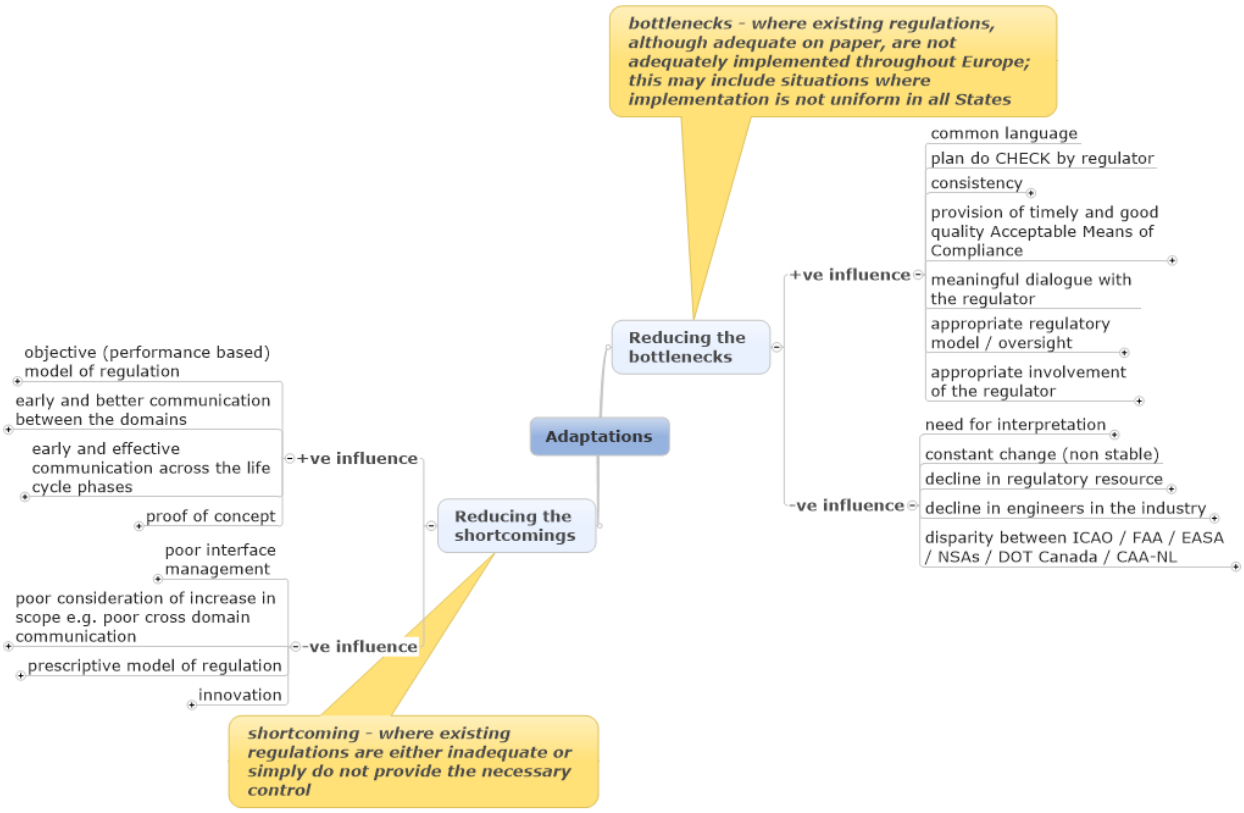

Figure 13 - Principles influencing the reduction of shortcomings and bottlenecks

4.2 Key principles

According to these identified influences, a set of key principles have been derived and adopted to consider the potential options to adapt the certification / approval processes:

- flexibility of regulation model (e.g. performance based vs compliance based),
- communication and consistent notion of risks between TAS domains,

- safety risks evolution and control between TAS domains,
- communication of data between life cycle phases regarding a change of system,
- communication and involvement levels between TAS stakeholders (e.g. regulators, industry),
- impact of technological innovation.

4.3 Derived new options for certification/ approval

Based on the former key principles, brainstorming sessions have identified potential options (in line with these influencing factors) to adapt certification/ approval processes. These potential improvements have been consolidated into eight approaches that can be applied to the Total Aviation System:

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.

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. Abolish all certification by authorities and transform into 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 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.

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.

5. Certify the applicants instead of their products

This process is already put in place to a large extend (DOA, POA etc.).

6. Use of Proof of Concept approach

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 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.

7. Enforce existing rules and 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.

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.

4.4 How to select these options?

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.

Moreover these options have been evaluated and consolidated for the different domains according these 15 criteria (detailed here after):

- Air operators,
- Aircraft & products,
- ATM & ANSPs,
- Ground Equipment,
- Airports.

4.4.1 Primary criteria

The following criteria are considered as primary criteria:

- safety benefits: 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.

- 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.

4.4.2 Additional criteria

- 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.

- 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.

- 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.

- 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 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.

- 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.

- 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.

- 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 worldwide 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 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.

- 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.

- 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.

- 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 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.

- 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.

- 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.

- Feasibility

Feasibility: the outcome of the evaluation of all criteria.

4.5 Conclusions and recommendations of WP1.2

By combining the former criteria the results of the assessment selected the following options as most promising ones:

- 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.

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.

5 Propose an initial approach to implement selected options (D1.3)

5.1 Consider D1.1/ D1.2 outcomes

The following fundamentals derived from the former studies have been particularly considered for D1.3.

- Minimise unnecessary change, recognising the good approaches already in place
- Provide a generic certification framework encompassing the total aviation system (TAS)
- Provide rigorous management of interfaces, both between domains and between the TAS and its environment key aim is to ensure that safety issues (e.g. assumptions, restrictions) are properly addressed and not lost at interfaces
- Allow, within each domain, certification approach to evolve from the current approach keeping the existing approach where no change is required
- Learning lessons from other domains where this gives improvement
- Ensure 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 process where there are:
    - demonstrable benefits and
    - no loss of confidence in the assurance of safety
- Champion / reinforce existing techniques where they are appropriate but not consistently applied
- Provide a mechanism for identification and resolution of further bottlenecks and Shortcomings

5.2 Principles of D1.3 proposed approach

The proposed approach [10] is trying to address the issues as mentioned before and can be summarised as follow. The domains of the TAS are driven by very different approaches of certification. These approaches work well in their respective domains but there is no panacea approach. It means that a common framework needs to be proposed but with a sufficient flexibility level in order to be adapted according to specific aspects of these TAS domains (e.g. already existing standards or methods satisfactorily working). This required flexibility can be supported and facilitated by a notion of modularity. However new technologies or concepts may not be adequately covered by current standards. Then there is a need to express a certain level of claims

without any reference to existing standards or Acceptable Means of Compliance. This is the challenge represented by “Objectives/ Performance” vs “Compliance-based” approaches for the regulatory framework.

Moreover interfaces (e.g. between TAS domains) present a particular concern because, where issues are transferred between domains, it is easy for them to be lost, overlooked or forgotten. The notion of risks and propagation of risks through the different domains of the TAS remains an important issue to be addressed.

ASCOS method focuses on establishing and substantiating a claim that a change to the system will be acceptably safe.

Therefore the selected approach is based on the development of safety arguments with the ability to be developed with a certain level of modularity depending the nature of the change to be certified. The safety argument is underlying every approval approach but it is often implicit. Using a common argument language helps with managing interfaces. Linking arguments with existing approaches helps limit the extent to which the arguments need to be developed. A special attention should be focused on the interfaces between these modular arguments in order to be confident regarding the control of risks propagation between TAS domains.

The core mechanism in the ASCOS method is the development of a justification by adapting, linking or establishing new approval approaches using Safety argument. The justification considers all aspects of the TAS and its environment affected by the change.

The Argument modularisation is used to manage the inherent fragmentation of the system and of the approval approaches Via Assurance Contracts.

The ASCOS method D1.3 reflects a set of activities according to the life cycle of a change and the justification of the claim by starting with identification of the concept and establishing its viability through development and implementation into operation. However, the activities do not depend on a particular lifecycle being followed.

- Modularisation of the Safety argument: The overall safety justification is split into modules aligned to the domains, approval paths, organisational roles and system hierarchy. Module interfaces are defined to manage interdependencies Using Assurance Contracts. The modules can then be developed separately by the owner. Interdependencies need to be managed and agreed between module owners. ASCOS proposes a TAS Engineering and Safety Group (see WP3).

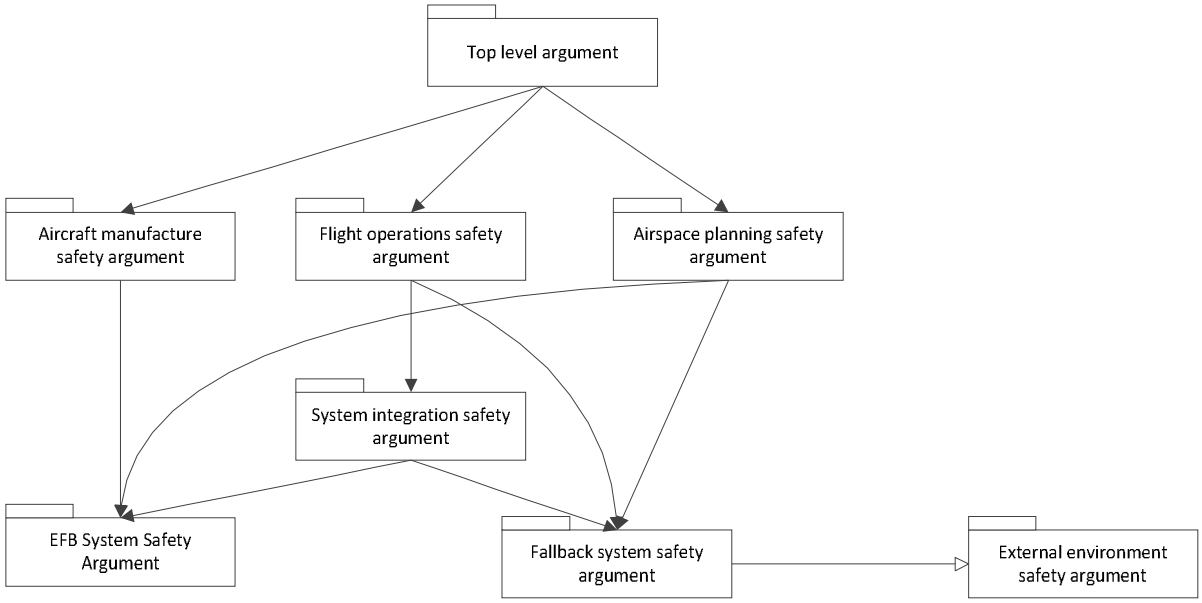

Figure 14 - Modular Safety Argument Architecture for Operation of Electronic Flight Bag (EFB)

- Operational service

The Safety argument extends to the transfer to and ongoing operation of the change post implementation. It can provide the justification for the adequacy of monitoring, change control, and other SMS controls and procedures. Adapted approval approaches can be transferred to existing processes and practices e.g. revised regulations, standards, AMC, guidance, etc. The safety argument can be retained and maintained as a record of the justification behind an approach to be used in future adaptations.

5.3 D1.3 Certification process adaptation description

The stages are defined for application to the "real" TAS. The first application will be in the ASCOS case studies which form WP4, whereas validation of the approach is addressed in WP5. It is intended to use the experience of the case studies and the validation to refine the approach; this will include refinement of the stages defined here. For the case studies, selected ASCOS User Group members are involved to provide assistance and act as "representative" stakeholders and acceptance authorities. The stages of the approach are listed below.

1. Define the change
2. Define the certification argument (architecture)
3. Develop and agree certification plan
4. Specification
5. Design

6. Refinement of argument
7. Implementation
8. Transfer into operation – transition safety assessment
9. Define arrangements for continuous safety monitoring
10. Obtain initial operational certification
11. Ongoing monitoring and maintenance of certification

These stages are aligned with the lifecycle stages and the generic argument is presented here after. In reality depending on the nature of the change (e.g. whether or not the change may be considered 'minor' or 'major') some of the stages may be skipped or combined, but the principles remain the same for each stage. However, it is important to note that the responsible party for each stage of the argument may be different and this means that there can be assurance contracts between the stages as well as between the various components of the system or service. For example an assurance contract will exist between the manufacturer of an aircraft and the operator / maintainer of the aircraft. If progressive certification is adopted, acceptance would be obtained from the relevant authorities following each of the stages listed, in order to derisk the achievement of operational certification.

Supporting the step 2 (argument architecture) several templates arguments have been provided as illustration of Generic Safety argument architecture.

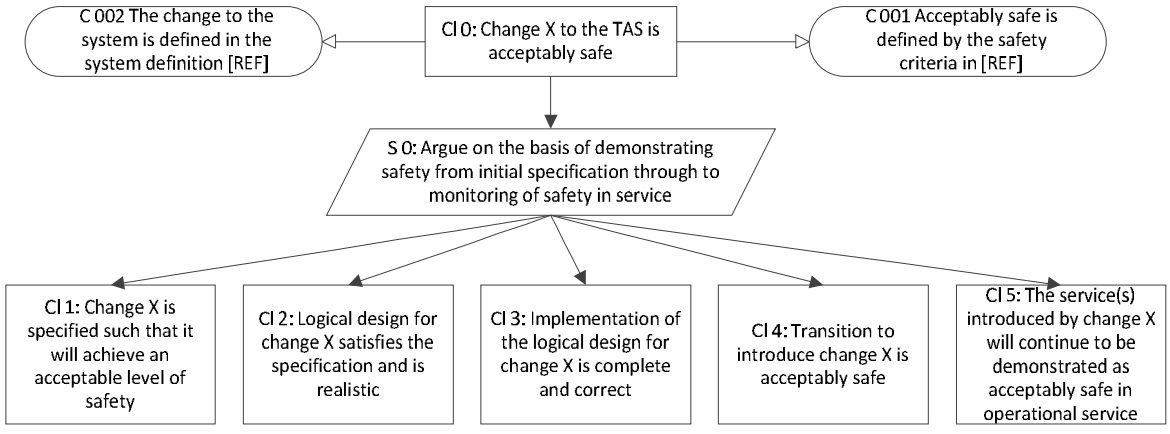

Figure 15 - Generic Safety argument Architecture

The argument is broken down into claims which address the different stages of the development lifecycle[2]. The development of these claims is further addressed in steps of the process. This includes a discussion of the processes used and the outputs of each stage of claim development.

- Cl 1: Change X is specified such that it will achieve an acceptable level of safety: This claim focuses on what is being changed (e.g. introduction of a new concept or service) without considering the details of how the change is implemented. At this stage, the change is considered at the functional specification level, in the context of high level functions, operational behaviour, modes of operation and scenario analysis. (However, even at this level, the change should be partitioned into the different domains within the TAS to facilitate initial development of the argument.) In an ATM argument, for example, this claim is made at the operational level, considering the paths which the aircraft take through the airspace, without considering the tasks or equipment employed to guide them to these paths. This claim includes the performance of the change as specified (including consideration of all normal, abnormal, degraded and emergency conditions) in the absence of failure.

- Cl 2: Logical design for change X satisfies the specification and is realistic: This claim demonstrates that the logical design15 of the change has the functionality and behavioural and performance attributes necessary to satisfy the specification considered in Cl 1. This claim considers all normal, abnormal, degraded and emergency conditions of the operational environment. In addition, this claim considers all the possible hazardous failure modes of the logical design and sets mitigations and assurance requirements such that the system is acceptably safe in the presence of these failures.

- Cl 3: Implementation of the logical design for change X is complete and correct: This claim demonstrates that the physical implementation16 of the change correctly implements the design. As well as directly ensuring that all the requirements are met, this part of the argument also assesses the design to ensure that any inadvertent adverse safety properties are identified and (where appropriate) mitigated. It is to support this claim that detailed assessments of the failure modes of the equipment, people and operations are made.

- Cl 4: The transition to introduce change X is acceptably safe: This claim is concerned with preparing the system (equipment, people and procedures) for bringing it into operational service. It also includes the question of how the system can be brought into service without adversely affecting the safety of the existing on-going operations during the period of the transition from the current operations to the new situation.

- Cl 5: The service(s) introduced by change X will continue to be demonstrated as acceptably safe in operational service: This claim is concerned with (a) ensuring that the a priori safety assessment (made in arguments 1 – 3) is supported by in service evidence (and addressing any deviations of the actual system from the predicted performance) and (b) with ensuring that any changes to the system or its environment are correctly monitored (and that any corrective actions needed are implemented). It is here that

[2] The argument is mapped to the E-OCVM lifecycle [Tableau 1 - Mapping the generic argument to the E-OVCM lifecycle]

complete and accurate identification of the relationship between the part of the system being changed and the rest of the TAS and the external environment is critical: this is necessary so that the correct items in the TAS and the external environment can be monitored and so that corrective action can be taken where necessary.

Argument leg	E-OVCM Life cycle stage
1-Specification	V0 (System Needs): V1 (Scope): V2 (Feasibility)
2- Design	V3 (Pre-industrial development and integration)
3- Implementation	V4 (Industrialisation): V5 (Deployment)
4- Transition	V5 (Deployment): V7 (Decommissioning)
5- Operation	V6 (Operations): V7 (Decommissioning)

Tableau 1 - Mapping the generic argument to the E-OVCM lifecycle

5.4 D1.3 Conclusions

The approach is to build a safety argument for the certification of any change to the total aviation system, supporting the top level claim that the change is acceptably safe. The argument captures the definition of the change including all relevant context (including acceptance criteria and assumptions). The argument is decomposed into supporting claims until the claims can be directly supported. The level of decomposition is limited initially to that necessary to support definition of the interface between the TAS domains, and to dovetail with the existing domain certification approaches. This framework advances the state of the art by driving unification of the argument across all domains.

The approach also includes the concept of modularization, where the overall argument is decomposed into manageable modules, each of which encapsulates the argument for a particular component of the overall argument. The boundary of each module represents the public view of the module and includes a definition of the claims made in the module and associated context, caveats and dependencies. The module boundary definition provides all the information necessary to facilitate linking with other modules. Definition of an interface then makes it possible to establish assurance contracts between modules; this approach is particularly useful when modules are being developed by different organisations as it allows a clear definition of the responsibilities of each. The overall argument architecture consists of the modules and the relationships between them, including the assurance contracts defined.

Modularization drives identification of these interface issues and definition of assurance contracts establishes responsibility for ensuring that these issues are correctly managed both during development and throughout the lifetime of the system.

Even with effective modularization, arguments can become very complex and include significant elements which are outside the responsibility of the applicant proposing the change. To reduce this complexity the proposed approach will avoid unnecessary development of detailed arguments where existing certification practices are sufficient. Nonetheless effective application of the approach requires an argument architect to take the overall responsibility for the development and maintenance of the argument architecture across all the affected domains. (It is recognised that the argument architect is not necessarily responsible for endorsing the overall argument; in fact there may be no single authority competent to do this; careful planning is therefore needed to confirm how endorsement is achieved.) The responsibility of the argument architect extends beyond the introduction of the change, as key elements of the argument will require confirmation throughout the lifetime of the system. There are a number of options for who would take the role of argument architect and, indeed, the role may transfer between parties during the lifecycle of the change. Where the change primarily affects a single domain, the applicant may be best placed to act as argument architect, but where the change is more widespread someone with wider responsibility would be needed to ensure that the implications of the argument are followed through in all domains. This needs to be explored further.

The safety argument approach is flexible, in that it allows retention of existing certification processes within individual domains (thus implementing Option 7), while also ensuring that the context in which the existing certification is developed is fully considered within the overall argument. The flexibility also allows for alternative approaches to be taken where the change being introduced is not covered by existing specifications, thus supporting innovation in process or technology, as required by the overall aims of the ASCOS project. This may involve changes between performance-based and compliance-based approaches (Option 2); it may also introduce approaches from other aviation domains or from other industries (Option 8). It also provides the flexibility to introduce the proof of concept approach (Option 6).

6 Initiate an e-learning environment to support education about adapted certification (D1.4)

In parallel of the studies, a framework of an e-learning environment has been developed to support the dissemination of ASCOS results and facilitate the appropriation of the approaches by the public [11]. The approach about a relevant scope and the way to design the framework was discussed during the User Groups meetings and also with EASA during the dedicated meeting between ASCOS consortium and EASA (April 2013).

A set of training modules were developed to be published through the e-learning environment. Among these modules the following list could be mentioned:

- ASCOS initiative
- Total Aviation System
- Existing regulations & processes
- Proposed certification process
- Safety Performance indicators
- Baseline Risks Picture
- Continuous Safety Monitoring
- Safety databases
- Safety tools/ methods
- Safety Standards

7 Consolidate certification approach by considering lessons learnt (D1.5)

The main goal of D1.5 is to consolidate the initial method developed in D1.3 with findings gathered from WP4 (ASCOS Certification Case studies), WP5 (ASCOS Validation results), and feedbacks from ASCOS Users Group. The outcome of D1.5, called the *ASCOS Method,* responds to the pressures in the aviation industry which are driving innovation and increased integration between domains and therefore making it imperative to streamline approval processes. The ASCOS Method integrates with the lifecycle of a change, from concept through into operational service, introducing activities which lead to building a safety argument supporting the application for approval. The proposed method considers the full impact of the change, and recognises and manages the interaction between domains. The method is also flexible to embrace innovation while encompassing existing established processes wherever appropriate.

7.1 Brief description of the ASCOS Certification Case studies

We present here certification case studies but it should be underlined that the ASCOS Method developed in D1.5 is not just applicable to certification; it is also applicable to more general approvals [12]. Within the ASCOS project timeframe, certification case studies have been specified to cover the steps 1 to 6 of the ASCOS Method:

1. Define the change

2. Define the certification argument (architecture)

3. Develop and agree certification plan

4. Specification

5. Design

6. Refinement of argument

7. Implementation

8. Transfer into operation – transition safety assessment

9. Define arrangements for continuous safety monitoring

10. Obtain initial operational certification

11. Ongoing monitoring and maintenance of certification.

Note: the steps 7 to 11 were not expected to be addressed by certification case studies within the timeframe of ASCOS project.

Below a short description the proposed certification case studies [16]

- RPAS failure management systems (Remotely Piloted Aircraft Systems)

  RPAS is conceived as a modification of a civil cargo piloted aircraft similar in size to an A320. The function of the Autonomous Failure Management system is to detect failures of the RPAS and to respond autonomously to these failures (by reconfiguration of the aircraft systems) with the intention to remain on the original intended flight path.

- Automatic aircraft recovery system

  The objective is to reduce the number of Loss of Control accidents by providing an on-board system (AARS) that can recover the aircraft automatically from Loss of Control or Loss of Situational Awareness events.

- Certificate for de-icers

  The de-icing/anti-icing service provider becomes responsible and accountable for providing a safe service. The air operator is then no longer responsible for a safe ground de-icing/anti-icing service. This is principally a change in responsibilities.

- Integrated surveillance system

  The system includes:

  - Cooperative Surveillance with distributed independent Wide Area Multilateration (WAM) and aircraft dependent ADS-B;
  - Independent Non-Cooperative Surveillance (INCS) composed of a network of “small” Multi-Static Primary Surveillance Radars able to mitigate failures of Cooperative Surveillance systems.

Due to a lack of maturity, some of the certification case studies were addressing only a subset of the steps 1-6. Nevertheless, the objectives of all ASCOS certification case studies were to use the logical safety argument approach, to analyse the risks induced by the change in a context of total aviation and to control these risks according to the complete life cycle of the system (e.g. definition of V0, V1, V2, …).

For this purpose some inputs were considered: from tool for safety risk assessment (WP3), continuous safety monitoring (WP2), area of change list (FAST) giving the TAS domains involved by a change description.

7.2 What are the issues to be taken in consideration from ASCOS Certification case studies?

The added value of ASCOS certification approach is due to the fact that it considers the Total Aviation System from the start of the design and certification activities, and covers the entire lifecycle. However the application of the ASCOS certification approach in the current certification framework introduces additional complexity as a result of the safety argument framework.

For example, the ASCOS certification approach is performance oriented and therefore not suitable for certification of items that cannot be directly linked to performance.

Therefore there is a need to provide additional guidelines about the necessary coordination between stakeholders and domains. These aspects need particularly to be addressed in stages 1-3.

Moreover there is a need also to provide guidelines about the way to balance safety effects across domains. Regarding these issues the outcomes from FAST studies should represent for example very interesting inputs. A common taxonomy of terms such as hazard, safety objective, severity level, safety requirement, etc. should also be refined and referenced in order to support a consistent view of risks management across the different domains of TAS.

Finally, guidance material is necessary to explain how the stages of the ASCOS certification approach can be related to existing, established certification processes. For example the decomposition of safety argument should be stopped at a certain level when existing certification framework works properly. To address this issue it is necessary to be sure that the risks propagation is completely and well addressed through the interfaces between modular arguments thanks to the concept of assurance contracts.

Therefore the main recommendations for D1.5 can be summarised as follow:

- Develop criteria for determining whether the ASCOS certification approach is suitable for a certain case.
- Provide an extensive explanation of the safety argument structure.
- Adapt the terminology so that it is understandable for a wide range of users and domains.
- Adapt stages 4 and 5 by not only considering failure conditions or hazards, but also achieving a certain performance level by the intended function and its design.
- Explain where and how the tools can be used.

7.3 How ASCOS Users Group recommendations are addressed?

Different meetings were organised during ASCOS project, including Users Group meetings and specific technical meetings with EASA and SESAR JU. All the comments and recommendations from these organisations were registered and tracked to check how they progressively have been taken in consideration in the different tasks of WP1 (WP1.1, WP1.2…and WP1.5).

A set of comments were concerning the scope and the approaches already used or promoted in existing regulations or initiatives/ projects. The scope of TAS was mentioned in particular during the first User Group meeting and finally properly addressed in D1.5. Related to this aspect of scope the derived concern of assurance contracts and the way to manage the risks across the life cycle of a change and for all the involved domains was largely discussed during the meetings and considered as a major issue.

Another point of view was also captured including the way to consider "data" and not only "function" regarding risks propagation. A good example seems to be ADQ regulation considering the cooperation between stakeholders for data originating, using, updating….The ASCOS approach is consistent with this alternative point of view of risks propagation.

The very important issue related Human factor aspects is addressed through Guidance of assurance contracts and in the stages of approach. HF is inherent in the whole system and therefore it may not be easy to pull out as a separate item. HF is one item which naturally falls across a boundary between domains. Most precursors identified in WP2 are related to human factors and this could be used to support the D1.5 approach.

The coordination between stakeholders as raised as a major issue during User Groups meetings is properly addressed in D1.5 describing the different roles during the life cycle of a change.

The proportionality issue stating that the most important is to assess the impact of a change rather than the size of a change. The point is considered through the customisation of the argument emphasising that the approach can be tailored in all or part depending of the scale of the change.

Finally even the approach is addressing the complete scope of TAS it remains valid when the severity of risks could change in one domain (e.g. ATM).

7.4 Synthesis of the ASCOS Method improvements done in D1.5

D1.5 uses the same basic safety argument ad D1.3, but changes the focus from a strictly linear lifecycle-based process, to a process focussed on understanding the change and developing an approval path. It also develops further the concept of modularisation, provides much more guidance on how to implement each of the steps of the method, and explains the roles of each organisation involved. The Figure 16 below illustrates these successive steps and more details are given in the following on each step.

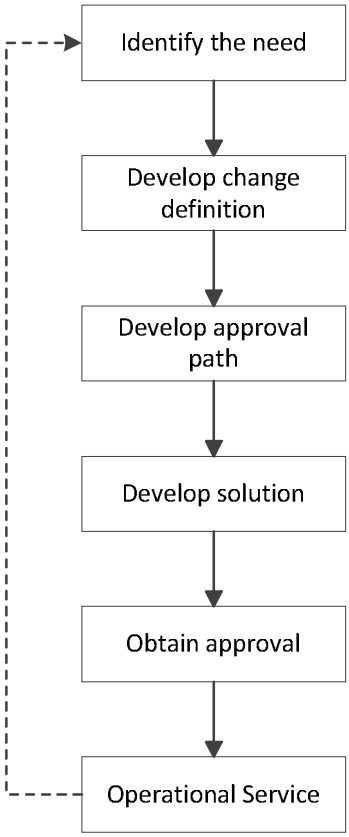

Figure 16 - The change life cycle description

- Identifying the need for change

There are many reasons to make a change to the TAS, e.g. a specific need to improve safety, in response to monitoring current performance (eg using the techniques described in WP2), organisational or structural changes to the TAS (e.g. change in transition altitudes, change in airspace structure), changes to operations (either processes or organisations), introduction of new aircraft, or aircraft component, development of new products.

There is also a need to identify who will be responsible for gaining the approval of the change: may be multiple actors across different aviation domains.

- Defining the change:

The change must be defined sufficiently to understand what is being changed, who is responsible for making the change. This may include multiple organisations but there must be an argument architect who is affected by the change (this should include everyone affected, including effects which may not initially be apparent).

The following items should be considered: what regulations apply to the change, factors in the environment which constrain the change, what level of safety the change needs to achieve, who is responsible for giving permission for the change to enter operational service.

- Deriving the path to approval:

Which approval approaches are followed depend on the nature and domain of the change. For some changes, it will be sufficient to follow existing approval approaches with little or no variation (CS-25, CS-23, SES IR…). For other changes, a new or modified approval path must be defined because no complete path currently exists or because the current path is too costly.

The approval approach is documented in an approval plan and agreed between applicant(s) and the relevant authority/ies before development commences.

- Existing paths to approval: the ASCOS method aims to use existing approaches that are fully applicable to the change being made, fully consider all the impacts of the change, there is no benefit to be gained from improving processes. This objective is supported even existing approaches between different domains may only be loosely coupled (e.g. introduction of a replacement equipment item on board of an aircraft, where the new item has the same fit, form and function as the existing item).

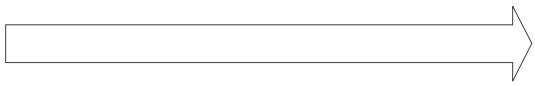

Figure 17 - Approval path using existing approaches

- Incomplete Paths to Approval: For other changes, established approaches will provide the majority of the evidence needed, but with some gaps e.g. the change may introduce a novel component which is not covered by the existing processes, say an aircraft auto recovery system. Here the path to approval may be established by developing processes which cover the novel solution

Figure 18 - Novel solution not fully covered by existing approaches

  - Safety argument is used to help to define the process and bridge the interfaces with the existing solution and the TAS: novel component of change

Figure 19 - New approaches developed to complete the approval path

- High novelty change (e.g. Airborne Separation Assurance Systems)

Figure 20 - Development of entirely new approval path

- Inefficient Path to Approval: In some cases, the existing approaches may be sufficient to provide a path to approval, but a more efficient (and therefore cheaper) approach may be possible (e.g. Electronic flight bag). Safety argument can be used to Compare alternative approaches Demonstrate that the final combination of existing and new approaches is at least as effective as the existing path.

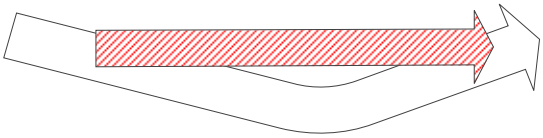

Figure 21 - New approaches developed to provide more efficient approval path

- Approval Path Complexity: Complex or large changes may involve a combination of the approval approaches (e.g. RPAS in non-segregated airspace). Some parts may be approved by existing approaches whereas others may require additional processes to be developed and still others may allow for a more efficient approach. The ASCOS method also addresses the interface between different approval paths and provides guidance on multiple actor approvals.

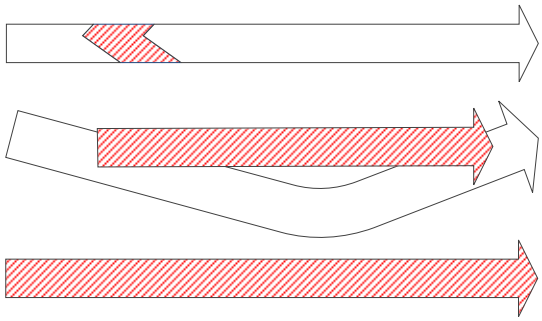

Figure 22 - Different approval paths for different parts of the system

Hence, central to the ASCOS Method is the development of an approval path for the proposed change. This path should follow existing approaches wherever possible, adapting and extending these approaches only where necessary to accommodate parts of the change which are not covered by existing regulations, or where significant efficiencies can be gained. When evaluating existing approaches it is critical to ensure that the validity of the context of the existing approach (including any implicit or explicit assumptions) is fully considered and any differences taken into account.

The approval path should be justified by a safety argument which demonstrates that the change will achieve the acceptable level of safety required by the approver of the change, and this is the purpose of the next point.

- Developing the solution:

The next step is to develop the solution and following the defined approval approach as illustrated in Figure 23. This development is iterative until the development is complete and approval is gained. It is based on three main concepts: the definition of an *acceptable level of safety*, the *modularisation of the argument* and the concept of *an argument architect.*

  - Definition of an acceptable level of safety

The ASCOS Method focuses on demonstrating that the change delivers an acceptable level of safety across the TAS. In other words, the level of safety after the change must be acceptable to all competent authorities who are affected by the change. Note: this does not necessarily mean that an improvement in safety must be demonstrated.

It is therefore necessary to determine appropriate safety targets in each domain affected by the change and demonstrate that each of these is met. Such criteria may be either absolute (specific safety objectives and integrity requirements based on apportionment of a safety target) or relative (comparison of the risk prior to the change against the predicted risk following the change). In the civil aircraft domain, the existence of the target for a catastrophic failure of 10^-9 per flight hour makes it much easier to apportion absolute targets, whereas the absence of (and difficulty of defining and agreeing) similar absolute targets in other domains means that relative targets are often used.

A change which decreases safety (i.e. increases safety risk) in one domain is usually difficult or impractical to justify, even when it significantly increases safety in other domains. To trade off safety between domains, it would be necessary to provide a robust quantification across all domains which demonstrates a significant overall positive impact on safety. Production of such a robust quantification is made more difficult by the fact that different domains use different types of targets (often with different units), making it difficult to create valid comparisons between domains. A corresponding assessment would be needed in the event of a change with differing impacts on different sovereign states.

As a result, each module of the safety argument will need to demonstrate that the change achieves the acceptable level of safety applicable in the domain for which the module is making the safety argument.

Note: It has been recommended in D1.5 that further research should be undertaken to develop the existing models to a level of maturity where such trade-offs between domains could be made.

- Modularisation of the argument

The ASCOS Method addresses the issue of interfaces within the TAS by introducing the concept of dividing the argument into modules aligned to domains of the TAS and organisational responsibilities. Assurance contracts are established between modules to define and manage dependencies between modules.

This approach has the advantages of:

a) making the overall safety argument easier to visualise and understand
b) allowing modules to be developed separately from one another in confidence that the final result will be consistent and correct
c) partitioning the safety argument such that each approver needs only:
    - to consider specified modules of the safety argument
    - to be assured that the assurance contracts at the boundary of those modules are correctly implemented

Modularisation also allows assumptions and dependencies which might otherwise be lost at the interface between domains to be formally agreed and documented – although this is not sufficient on its own: affected parties must also fully understand their responsibilities and commit to meeting them. This is particularly important given that such interface issues are a key concern within the aviation industry

- Concept of an argument architect

The ASCOS Method introduces the role of an argument architect, with the role of designing and maintaining the safety argument, which includes ensuring that the argument modules are correctly bounded and interfaced to other modules throughout the development.

When considering the number of organisations involved in the TAS and their disparate roles, it is often not easy to identify who should be the argument architect. This in part explains why a key concern within the

industry is the inadequacy of the management of interfaces between domains; sometimes integration is supervised by the approver or even ignored altogether.

ASCOS proposes (D3.6) that any complex development should be co-ordinated by a TAS Engineering and Safety Group (TESG); the TESG would be responsible for co-ordinating all the engineering and safety activities involved in the development of the change. The TESG would therefore play the role of argument architect for changes involving multiple organisations.

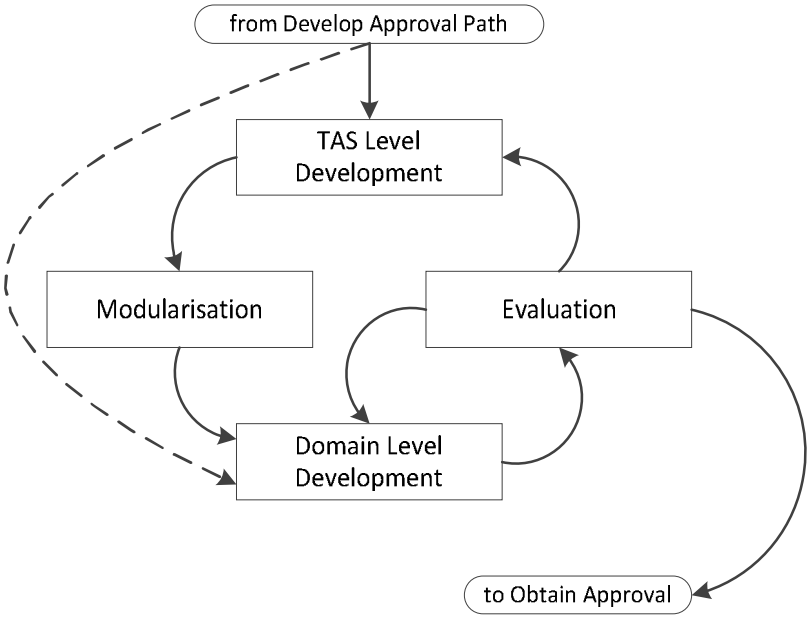

Figure 23 - Iterative workflow of argument development

Conclusions

The ASCOS Programme was established to explore the need for adaptation of existing *approval* processes in response to:

- fundamental changes in the institutional arrangements for aviation regulation in Europe
- the introduction of new technologies and operations
- demands for higher levels of safety performance

Adaptations of approval processes proposed within Certification Process Work Package (WP1) are based on the assessment of issues where no improvement has been observed during the past years. These adaptations aim at delivering as far as possible:

- efficiency in terms of cost and time
- ability to analyse and demonstrate acceptable safety for new concepts and technologies
- ability to analyse and consider the entire aviation system rather than sub-elements in isolation

The scope of WP1 is the Total Aviation System (TAS) which encompasses all stakeholders involved in aviation: products, operators, crews, and aerodromes, ATM, ANS, on the ground or in the air. This large scope is a real and significant added value compared to what exists today.

Identification shortcomings and bottlenecks in existing regulation and certification/approval processes

A key step in an improved certification process is firstly to understand as much as possible how the current regulation could influence at the end the operational safety occurrences in a context of Total Aviation System (TAS). Regarding this clarification an analysis has been performed in D1.1 in order to identify potential shortcomings and bottlenecks in the current certification processes and more generally the regulatory framework. Shortcomings and bottlenecks are distinguished as follows:

A **shortcoming** is '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.

A **bottleneck** is; '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.

The main conclusions regarding shortcomings and bottlenecks in the current regulations and certification processes are:

- In many cases, human errors can be identified as direct cause of the accidents, both when piloting as well as during maintenance works. Elaboration of design techniques in the area of piloting as well as maintenance to better address the avoidance of error-prone solutions is

necessary. There is a need for developing adequate regulations addressing the human-machine interface, ergonomics and human limitations aspects, as well as eliminating error-prone solutions. Due to the importance of human factors aspects as source of risks, this aspect must be considered whatever the regulatory domain (airborne and ground).

- Aerodromes: Elaboration of tools ensuring proper and full execution of ICAO Annex 14 SARPs at Aerodromes. Lack of regulatory requirements to provide flight crews with a consistent format of take-off and landing data for all runway conditions. Inadequate regulation for the provision of correct, up-to-date and timely runway condition reports. Currently, no international standard exists for measuring and reporting runway conditions.

- CNS/ATM can be identified as a critical area for safety benefit due to the importance of human factors aspects as source of risks, level of change of operational concepts for the coming years evolving from SESAR, no visible improvement regarding the situation of ATM support functions (e.g. software), and level of implementation of interoperability regulation. Improvements in this field could help significantly in further reducing commercial aviation incidents and accidents. In this context, it should be noted that improving the collection of incidents and accident statistics to better understand the severity of incidents in the CNS/ATM domain may bring additional insight and benefits.

- Existing studies: a review was conducted of existing studies of identified shortcomings and bottlenecks in the certification process and regulations. The main conclusions from this review are as follows: several shortcomings exist in the following certification areas:

  - the aircraft certification process;
  - aviation safety data management;
  - the interfaces between maintenance, operations, certification, major repairs and modifications;
  - the safety oversight process.

- Safety Cases: there are certain risks with the use of safety cases in certification. Various potential shortcomings of the use of safety cases were identified in a military setting, but are of potential interest for the civil domain as well. It should be considered that safety cases need to be improved due to the current level of maturity of stakeholders regarding this approach.

On top of shortcomings and bottlenecks precisely identified in D1.1, it has been recommended to continue this analysis work with the following activities not yet addressed:

- To analyse the question, based on current certification and rulemaking processes, if there is any overlap between regulatory requirements, and if so how serious is that; an example could be the certification requirements and the operational requirements for standby instruments, which are overlapping and inconsistent. But there may be many more (e.g. for TCAS, ACAS, etc.);
- To analyse the issue of lack of clear accountability for regulated entities in current certification and rulemaking processes; for instance how is accountability organised at European level and at National Level, what is the impact of the Single European Sky (SES) regulations on this, how is the accountability organised between EASA and national authorities, in the various domains, etc….To analyse the issue of inappropriate actual requirements due to technological changes and emerging risks; can we identify inappropriate actual requirements? Most likely there are several issues, e.g. the role of the Flight Management System (FMS) in light of the ever increasing functionality of FMS (e.g. due to introduction of advanced RNP); the requirements for training of rare failure modes (e.g. consider the Airbus France Flight 447, which crashed on 1 June 2009); the currently applicable target levels of safety (are they still appropriate in view of the anticipated changes?).

Key principles influencing the reduction of shortcomings and bottlenecks

The following key principles have been selected in D1.2 as the most promising ones for influencing the reduction of shortcomings and bottlenecks in existing regulation and certification/approval processes:

- Change between performance based and compliance based;
- Proof of concept approach;
- Enforce existing rules and improve existing processes;
- Cross-domain fertilisation.
- 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.

Overview of the ASCOS Method

The Total Aviation System scope, together with the key principles identified through D1.1 and D1.2 obviously imply additional complexity regarding the certification/approval frameworks. Therefore a set of guidance material has been developed to address this complexity. The consolidated outcome of WP1 is what is called the *ASCOS Method* initially developed in D1.3 and then consolidated in D1.5 with findings gathered from WP4 (ASCOS Certification Case studies), WP5 (ASCOS Validation results), and feedbacks from ASCOS Users Group.

The ASCOS Method (fully described in D1.5 [12]) responds to the pressures in the aviation industry which are driving innovation and increased integration between domains and therefore making it imperative to

streamline approval processes. The ASCOS Method integrates with the lifecycle of a change, from concept through into operational service, introducing activities which lead to building a safety argument supporting the application for approval. The proposed method considers the full impact of the change, and recognizes and manages the interaction between domains. The method is also flexible to embrace innovation while encompassing existing established processes wherever appropriate.

Concept of approval path

Central to the ASCOS Method is the development of an approval path for the proposed change. This path should follow existing approaches wherever possible, adapting and extending these approaches only where necessary to accommodate parts of the change which are not covered by existing regulations, or where significant efficiencies can be gained. When evaluating existing approaches it is critical to ensure that the validity of the context of the existing approach (including any implicit or explicit assumptions) is fully considered and any differences taken into account. The approval path should be justified by a safety argument which demonstrates that the change will achieve the *acceptable level of safety* required by the approver of the change, and this is the purpose of the next point.

Definition of an acceptable level of safety

The ASCOS Method focuses on demonstrating that the change delivers an acceptable level of safety across the TAS. In other words, the level of safety after the change must be acceptable to all competent authorities who are affected by the change. Note: this does not necessarily mean that an improvement in safety must be demonstrated. It is therefore necessary to determine appropriate safety targets in each domain affected by the change and demonstrate that each of these is met. Such criteria may be either absolute (specific safety objectives and integrity requirements based on apportionment of a safety target) or relative (comparison of the risk prior to the change against the predicted risk following the change). In the civil aircraft domain, the existence of the target for a catastrophic failure of 10^-9 per flight hour makes it much easier to apportion absolute targets, whereas the absence of (and difficulty of defining and agreeing) similar absolute targets in other domains means that relative targets are often used.

A change which decreases safety (i.e. increases safety risk) in one domain is usually difficult or impractical to justify, even when it significantly increases safety in other domains. To trade off safety between domains, it would be necessary to provide a robust quantification across all domains which demonstrates a significant overall positive impact on safety. Production of such a robust quantification is made more difficult by the fact that different domains use different types of targets (often with different units), making it difficult to create valid comparisons between domains. A corresponding assessment would be needed in the event of a change with differing impacts on different sovereign states.

As a result, each module of the safety argument will need to demonstrate that the change achieves the acceptable level of safety applicable in the domain for which the module is making the safety argument. The building of safety arguments shall be modular and iterative until the development is complete and approval is gained.

Note: It has been recommended in D1.5 that further research should be undertaken to develop the existing models to a level of maturity where such trade-offs between domains could be made.

Modularisation of the argument

The ASCOS Method addresses the issue of interfaces within the TAS by introducing the concept of dividing the argument into modules aligned to domains of the TAS and organisational responsibilities. Assurance contracts are established between modules to define and manage dependencies between modules.

This approach has the advantages of:

a) making the overall safety argument easier to visualise and understand
b) allowing modules to be developed separately from one another in confidence that the final result will be consistent and correct
c) partitioning the safety argument such that each approver needs only:
    - to consider specified modules of the safety argument
    - to be assured that the assurance contracts at the boundary of those modules are correctly implemented

Modularisation also allows assumptions and dependencies which might otherwise be lost at the interface between domains to be formally agreed and documented – although this is not sufficient on its own: affected parties must also fully understand their responsibilities and commit to meeting them. This is particularly important given that such interface issues are a key concern within the aviation industry. And that is also the reason why the concept of *an argument architect* is central n the ASCOS Method.

Concept of an argument architect

The ASCOS Method introduces the role of an argument architect, with the role of designing and maintaining the safety argument, which includes ensuring that the argument modules are correctly bounded and interfaced to other modules throughout the development.

When considering the number of organisations involved in the TAS and their disparate roles, it is often not easy to identify who should be the argument architect. This in part explains why a key concern within the industry is the inadequacy of the management of interfaces between domains; sometimes integration is supervised by the approver or even ignored altogether.

ASCOS proposes (D3.6) that any complex development should be co-ordinated by a TAS Engineering and Safety Group (TESG); the TESG would be responsible for co-ordinating all the engineering and safety activities involved in the development of the change. The TESG would therefore play the role of argument architect for changes involving multiple organisations.

Clarification of the key roles

Another main significant example of the ASCOS Method added value is the development and clarification of the roles of different stakeholders across the certification process steps highlighting the complexity of the TAS aspects in the control of risks (see table below).

Step	Organisation					
	Change Leader (supported by *TESG*)	*Applicant*	*Approver*	*Argument architect*	Manufacturer	Affected Organisations
Identify the need	The need for a *change* may be identified by one or more parties across industry: the type of need will then drive which organisation(s) become *change leader*.					
Develop change definition	Lead definition of change at TAS level	Support development of change definition	Support change definition (provide information about requirements and targets)		Provide information about capabilities of products. Support development on concept.	Provide information about impact of change
Develop *approval path*	Lead definition of *approval path*, in collaboration with individual *applicants* where appropriate	Agree *approval plan* with *approver*	Review and accept *approval plan*	Develop *safety argument modules* as required to support *approval path*	Provide information about compliance with requirements	Provide information about impact of change
Develop solution	Lead development of solution at *TAS* level	Detailed development of relevant *safety argument module* and *assurance contracts* and generation of supporting evidence		Monitor compliance with *assurance contracts* between *modules* and ensure that *safety argument* remains complete, consistent and correct across *TAS*	Develop product(s) and services. Supply evidence to support relevant *safety argument modules*	Monitor impact of solution on organisation's domain / operations
Obtain *approval*	Ensure applications for *approval* are co-ordinated and consistent	Make application for *approval*	Review application and grant *approval*		Provide supplementary evidence as required	Provide supplementary evidence as required
Operational Service	Introduce *change* into operation and monitor occurrences of precursor events or other incidents	Responsible for operation under terms of *approval*	Monitor operator's compliance with their SMS	Maintain argument based on monitoring of performance	Investigate occurrences of precursor events or other incidents	Monitor impact of operation on organisation's domain / operations

Tableau 2 - Participation within the steps of ASCOS Method

Finally, further opportunities for improvement and refinement of the ASCOS Method have been identified. However, the greatest opportunity for improvement will come from application of the ASCOS Method. The ASCOS Consortium commends this ASCOS Method to EASA for adoption as a means of establishing approval for changes to the TAS within Europe.

References

#	Authors(s), Title, Year
1	EASA Annual Safety Review 2011
2	ICAO Aviation Occurrence Categories (Definitions and Usage Notes) (4.1.5) ICAO CAST Commercial Aviation Safety Team May 2011
3	EUROCONTROL Report on the SES legislation Implementation (period January 2011- December 2011) Ed 1.1 (Eurocontrol)
4	EUROCONTROL Safety Team SW Workshop (Lubjiana September 2011)
5	EUROCONTROL SRC Annual Safety Report 2012
6	EASA RIA [Regulatory Impact Assessment] Process template
7	FAA Commercial Airplane Certification Process Study (March 2002)
8	ASCOS, Analysis existing regulations and certification processes (D1.1 report, version 1.3), 2013, Restricted classification
9	ASCOS, Definition and evaluation of innovative certification approaches (D1.2 report, version 1.3), 2013, Restricted classification
10	ASCOS, Outline proposed certification approach (D1.3 report, version 1.2), 2013, Public classification
11	ASCOS, E-learning environment to support certification processes (D1.4 report, version 1.1), 2013, Public classification
12	ASCOS, Consolidated New Approval Method (D1.5 report, version TBD), 2015, Public classification
13	European Commission; ACARE Strategic Research Agenda (SRA) 2, October 2004.
14	European Commission; ACARE Addendum to the Strategic Research Agenda, 2008.
15	European Commission; Flight Path 2050 – Europe's Vision for Aviation – Maintaining global leadership & Serving society's needs, Report of the High Level Group on Aviation Research, ISBN 978-92-79-19724-6, EUR 098 EN, 2011.
16	ASCOS, Evaluation of certification case studies (D4.5 Version 1.0), 2015
17	ASCOS, Validation Results (D5.4), 2015

Note: in order to not list more than 120 references here, it has been decided to give the references of the WP1.1 to WP1.5 reports where more specific references can be found.