Total Aviation System Safety Standards Improvements

J.P. Heckmann, S. Bravo Muñoz, J.F. Delaigue (APSYS), B. Dziugiel (IoA), T. Longhurst (CAAi), B. Pauly (TR6)

The aim of this study is to develop a process to improve the safety standards used at Total aviation system TAS) level and by each stakeholder of the Total aviation system. This is done by defining a common safety standard framework to be used at TAS level and by each stakeholder and by implementing a feedback loop from in operation experience to allow continuous safety standard improvement.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	S. Bravo Muñoz (APSYS)

Grant Agreement No.	314299
Document Identification	D3.5a
Status	Approved
Version	1.3
Date of Issue	12-05-2015
Classification	Public

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	J.P. Heckmann et al.	18/06/2014	All	Version for approval by PMT
1.1	L.J.P. Speijker	22/08/2014		Update by ASCOS coordinator
1.2	L.J.P. Speijker	31/08/2014		PMT comments processed
1.3	J.P. Heckmann	30/04/2015		Revised 2015 issue
1.4	L.J.P. Speijker	15/09/2015		Made publicly available

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	R. Wever, J.J. Scholte, A.L.C. Roelen	11/06/2014
TU Delft	H. Udluft	10/06/2014
Deep Blue	L. Save	10/06/2014
Institute of Aviation	A. Iwaniuk	10/06/2014
Thales Air Systems	B. Pauly	27/08/2014
Avanssa	N. Aghdassi	25/08/2014
CertiFlyer	G. Temme, M. Heiligers	27/08/2014
Organisation Responsible for Approval	Name of person approving the document	Date
APSYS	S. Bravo Muñoz	06/05/2015
NLR	L.J.P. Speijker	12/05/2015

Document Distribution

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

Acronyms

Acronym	Definition
AHM	Airplane Health Monitoring
AiRTHM	Airbus Real Time Health Monitoring
ACMS	Airplane Condition Monitoring System
APU	Auxiliary Power Unit
CMCF	Central Maintenance Computing Function
AoC	Angle Of Attack sensors
APS	APSys, an Airbus Group Company
ARP	Aerospace Recommended Practices
ASCOS	Aviation Safety and Certification of new operations and Systems
ATM	Air Traffic Management
CATS	Causal Model for Air Transport Safety
CICTT	CAST/ICAO Common Taxonomy Team
CMA	Common Mode Analysis
CMC	Central Maintenance Computer
CMS	Centralized Maintenance System
CS	Certification specification (from EASA)
DAL	Development Assurance Level
DAR	Direct Access Recorder
EASA	European Aviation Safety Agency
EASP	European Aviation Safety Plan
ESD	Event Sequence Diagram
ESG	Engineering and Safety Group
EUROCAE	EURopean Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FAST	Future Aviation Safety Team
FDE	Flight Deck Effect
FDM	flight data monitoring
FDR	flight data recorder
FHA	Functional Hazard Assessment

FMEA	Failure Mode and Effect Analysis
FMES	Failure Mode and Effect summary
FOQA	Flight Operational Quality Assurance
GDRAS	Ground Data Replay and Analysis Station
ICAO	International Civil Aviation Organization
IR	Implementing rule
LLR	Lessons Learned Requirement
MCDU	Multifunction Control Display Unit
MOQA	Maintenance Operational Quality Assurance
PCL	Precursor Criticality Level
PSSA	Preliminary System safety assessment
QAR	Quick Access Recorder
RMT	Rule Making Task
SMS	Safety Management System
SA	Safety assurance (from ICAO in operation)
SAE	Society of Automotive Engineers
SARP	Standard And Recommended Practices (from ICAO)
SWIM	System Wide Information Management
SMM	Safety Management Manual (from ICAO)
SMS	Safety Management System (from ICAO)
SRM	Safety Reference Manual (from ICAO)
SRM	Safety Risk Management
SSA	System safety assessment
TAS	Total Aviation system
IVHMS	Integrated Vehicle Health Monitoring system

This page is intentionally left blank

Executive Summary

This study proposes a comprehensive and logical process to improve the safety standards used in total aviation system with a continuous feedback process from experience in operation and from consideration of novelties and future modification of organizations and operational procedures in the Total Aviation System (TAS). It defines also principles for a safety management activity at TAS inter-stakeholder level and at stakeholder level, which should give birth to the standards needed to create the necessary working harmonization. The proposed process is mainly based on:

- The definition of a harmonized safety standards framework applicable at total aviation system (inter-stakeholder level) and at stakeholder level, including standards for the development of products, safety assessments methods, software items development, electronic hardware items development and procedures and services development.
- The development of Lessons Learned Requirement (LLR) for continuous safety standards improvement and product design improvement based on:
    - The identification during the development process of safety event to monitor (safety precursor) during operation.
    - The collection and analysis of events occurring during development testing and during operation including improvement of the safety assurance process by using an automatic capture/coding of safety precursors when occurring during operation.
    - The identification and the consideration of the impact of novelties and future changes in the total aviation system organization, standards and operations.
- The implementation of a safety management activity at TAS level for a coordinated implementation within TAS stakeholders of a harmonized framework for safety standards, for implementation of a continuous in operation feedback for safety standard improvement and for identification of safety issues and decide on mitigation means.

This aims at improving the actual situation where depending on the different stakeholders of the Total aviation system and on the field of application, the set of applicable safety standards is often not complete and not coherent between the different TAS stakeholders. This situation leads to difficulties in communications with the certification authorities and between the TAS stakeholders and may lead to overlook inter stakeholder safety issues. Moreover applying Total Aviation Systems Management in increasingly complex organizations with due consideration of new threats and interactions, requires harmonization of working methods and the setting up of standardized organization rules right from early program phases.

This study builds on previous work in ASCOS WP3 (Safety Risk Management) as well as the outputs of ASCOS WP1 (Certification processes) and WP2 (Continuous safety monitoring). It is compliant with the ICAO Safety Management Manual (SMM) recommendations and with international safety recommended practices from SAE and EUROCAE organizations. Note that this document comprises two volumes: this main document is supplemented by an Appendix with a set of methods for automatic precursor detection and capture in accordance with safety barrier failure oriented taxonomy related to the ASCOS CATS safety risk model.

This page is intentionally left blank

Table of Contents

Content

This page is intentionally left blank

List of Figures

List of Tables

1 Introduction

1.1 Background

The ASCOS project aims at developing certification process adaptations with supporting safety tools to ease certification and safety enhancement in operation of the total aviation system. This study is proposing a process for improvement of the total aviation system safety standards using lessons learned from experience. It proposes a common safety standard framework applicable to each stakeholder of the TAS Consideration of future risks associated to the impact of future changes in total aviation system organization is also part of the study.

Problem: A seamless certification process needs to identify at the very beginning of a development process all the safety activities to perform to show that the final product will be acceptably safe. This is done through the application of safety standards recognized efficient by the certification authorities.

The set of safety standards to use for a product development aims at describing the safety process and safety activities to carry out at each level of a development process: TAS level, Stakeholder level, system level, sub system level, Hardware and software item development level, procedure, and service development level. Depending on the different stakeholders of the TAS and on the field of application, the set of applicable safety standards is often not complete and often does not refer to internationally agreed methods. This situation leads to difficulties in communications with the certification authorities and between the TAS stakeholders.

Approach: In this context a common safety standard framework applicable by each of the TAS stakeholder will help to avoid certification bottlenecks, to avoid identifying certification safety issues late in the certification process, and to give confidence and transparence to the certification authorities on the application of the safety standards.

Nevertheless safety standards should be living documents that should be updated considering the results of their application on product certification performances and on in operation safety behavior of the products. This updating loop will assure the permanent adaptation of the standards to the safety and certification needs while maintaining a seamless certification process.

The ASCOS work package 3.5 is in relation with, and builds on recommendations from, the following other ASCOS work packages:

> In ASCOS "Outline Proposed Certification Approach" (D1.3) in the certification stage 1 (Define the Change), it is requested that "*the safety standards to be used for the change development are identified.*" In this sense this study aims at defining a common standard framework for product development applicable to each stakeholder.

In the ASCOS "Process for Safety Performance Monitoring" (D2.3), it is recommended that "*no matter what approach is chosen for continued airworthiness purposes, it is recommended to address requirements including a common taxonomy and data format, etc. at operator level as well as the potential use of FDM in airlines and ASDG in ATM for continuous safety monitoring at a regulatory level (standard level)*". In this sense, this study develops further concept proposed in D2.3, and recommends a common standard framework for safety continuous monitoring and for deriving Lessons Learned to improve product development safety standards to avoid reoccurrence of safety issues on new product.

In the ASCOS "Total aviation system safety assessment methodology" (D3.1), the recommendations highlight the following:

- It is recommended that: "*management methods have to promote more safety effort in early program phases, in coordination with engineering and certification, the latter considered as a direct product from design justifications. This can be achieved by introducing common framework for organization and development standards with definition of interrelation and responsibilities*". This study develops a common standard framework to apply for process development by any of the TAS stakeholder. A safety management organization to address all the inter-stakeholder activities is also proposed.
- It is recognized that the "*current safety standards in aviation are very domain specific, and it is recommended to promote common standards framework covering the total aviation system. It is suggested to rely on the work done for issuing ARP 4754 Rev A by SAE S18/EUROCAE WG 63 and to introduce recommendations from this study into standardization material applicable to the Total Aviation System*." This study develops a common standard framework to apply for process development by any of the TAS stakeholder.

1.2 Objectives

The main objective of this study is to develop a comprehensive and logical process to improve the total aviation system safety standards with regard to the results of their application. This is necessary to set up and maintain the engineering and safety management requested by the authorities.

1.3 Approach

This approach is to consider future changes in the TAS organization and operational procedures and needs from continuous feedback from experience in operation. This process will be mainly based on:

- The definition of a harmonized safety standards framework applicable at total aviation system inter-stakeholder level and at each stakeholder level.

- The safety standard continuous improvement process considering
    - The identification during the development process of precursor events to monitor during operation.
    - The collection and analysis of events occurring during operation.
    - The development of Lessons Learned Requirement for safety standards improvement.
    - The identification and the consideration of the impact of future changes in the total aviation system organization or operations.
- The implementation of a necessary coordination activity between the TAS partners to assure a coherent and seamless certification activity.

This process will derive proposal of requirements to apply in the development cycle of industrial product. These requirements are called "Lessons Learned Requirements (LLR)". It will identify the safety standards in which the proposed Lessons Learned Requirement and associated means of compliance should be deployed and maintained.

The general principles of the safety standards improvement process are described (in chapter 3). These general principles implementation are detailed following three steps

- Step 1: Harmonization of safety standards documentation within each TAS stakeholder organization. Refer to chapter 4.
- Step 2: Process for Continuous Safety standards improvements using feedback from precursor events in development and in operation. Refer to chapter 5 and 6.
- Step 3: Management activity for a coordinated implementation within TAS stakeholders of a harmonized framework for safety standards for implementation of a continuous in operation feedback for safety standard improvement, for identification of safety issues and mitigation means. Refer to chapter 7.

2 References

2.1 Definitions

- **Product**: in this document the term “product” includes any result of an activity. It may be a system, a sub system, an item, a component, a procedure, a service.
- **Total Aviation System (TAS)**: The TAS includes e.g. aircraft manufacturer, ATM, Airports, Airlines. In this document the airlines are considered only through the operational procedures they should apply, these operational procedures being the results of ATM requests, airport requests, Aircraft manufacturer requests through the aircraft operational documentation (e.g. Aircraft Flight manual, Flight crew operating manual, Master Minimum Equipment List, Maintenance manual) or Airlines internal operational requests
- **Malfunction**: The occurrence of a condition whereby the operation is outside specified limits. A malfunction covers any cause that can make a system to operate outside of specification. It may be the result of a failure (random), an error in design, an error in procedure application, etc.
- **Event**: the occurrence of a malfunction during testing or operation. In this context event is synonym of “Occurrence”
- **Precursors**: “identifiable event that may be used as early warning for known or potential hazards. For more details refer to &5.2.1.2.2

2.2 Applicable and reference documents

- REAIMS European Esprit project: Requirement Engineering Adaptation and Improvement for Safety and dependability (1994- 1996)
- EUROCAE ED79A /SAE ARP 4754A: Guideline for development of civil aircraft and systems
- SAE ARP 4761: Guidelines and methods for conducting the safety assessment process on civil airborne system and equipment
- SAE ARP 5150: safety assessment of aircraft in commercial service, appendix O: lessons learned
- EUROCAE ED 78A: “Guidelines for approval of the provision and use of Air Traffic Services supported by data communications” (WG 53)
- EUROCAE WG 91 document: Recommendations for Revision of ED-78A Volume 1 – Report
- ICAO SMM1: ICAO Safety Management Manual
- Management of risks: Guidance for Practitioners published by TSO (The Stationary Office) on behalf of Office of Government Commerce
- ASCOD D3.1 deliverable: Total aviation safety assessment methodology
- ASCOS D3.2 deliverable: Risk models and accident scenarios
- ASCOS D1.3 deliverable: Development of new certification approach
- ASCOS D2.3 deliverable: Process safety performance monitoring
- Eurocontrol Safety Assessment Methodology
- SESAR Safety Reference Material (SRM)
- European Aviation Safety plan (EASp)
- IR / AMC / GM . from RMT 469/470 working group, (EASA Rule Making Task)

[1] ICAO Safety Management Manual Doc 9859, 2nd edition, Part 9.10

3 Principles for safety standards improvement

3.1 Safety standards

The aim of the ASCOS WP 3.5 is to develop a method to improve safety of the total aviation system by improving development processes and safety assurance processes of TAS elements (product or system) trough improvement of applicable safety standards. This approach needs to:

- Identify the safety standards used by the different stakeholders of the total aviation system for product/service development and certification,
- Identify and evaluate the application status of the safety standards used by the different stakeholders of the total aviation system for in operation safety assurance and lessons learned feed back
- Propose a common framework for safety standards organization generic enough to be applied over the different stakeholders of the total aviation system.

These safety standards and related applicable documents are guideline documents of the safety processes and certification process associated to TAS level or Stakeholder level activities for product development and in operation safety assurance. In the context of this document, the TAS includes the following stakeholders: aircraft manufacturer, ATM, Airports, Airlines, service providers. The activities are structured considering:

- A TAS level with inter-stakeholder activities
- A Stakeholder level with sub-stakeholder activities
- An item level with software/hardware/procedure item development activities

For this study, safety standards cover several levels of applicable documents in relation with certification:

1. The Authority level regulation (e.g. SARPS, CS and FAR regulation for aircraft IR and CS for ATM)
2. The TAS level product development and in operation safety assurance guidelines (e.g. IR / AMC / GM from RMT 469/470 working group, ED78A: Guidelines for approval of the provision and use of air traffics services supported by data communications)
3. The stakeholder level with product development Guidelines (e.g. ARP4754A/ED79A for aircraft stakeholder)) and in operation safety assurance guidelines (e.g. ARP 5150 for commercial airplane in service follow-up)
4. The item level with development guidelines (e.g. DO 178 for software, DO254 for hardware)
5. All the applicable documents (safety plan, Validation/Verification plan, review check lists, etc.) issued at TAS level and at TAS stakeholder level to comply with the level 1, 2, 3 and4 guidelines and necessary for certification

The following sub chapters intend to propose a common safety framework covering level 2, 3, 4 and 5 standard used to structure product development process (System, subsystem, etc.), item development process (Hardware item, software item, procedure item, etc.) and in operation safety assurance process, this approach being generic and applicable by each stakeholder of the total aviation system. Level 1 standards (authority level) are not included as they are under the Authority responsibility. Level 1 standards are inputs for developing level 2, 3, 4 and 5 standards.

3.2 Applicable safety standards and certification documentation for TAS product development

The ASCOS results of WP1 and WP2 on the study of the certification process of the different stakeholders of the total aviation system shows that, due to mainly historical reasons, there is no harmonized approach for stakeholder product development, for certification and for in operation follow up.
If the basic safety assessment methods (FMEA/FMES, PSSA, SSA, CMA, FHA, OSA, Fault Trees, etc.) are more or less similar for each stakeholder of the total aviation system, there is no harmonized standard for product development organization, for certification process and for in operation safety assurance. This induces difficulties in interrelation between the TAS stakeholders and may generate certification bottleneck.

The results of ASCOS WP1.3 (see D1.3) recommend to follow a logical “safety argument framework” approach to provide a basis for unification of multiple certification approaches from multiple domains of the different stakeholders of the TAS (Safety argument approach). However, if this safety argument approach is used on a product development process that is not using structured development standards, it ends up with a very complex argument tree specific to the project considered, difficult to manage and even barely verifiable.

To make the development process generic and limit the complexity of the argument tree it is necessary to identify as soon as possible the safety standards or safety guideline documents that may be applied. If there is no standard available the argument tree should be used to request the stakeholder to develop such standards and make them approved.

The aim here is not to use standards to uniform processes used by each stakeholder of the TAS but to assure harmonization of the processes through the use, by each stakeholder, of the same safety standard framework and the application of identified and recognized standards that are adapted to specificities of each stakeholder but coherent within the standard framework.

In this context, it is worth to request that each stakeholder of the TAS uses the same generic safety standards framework for **organization of product development** and that it is define a safety standard applicable at inter-stakeholder level.

Of particular importance is the overall coordination based on a sound and clear breakdown structure, accurate definition of interfaces of responsibilities. Program phasing and planning dispositions, also standardized, shall be the backbone for implementation.

The application of these standards/guidelines is supporting material for certification considering that the certification is a product from the design justifications and not a stand-alone exercise disconnected from the product development process.

3.3 Generic process for product life cycle and associated safety standards

The figure 1 below shows the lifecycle principles for product development and for elaboration and reuse of lessons learned from experiences during development phases and during "operation" phases.

The process starts with the identification of the safety standards to apply for product development and certification. It ends up with a feedback loop to improve these standards using a continuous improvement process from lessons learned from operation. This process applies at any level of the Total Aviation System. In the following figure the standards are in blue boxes, the product lifecycle phase are in yellow boxes and the feedback loop from events in operation in green boxes.

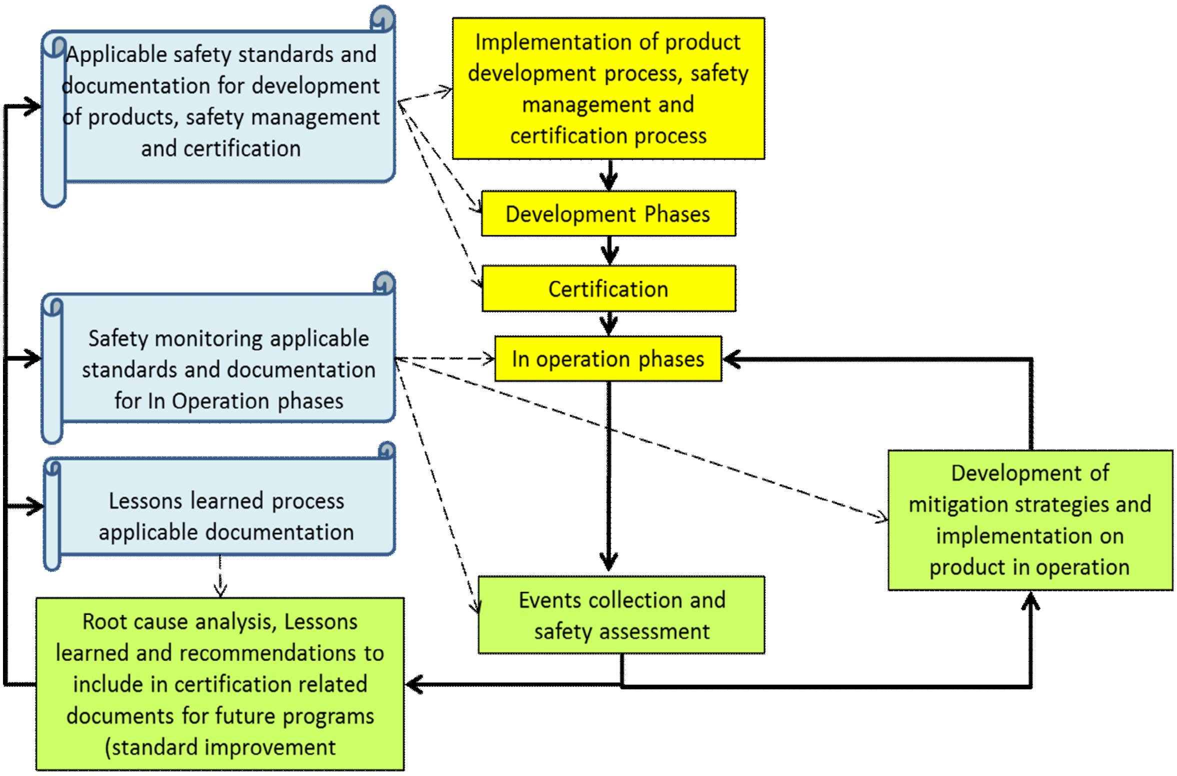

Applicable safety standards and documentation for development of products, safety management and certification
Implementation of product development process, safety management and certification process
Development Phases
Certification
Safety monitoring applicable standards and documentation for In Operation phases
In operation phases
Development of mitigation strategies and implementation on product in operation
Lessons learned process applicable documentation
Events collection and safety assessment
Root cause analysis, Lessons learned and recommendations to include in certification related documents for future programs (standard improvement

Figure 1 Generic process for product life cycle and associated safety standards.

In this figure the roles and responsibilities of the involved stakeholders are not detailed on purpose in order the process remains generic and can be customized in terms of roles and responsibilities by the different stakeholders.

To apply the above generic process, it is necessary to identify the standards and documentation that will be the target of the continuous standard improvement process.

4 Common framework for Safety standards for product in development and in operation

The aim of this section is to propose a common scheme of safety organization for product development and product in operation that can be used as model at each stakeholder level and at inter-stakeholder level.

4.1 Introduction

Due to history and diversified roles, the stakeholders of the Total Aviation System have safety organizations and processes that cannot be described through a unique scheme.

Nevertheless, each total aviation system stakeholder should be compliant to the ICAO SMM[2] models. Taking reference of the ICAO SMM[3], some key aspects can be outlined that depend on the type of activity an organization is dedicated to:

- Design activities
- Operational activities

As per the concepts developed in the ICAO SMM, the SMS (Safety Management System) is to be applied to an organization that may exercise both types of activities, thus exercising activities related to Safety Risk Management (SRM) and Safety Assurance (SA) as part of their SMS. This gives schematically the following workflow of safety activities on which ASCOS proposed enhancements can be added (Figure 2).

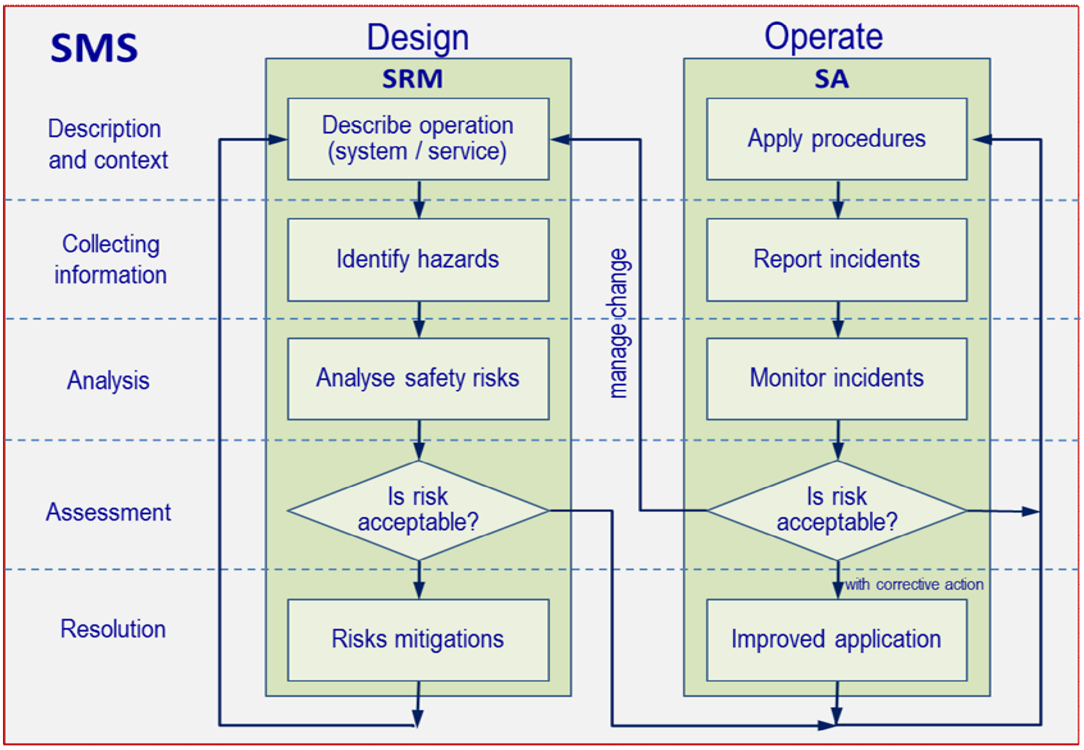


Figure 2 SMS process for SRM and SA

[2] ICAO Safety Management Manual Doc 9859, 2nd edition, Part 9.10
[3] ICAO Safety Management Manual Doc 9859, 2nd edition, Part 9.10

However, a number of stakeholders of the aviation system exercise activities related to the design of products or services, when other stakeholders take duty to operate them. This separation creates a gap between the two activities and highlights the need to keep both SMS parts "connected", i.e. "connecting" SRM and SA by exchanging appropriate safety information:

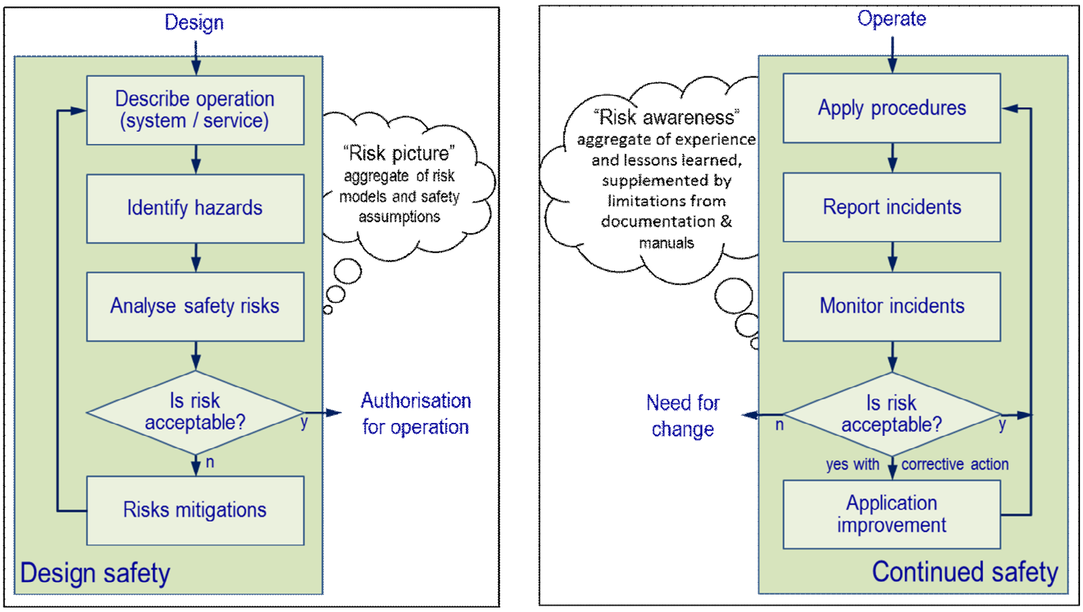

Design
Describe operation (system / service)
Identify hazards
Analyse safety risks
Is risk acceptable?
y
n
Risks mitigations
Design safety
"Risk picture" aggregate of risk models and safety assumptions
Authorisation for operation
Operate
"Risk awareness" aggregate of experience and lessons learned, supplemented by limitations from documentation & manuals
Apply procedures
Report incidents
Monitor incidents
Is risk acceptable?
n
y
yes with corrective action
Need for change
Application improvement
Continued safety

Figure 3 disconnected SMS process

Experience reveals that those in service events are often associated with combination of elements under the responsibility of different stakeholders. These elements are a main part of the safety information that has to be exchanged through "risk picture" and "risk awareness" between the stakeholders and between design activities and in-operation activities. This exchange should be both way.

The proposed following scheme allows harmonization of the development safety activities and in-operation safety activities through standards:

- Allowing identification of the safety precursors during the design,
- Implementing a process of a systematic identification of events precursors in development testing results and in operation,
- Assuring a feedback loop for continuous safety standards improvement.

This would pave the way for commonly shared, "improved risk vision" resulting in a better communication between development and operation and a better anticipation for consolidation of the risks perceived by stakeholders on both sides, and at the end an improved management of safety over multiple organizations.

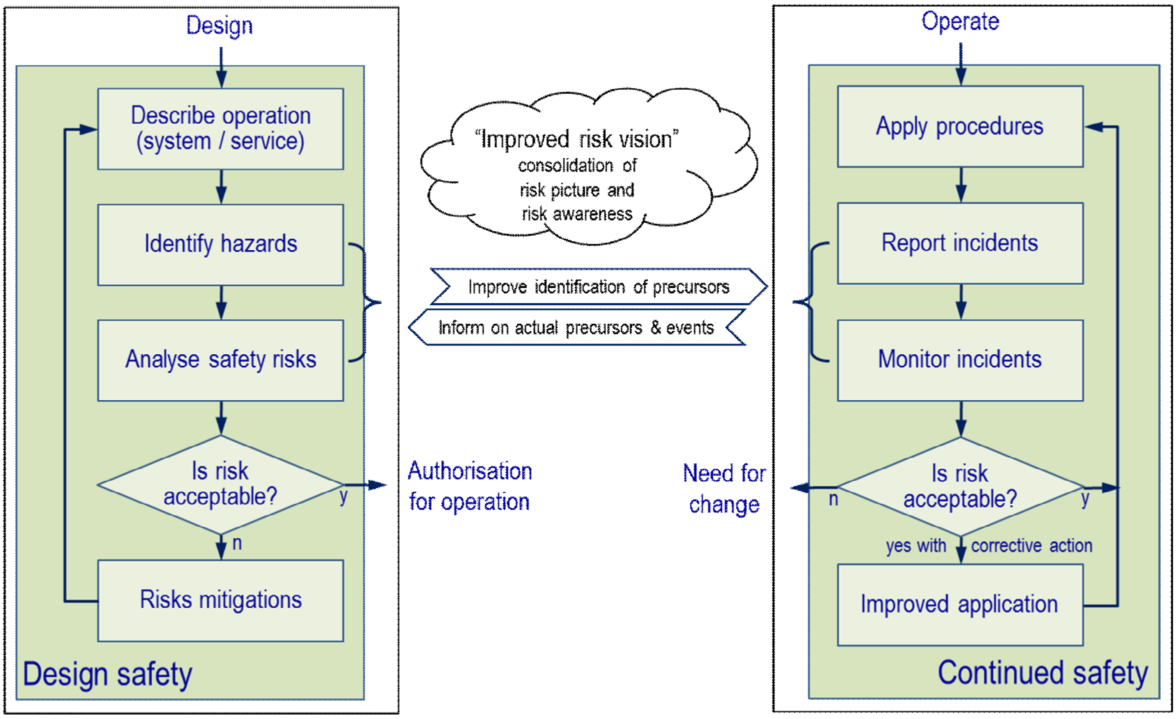

Design
Describe operation (system / service)
Identify hazards
Analyse safety risks
Is risk acceptable?
y
n
Risks mitigations
Design safety
"Improved risk vision" consolidation of risk picture and risk awareness
Improve identification of precursors
Inform on actual precursors & events
Authorisation for operation
Need for change
Operate
Apply procedures
Report incidents
Monitor incidents
Is risk acceptable?
n
y
yes with corrective action
Improved application
Continued safety

Figure 4 Reconnected ICAO SMS process

In addition to the SRM and SA ICAO SMS recommendations, the following standards aims at structuring the product development and safety assurance activities,

- ➢ The IR / AMC / GM from RMT 469/470 working group and the EUROCAE standard ED78A structure the activities at TAS level for development of product associated to data link operation. Even if these documents is still under development they may be considered as a base for the TAS level activity organization especially for the ED78A if its scope is extend to other development activities than data link.

The aircraft airworthiness authorities (EASA, FAA) recommend applying the ED79A/ARP 4754A standards for aircraft system development and the ARP 4761 for safety methods. In addition the ARP 5150 standard is used for aircraft safety assessment in operation. The process models used in these aircraft standards are not only compliant with ICAO SRM models but in some aspects more detailed and clearly oriented toward the application in an industrial context of multiple stakeholders.

These aircraft standards are widely applied by aircraft manufacturers and suppliers. They are:

- The results of international consensus between aircraft manufacturers (including aeronautical system and equipment manufacturers). Both SAE and EUROCAE WG have participated to the development of this process
- Formalized in common EUROCAE/SAE recommended practices (ED79A/ ARP 4754A) for aircraft system development, ARP 4761 for safety methods, ARP 5150 for in operation follow up)
- Applied by all of the aircraft manufacturers in the frame of a CS25 aircraft certification by FAA and EASA

From model of ICAO SRM and from ED/SAE ARP model a generic ASCOS process model can be proposed for describing safety aspects of product development and safety assurance in operation.

4.2 Process model for product development

In the ICAO SMM the Safety Risk Management part gives the principles for a safety assessment process during design that any stakeholder of the total aviation system should apply:

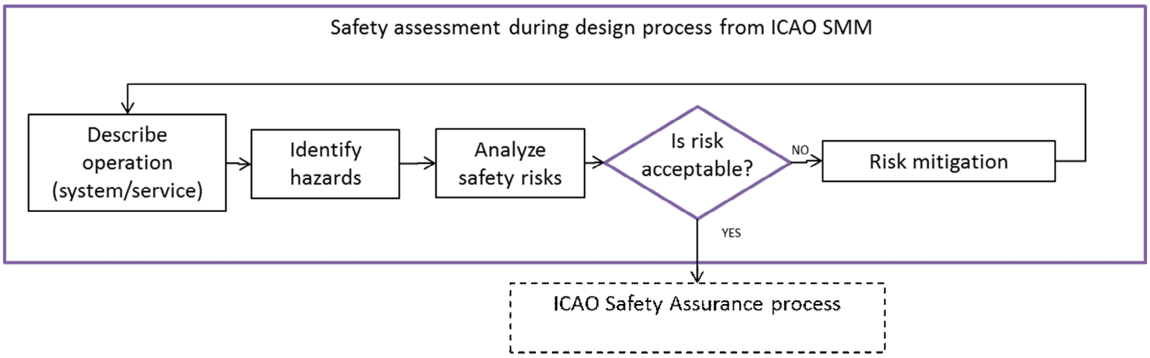

Safety assessment during design process from ICAO SMM
Describe operation (system/service)
Identify hazards
Analyze safety risks
Is risk acceptable?
NO
Risk mitigation
YES
ICAO Safety Assurance process

Figure 5: ICAO model for safety assessment during design/ development

During a product development process, the safety assessment process plays a key role generating safety requirements and assigning the Development Assurance Level (DAL) to function development and item development.

To play this key role the safety assessment process should be embedded in each step of the product development life cycle and should be supported by other safety related processes such as development planning, requirement capture, requirement validation/verification, Development Assurance Level assignment (DAL), process assurance, etc.

All these processes (including the safety assessment process) are called" Integral processes" as they run from the beginning up to the end of the development process of a product.

As recommended by ASCOS WP 3.1 which stresses the need to ensure a tight harmonization of organizations and methods, the recommended industrial practices for a safety oriented development process should be organized around:

- A coordinated planning activity to issue the product development planning with the mandatory milestones and a sound and clear Work break down structure with clear interfaces and
- The implementation of 8 safety oriented integral processes:
  1. Safety assessment process: to define safety objectives and showing compliance with these objectives
  2. Development Assurance Level (DAL) assignment process: to mitigate development errors
  3. Requirement Capture process: to assure that all requirement sources are collected

4. Requirement Validation process: to assure that requirement list is complete and that each requirement is correct
5. Requirement verification process: to assure that validated requirement are applied
6. Configuration management process: to control the configurations of the systems
7. Process Assurance: to assure that all the development process activities are performed in accordance with the various plans that structure these activities.
8. Certification and regulatory authority coordination process: to assure the interface with the authorities

Each integral process should be structured in the same way:

- A plan describing, in accordance with the development plan, the activity organization and its management, the tasks to perform, the responsibilities, the deliverables associated to each task.
- Method document to describe how to perform the tasks described in the plan
- Technical deliverables resulting from the application of the methods and the plan

Models for a development process with such an organization are given in the ED79A /ARP 4754A for aircraft and system development.
These models are generic enough to be applied to the development process of each stakeholder of the total aviation system. These models are illustrated in following figures 6 and 7.

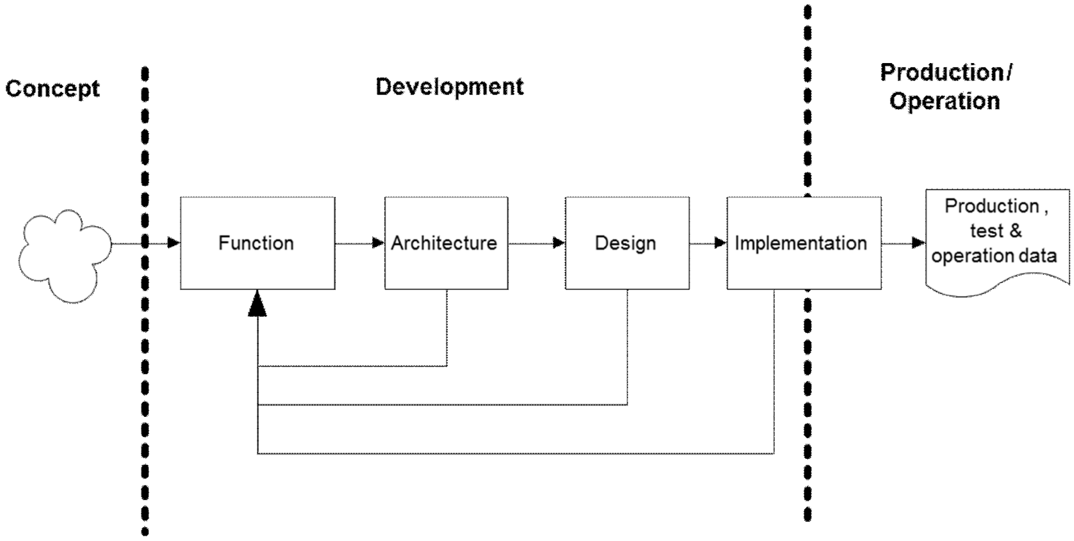


Figure 6 - Product development life cycle (derived from ED79A /ARP 4754A)

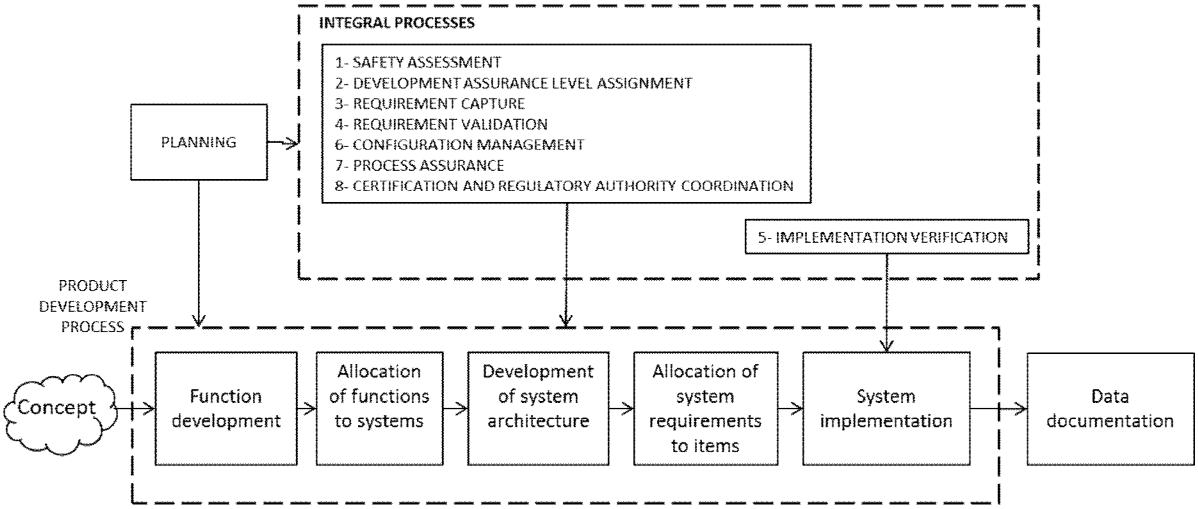

INTEGRAL PROCESSES
1- SAFETY ASSESSMENT
2- DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT
3- REQUIREMENT CAPTURE
4- REQUIREMENT VALIDATION
6- CONFIGURATION MANAGEMENT
7- PROCESS ASSURANCE
8- CERTIFICATION AND REGULATORY AUTHORITY COORDINATION
5- IMPLEMENTATION VERIFICATION
PLANNING
PRODUCT DEVELOPMENT PROCESS
Concept
Function development
Allocation of functions to systems
Development of system architecture
Allocation of system requirements to items
System implementation
Data documentation

Figure 7- Development process model including integral processes (derived from ED79A/ARP 4754A)

In the above organization the steps of the ICAO SRM model (see figure 2) are included in the "Safety assessment" integral process that aims at defining safety objectives and showing compliance with these objectives. All the other integral processes are not detailed in the ICAO SRM but are necessary to assure an efficient safety oriented development and to perform efficient safety assessment activities.

The approach proposed in ASCOS is to consider these models as a framework applicable at the level of each stakeholder of the total aviation system.

4.3 Model for Safety Assurance Process in operation

This paragraph aims at establishing an ASCOS model for Safety Assurance in operation that can be shared by all the stakeholders of the total aviation system.

The ICAO SRM model for Safety Assurance in operation is illustrated below:

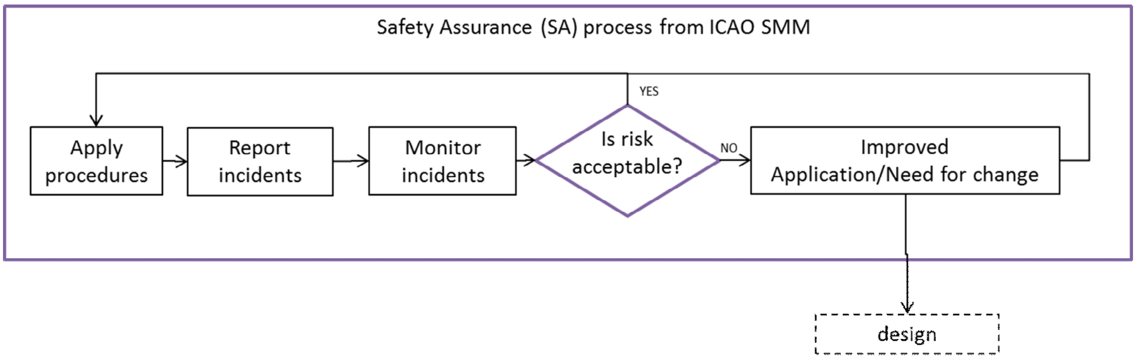

Safety Assurance (SA) process from ICAO SMM
Apply procedures
Report incidents
Monitor incidents
Is risk acceptable?
YES
NO
Improved Application/Need for change
design

Figure 8: Safety assessment (SA) process from ICAO SMM

A similar process is applied for "aircraft safety assessment in commercial service". It is described in the SAE recommended practice ARP 5150.

The ARP 5150 model is illustrated in the following figure:

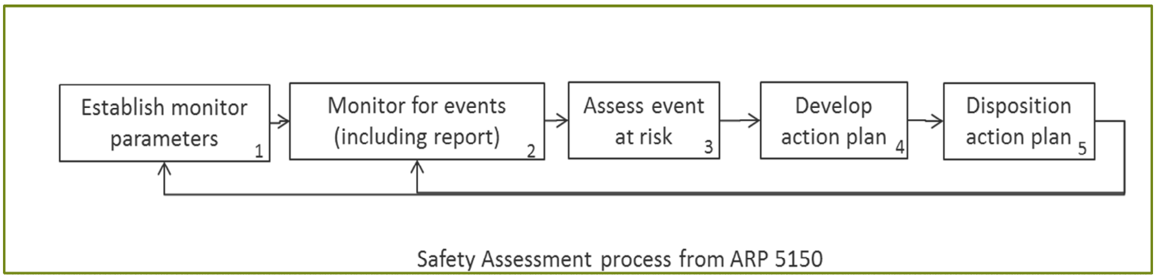

Establish monitor parameters 1
Monitor for events (including report) 2
Assess event at risk 3
Develop action plan 4
Disposition action plan 5
Safety Assessment process from ARP 5150

Figure 9: ARP 5150 Safety assessment process for aircraft in commercial service

The ARP process is compliant with the ICAO SRM Safety Assurance process principles, but more detailed in order to be applied in the aircraft industrial context of multiple stakeholders. In particular, the ARP process recognizes a step for "Establishing monitor parameters" and a step for "developing action plan".

- "Establishing monitor parameter": this step is necessary to identify the event that should be monitored in operation. In the ASCOS project this step will allow the link with the design process where a" precursor identification" activity can be performed.

- "Developing action plan": This step is necessary to propose for acceptance by the authorities the mitigation means to implement on aircraft products to restore the safety level as well as the planning of this restoration.

The relations between the two models are illustrated in figure 7 below.

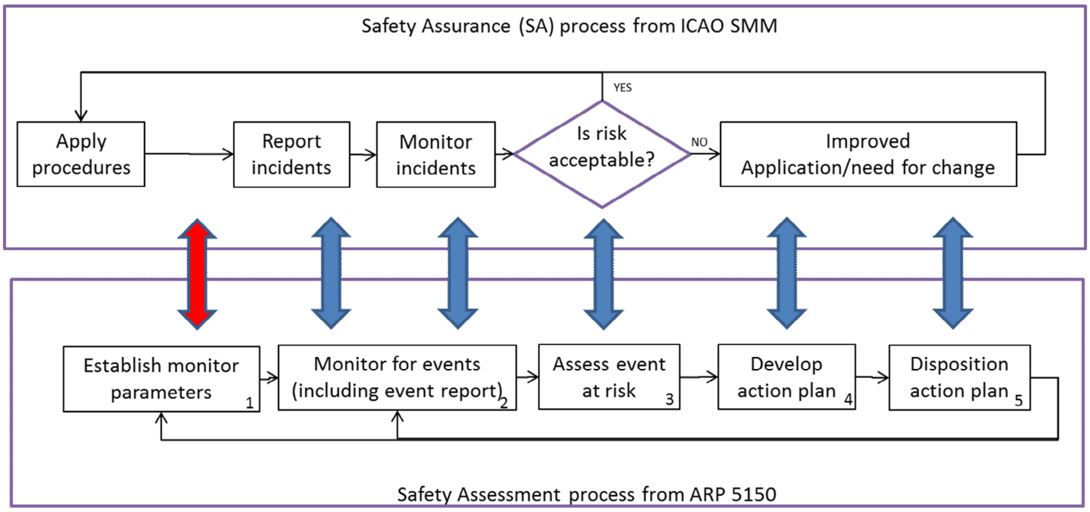

Safety Assurance (SA) process from ICAO SMM
Apply procedures
Report incidents
Monitor incidents
Is risk acceptable?
YES
NO
Improved Application/need for change
Establish monitor parameters 1
Monitor for events (including event report) 2
Assess event at risk 3
Develop action plan 4
Disposition action plan 5
Safety Assessment process from ARP 5150

Figure 10: Safety assessment process from ARP 5150 for aircraft in commercial service

From the two above models we can build an ASCOS model for Safety Assurance in operation. This model is illustrated in the following figure:

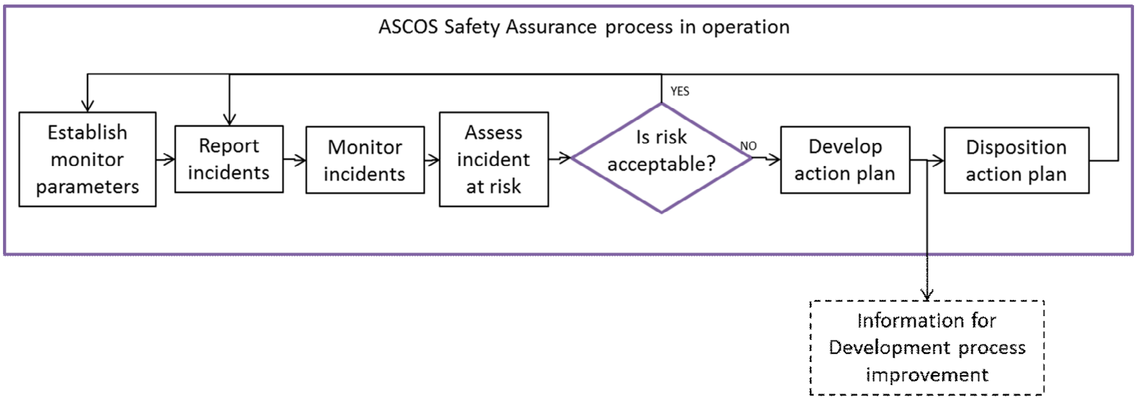


Figure 11: Safety assessment process for TAS product in operation

ASCOS WP 3.2 (see D3.2 deliverable) has proposed a process of safety improvement of the Total Aviation System based on determination of accident precursors and safety barrier malfunctions.

It is worth noting that these processes merge naturally into the generic steps of ASCOS in operation Safety Assurance process and can be used for improvement of a standard for TAS "Product Safety Assurance in operation". This is illustrated in the following figure:

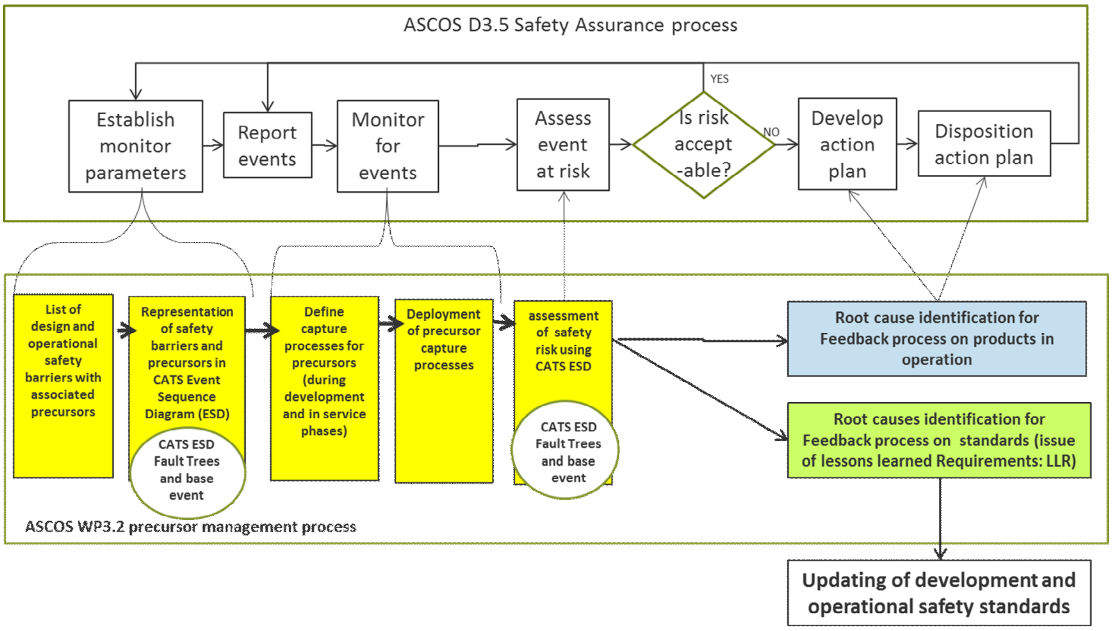

ASCOS D3.5 Safety Assurance process
Establish monitor parameters
Report events
Monitor for events
Assess event at risk
Is risk accept -able?
YES
NO
Develop action plan
Disposition action plan
List of design and operational safety barriers with associated precursors
Representation of safety barriers and precursors in CATS Event Sequence Diagram (ESD)
CATS ESD Fault Trees and base event
Define capture processes for precursors (during development and in service phases)
Deployment of precursor capture processes
assessment of safety risk using CATS ESD
CATS ESD Fault Trees and base event
Root cause identification for Feedback process on products in operation
Root causes identification for Feedback process on standards (issue of lessons learned Requirements: LLR)
ASCOS WP3.2 precursor management process
Updating of development and operational safety standards

Figure 12: Detailed safety assurance process in operation

From the ASCOS WP3.2 results, the process described above starts with a list of precursors to monitor. It ends up with a continuous feedback from in operation lessons learned process aiming at improvement of the products in operation and at improvement of the standards used for product development. This is illustrated in the following figure.

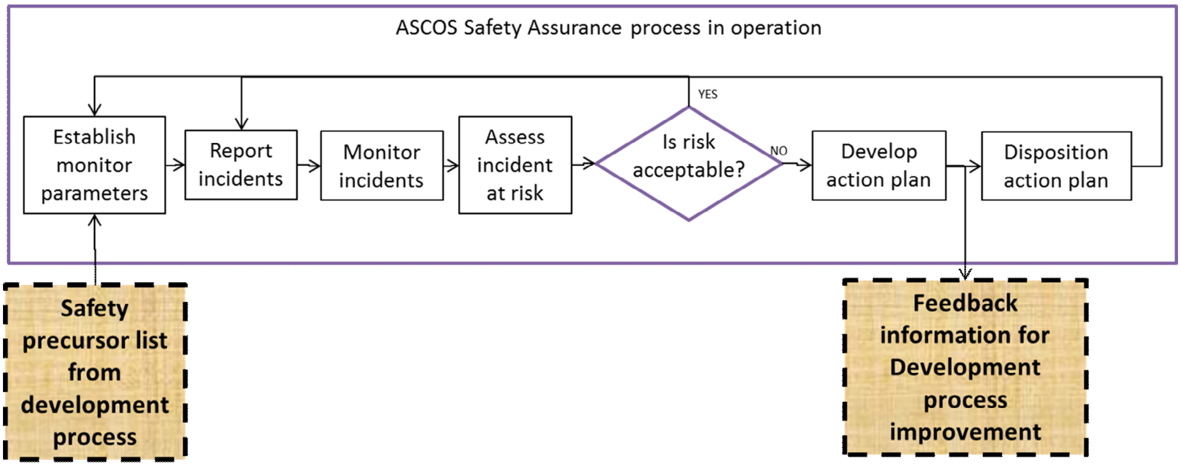

ASCOS Safety Assurance process in operation
Establish monitor parameters
Report incidents
Monitor incidents
Assess incident at risk
Is risk acceptable?
YES
NO
Develop action plan
Disposition action plan
Safety precursor list from development process
Feedback information for Development process improvement

Figure 13 Safety assurance process in operation with links with development process

The description of the tasks associated to each step of the process should be part of a standard for "total aviation system Safety Assurance in operation".

Note: The list of the precursor events to monitor during operation is an output from the development process. The precursors are identified during the development process (particularly through the safety assessments process). The way to identify the precursors is described in ASCOS WP3.2 deliverable (D3.2).

Even if each stakeholder adopts the same model for safety assurance in operation, the details of the activities at the level of each actor of the assurance process will have to be customized considering the different stakeholders of the TAS.

As examples:

- For Aircraft assurance processes in operation all the detailed activities and deliverables at the level of the aircraft manufacturer, airlines, suppliers, and authorities are described in the SAE ARP 5150 international standard.
- For ATM assurance process in operation there is no common standard applied by the different ATM organizations in charge of ATM management in the different European countries. The processes may defer depending on the nations responsible for ATM management in its zone of influence. As an example for UK the reference document recommended by CAA is “Management of Risk: Guidance for Practitioners” published by TSO (The Stationary Office for other countries this document is not the reference)

An effort in standardization of all the assurance process activities at the level of each nation and at the level of each stakeholder of the ATM activity is necessary to have a coherent approach between all the ATM stakeholders and assure compatibility with the safety assurance process used for aircraft (airworthiness monitoring). An effort in the standardization of the data exchanged between the safety assurance processes of the different stakeholders of the TAS is also necessary.

4.4 Recommended common framework for safety standards applicable during product development and product in operation

4.4.1 Recommended common framework for safety standards organization at TAS stakeholder level

To be applied efficiently all along an industrial process of the TAS, the product safety activities during development and all the activities for Safety Assurance in operation should be described through standards and standards applied by each stakeholder of the total aviation system.

The SRM ICAO model does not give information on the standard organization that can support the product development process, and the safety assurance process in operation.

To be performed efficiently, the tasks associated to a safety oriented development process should be described in an applicable document (industrial standard) and then implemented in accordance with the standard requirements.

The minimal structure for standards is:

For development process:

- A standard for safety oriented product development,
- A standard for the methods to use for Safety assessment activities supporting the development process,
- One or several standards for development of items (e.g. software item, hardware item, procedure and services items).

For safety assurance in operation:

- A standard for safety assurance in operation including a process for Lessons learned feedback loop for development process.

An example of such standard organization is given in the ED79A/ARP 4754A for aircraft product development. The following figure illustrates how the guidelines documents are structured within this standard framework.

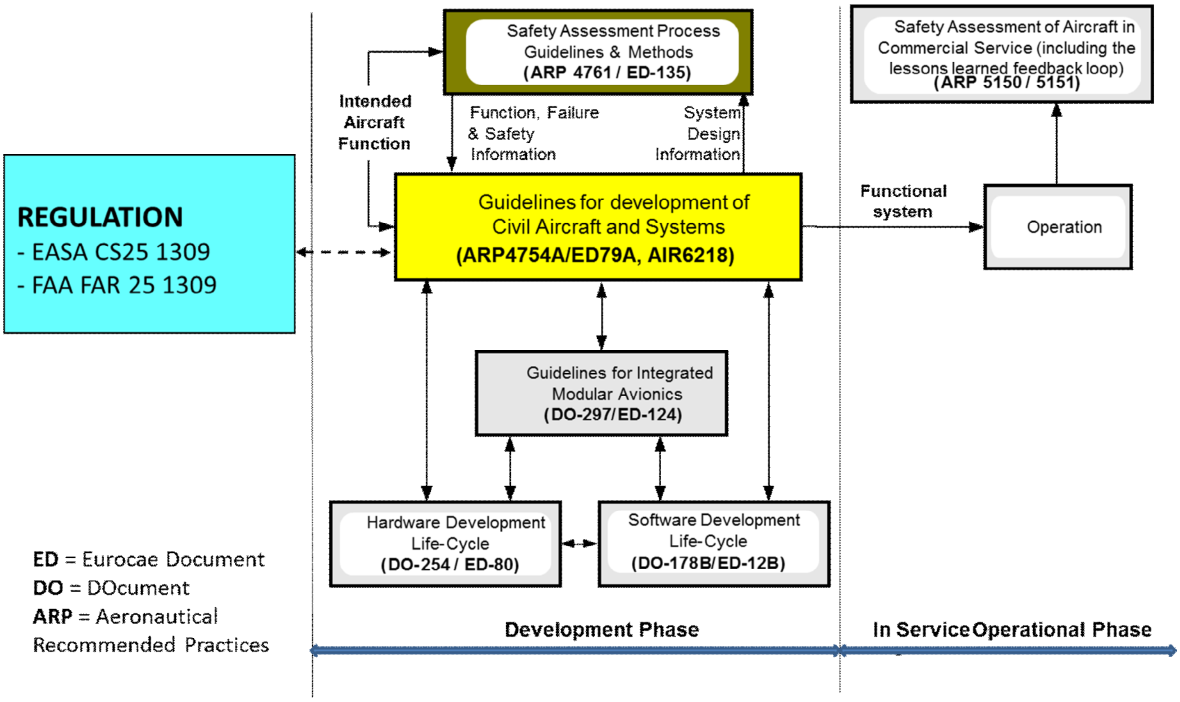

REGULATION
- EASA CS25 1309
- FAA FAR 25 1309
Safety Assessment Process Guidelines & Methods (ARP 4761 / ED-135)
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
Guidelines for development of Civil Aircraft and Systems (ARP4754A/ED79A, AIR6218)
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
Hardware Development Life-Cycle (DO-254 / ED-80)
Software Development Life-Cycle (DO-178B/ED-12B)
Safety Assessment of Aircraft in Commercial Service (including the lessons learned feedback loop) (ARP 5150 / 5151)
Functional system
Operation
ED = Eurocae Document
DO = DOcument
ARP = Aeronautical Recommended Practices
Development Phase
In Service Operational Phase

Figure 14- Safety Standard (guidelines) organization for aircraft product in development and in operation

This model of standard organization completed for consideration of procedures and services development and slightly simplified may become an ASCOS recommendation for a common harmonized model of standard organization at the level of each TAS stakeholder:

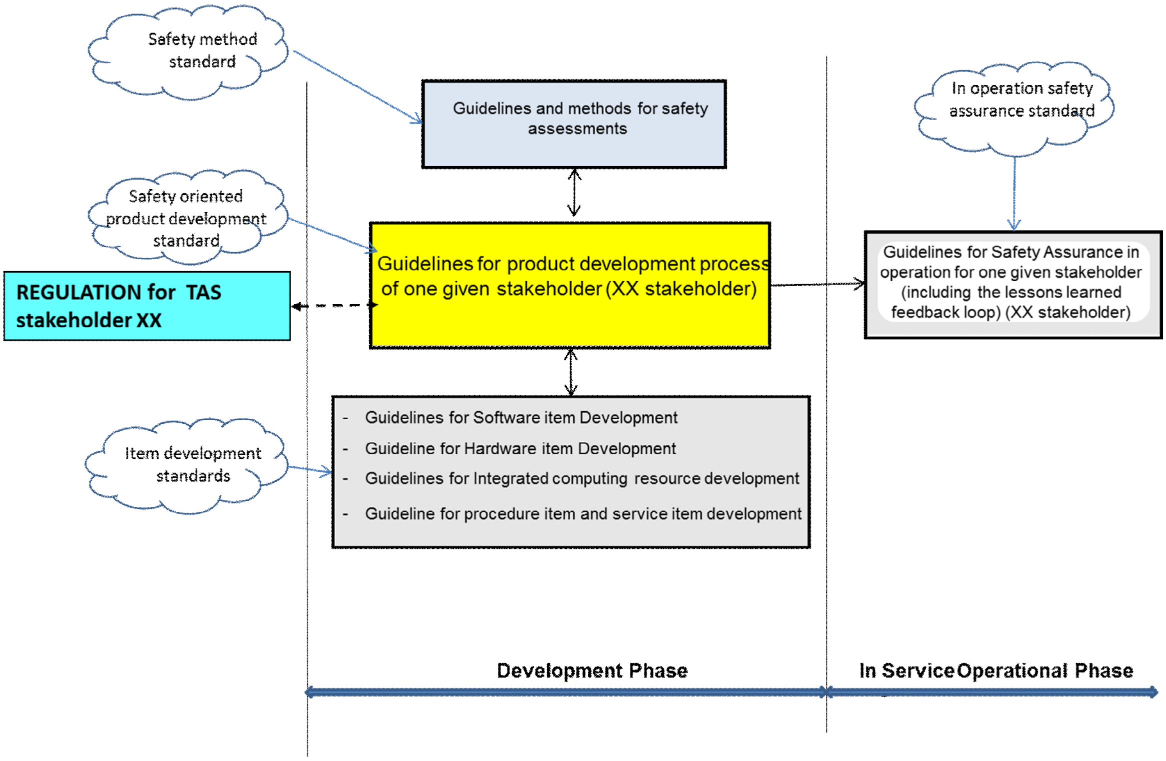

Safety method standard
Guidelines and methods for safety assessments
In operation safety assurance standard
Safety oriented product development standard
REGULATION for TAS stakeholder XX
Guidelines for product development process of one given stakeholder (XX stakeholder)
Guidelines for Safety Assurance in operation for one given stakeholder (including the lessons learned feedback loop) (XX stakeholder)
Item development standards
- Guidelines for Software item Development
- Guideline for Hardware item Development
- Guidelines for Integrated computing resource development
- Guideline for procedure item and service item development
Development Phase
In Service Operational Phase

Figure 15- ASCOS proposed model of standard organization for product development and product safety assurance in operation

Using this model the aircraft stakeholder development standards are pluged as follows:

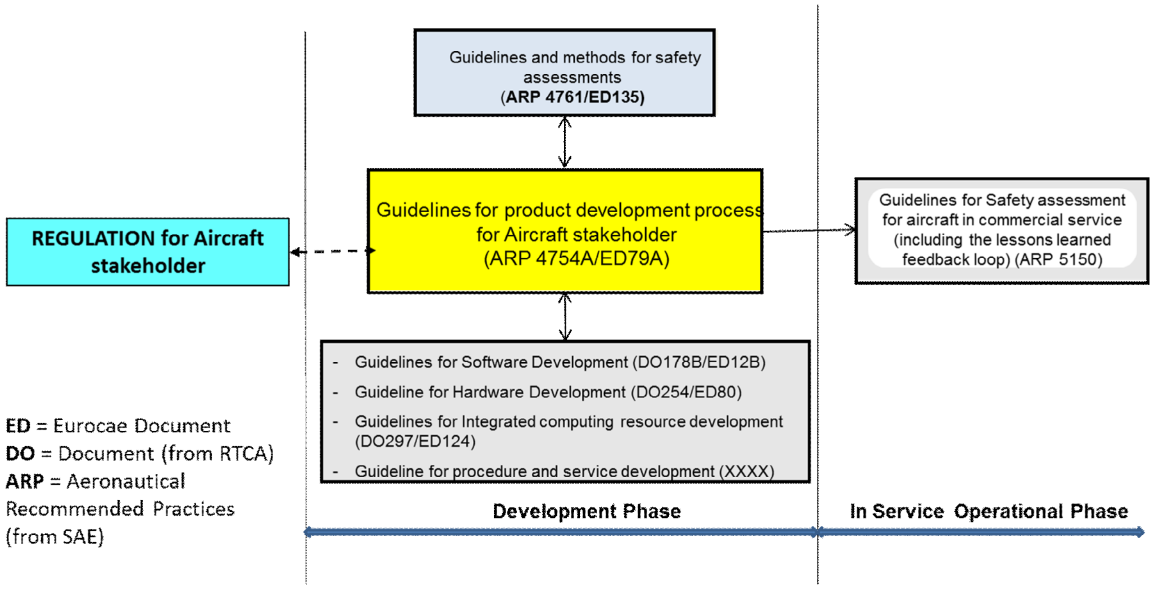

Guidelines and methods for safety assessments (ARP 4761/ED135)
REGULATION for Aircraft stakeholder
Guidelines for product development process for Aircraft stakeholder (ARP 4754A/ED79A)
Guidelines for Safety assessment for aircraft in commercial service (including the lessons learned feedback loop) (ARP 5150)
- Guidelines for Software Development (DO178B/ED12B)
- Guideline for Hardware Development (DO254/ED80)
- Guidelines for Integrated computing resource development (DO297/ED124)
- Guideline for procedure and service development (XXXX)
ED = Eurocae Document
DO = Document (from RTCA)
ARP = Aeronautical Recommended Practices (from SAE)
Development Phase
In Service Operational Phase

Figure 16- ASCOS proposed Safety Standard organization for aircraft product in development and in operation

The same model can be used to structure ATM guidelines used for ATM product development. It applies for any ATM product including procedures and services.

How the ATM standards could be inserted into ASCOS development standard model [derived from SAM (Eurocontrol Safety Assessment Methodology V2.1/ SRM (SESAR Safety Reference Material)/ ED78A]

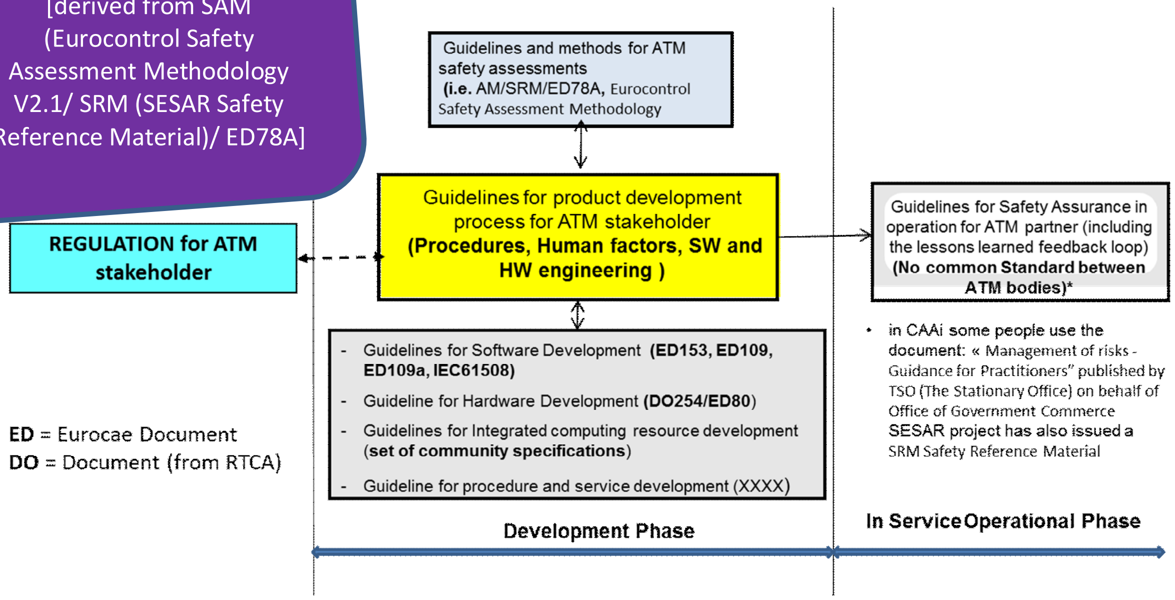

Guidelines and methods for ATM safety assessments (i.e. AM/SRM/ED78A, Eurocontrol Safety Assessment Methodology
REGULATION for ATM stakeholder
Guidelines for product development process for ATM stakeholder (Procedures, Human factors, SW and HW engineering)
Guidelines for Safety Assurance in operation for ATM partner (including the lessons learned feedback loop) (No common Standard between ATM bodies)*
- Guidelines for Software Development (ED153, ED109, ED109a, IEC61508)
- Guideline for Hardware Development (DO254/ED80)
- Guidelines for Integrated computing resource development (set of community specifications)
- Guideline for procedure and service development (XXXX)
• in CAAi some people use the document: « Management of risks - Guidance for Practitioners" published by TSO (The Stationary Office) on behalf of Office of Government Commerce SESAR project has also issued a SRM Safety Reference Material
ED = Eurocae Document
DO = Document (from RTCA)
Development Phase
In Service Operational Phase

Figure 17- ASCOS proposed Safety Standard organization for ATM product in development and in operation

In the same way the ASCOS standard organization apply to Airlines and airports where the “products” of their development processes are mainly procedures and services.

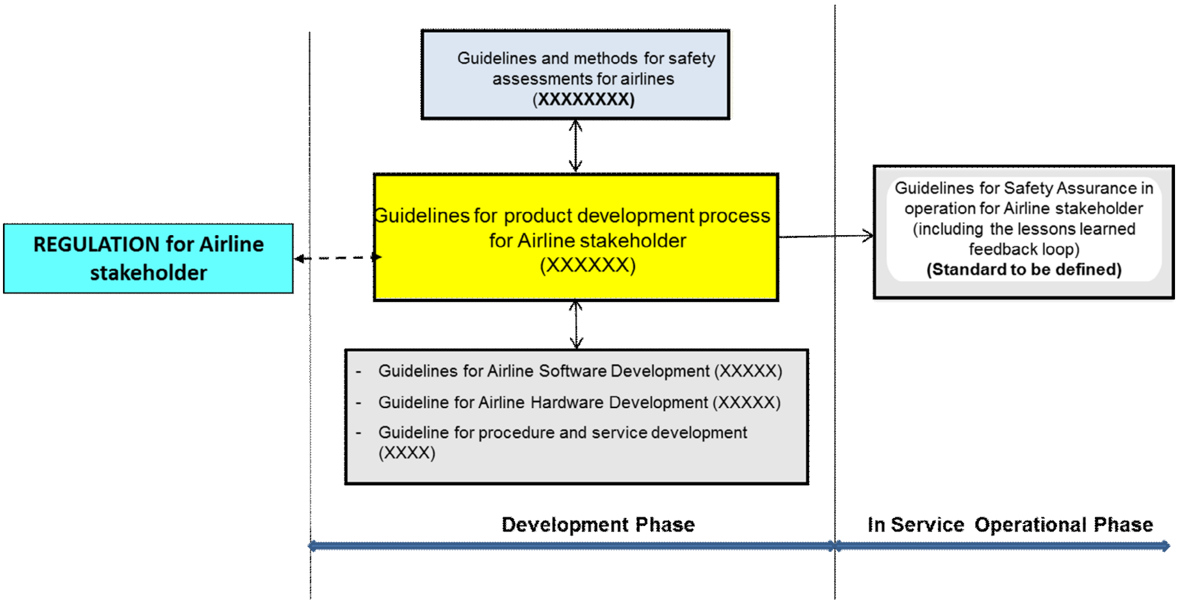

Guidelines and methods for safety assessments for airlines (XXXXXXXX)
REGULATION for Airline stakeholder
Guidelines for product development process for Airline stakeholder (XXXXXX)
Guidelines for Safety Assurance in operation for Airline stakeholder (including the lessons learned feedback loop) (Standard to be defined)
- Guidelines for Airline Software Development (XXXXX)
- Guideline for Airline Hardware Development (XXXXX)
- Guideline for procedure and service development (XXXX)
Development Phase
In Service Operational Phase

Figure 18- ASCOS proposed Safety Standard organization for Airline product in development and in operation

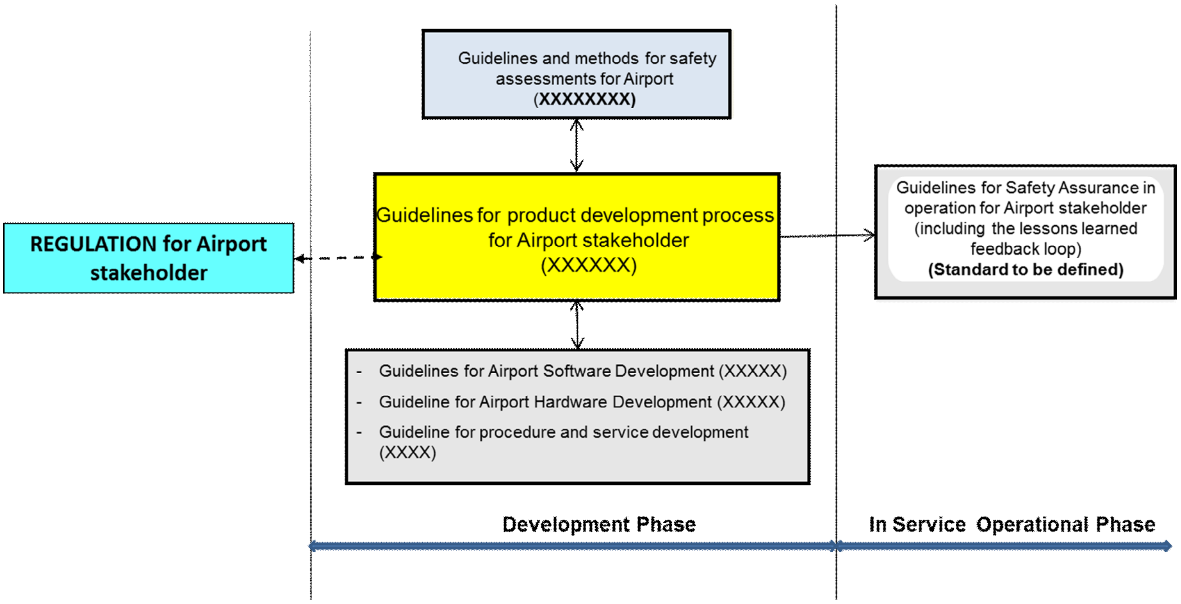

Guidelines and methods for safety assessments for Airport (XXXXXXXX)
REGULATION for Airport stakeholder
Guidelines for product development process for Airport stakeholder (XXXXXX)
Guidelines for Safety Assurance in operation for Airport stakeholder (including the lessons learned feedback loop) (Standard to be defined)
- Guidelines for Airport Software Development (XXXXX)
- Guideline for Airport Hardware Development (XXXXX)
- Guideline for procedure and service development (XXXX)
Development Phase
In Service Operational Phase

Figure 19- ASCOS proposed Safety Standard organization for Airport product in development and in operation

ASCOS recommends that a rationalization activity should be performed by the different stakeholders of the total aviation system to harmonize the standards to apply for product development process, safety assessment/analysis methods, software/hardware/procedure/services development and safety assurance in operation. An inter-stakeholder activity should be performed to assure the complete coverage and coherency of the standards between the stakeholders.

The standards organization should remain as described in figure 15 with the development at the level of each stakeholder of coherent document:

- One coherent standard for safety oriented product development process,

- One coherent standard for safety assessment methods,
- One coherent standard for safety assurance in operation including lessons learned feedback,
- Coherent standards for item development (e.g. software items, hardware items, integrated computing resources, procedures, services,)

4.4.2 Recommended common scheme for standards organization at total aviation system level (multi-stakeholder level)

Even If the development and in operation standard is structured in the same way at each stakeholder level, it is necessary to develop standards at Total Aviation System level (inter-stakeholder level) to define the safety oriented tasks to perform at this level. The actual standard that describes some TAS tasks at inter-stakeholder level is the ED78A recommended practice. This standard may need to be revisited to give more details on the inter-stakeholder activities (especially for requirement validation process, requirement transmission to stakeholders, DAL assignment process and safety assurance in operation). It is necessary also to update the interface with the standards used at each stake holder level. As an example, the ED78A used for TAS level data link activities and the ARP4754A used for aircraft stakeholder activities should be revisited in order to make them consistent in term of requirement capture (exchange), requirement validation, DAL assignment and consideration of aircraft failure/errors repercussions on ATM operation.

A EUROCAE working group (WG 91) has already issued proposal for ED78A revision (EDXX: Recommendations for Revision of ED-78A Volume 1 – Report). The scope of ED78A should be extended to make it applicable to other development activities than data link.

The ASCOS proposal for standard organization at TAS level is illustrated in the following figure.

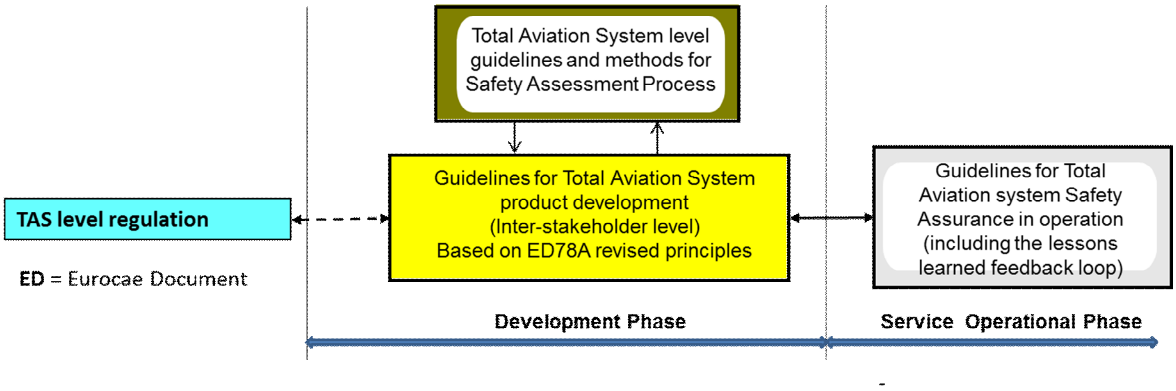
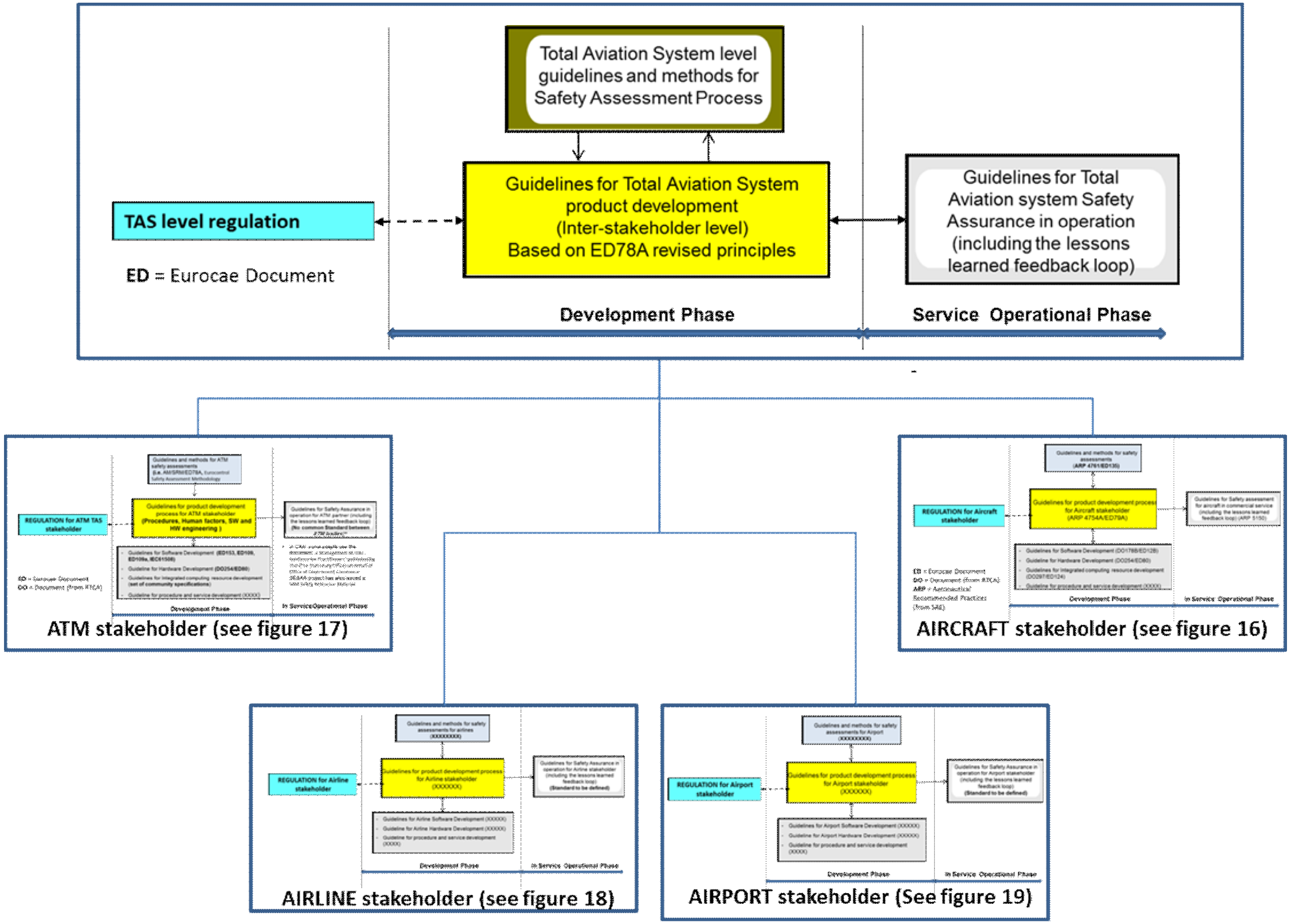

Total Aviation System level guidelines and methods for Safety Assessment Process
TAS level regulation
Guidelines for Total Aviation System product development (Inter-stakeholder level) Based on ED78A revised principles
Guidelines for Total Aviation system Safety Assurance in operation (including the lessons learned feedback loop)
ED = Eurocae Document
Development Phase
Service Operational Phase

Figure 20- Standard document organization at TAS (inter-stakeholder) level

The overall standards organization at TAS inter-stakeholder level and at TAS stakeholder level is then represented in the following figure:


Total Aviation System level guidelines and methods for Safety Assessment Process
TAS level regulation
ED = Eurocae Document
Guidelines for Total Aviation System product development (Inter-stakeholder level) Based on ED78A revised principles
Guidelines for Total Aviation system Safety Assurance in operation (including the lessons learned feedback loop)
Development Phase
Service Operational Phase
REGULATION for ATM TAS stakeholder
Guidelines and methods for ATM safety assessments (i.e. AMSRM/ED78A, Eurocontrol Safety Assessment Methodology
Guidelines for product development process for ATM stakeholder (Procedures, Human factors, SW and HW engineering)
Guidelines for Safety Assurance in operation for ATM partner (including the lessons learned feedback loop) (No common Standard between ATM leaders)
Guidelines for Software Development (ED153, ED109, ED109a, IEC61508)
Guideline for Hardware Development (DO254/ED80)
Guidelines for integrated computing resource development (set of community specifications)
Guideline for procedure and service development (XXXX)
Development Phase
In Service Operational Phase
ATM stakeholder (see figure 17)
REGULATION for Aircraft stakeholder
Guidelines and methods for safety assessments (ARP 4761/ED135)
Guidelines for product development process for Aircraft stakeholder (ARP 4754A/ED79A)
Guidelines for Safety assessment for aircraft in commercial service (including the lessons learned feedback loop) (ARP 5150)
Guidelines for Software Development (DO178B/ED12B)
Guideline for Hardware Development (DO254/ED80)
Guidelines for integrated computing resource development (DO297/ED124)
Guideline for procedure and service development (XXXX)
Development Phase
In Service Operational Phase
AIRCRAFT stakeholder (see figure 16)
REGULATION for Airline stakeholder
Guidelines and methods for safety assessments for airlines (XXXXXXX)
Guidelines for product development process for Airline stakeholder (XXXXXX)
Guidelines for Safety Assurance in operation for Airline stakeholder (including the lessons learned feedback loop) (Standard to be defined)
Guidelines for Airline Software Development (XXXXX)
Guideline for Airline Hardware Development (XXXXX)
Guideline for procedure and service development (XXXX)
Development Phase
In Service Operational Phase
AIRLINE stakeholder (see figure 18)
REGULATION for Airport stakeholder
Guidelines and methods for safety assessments for Airport (XXXXXXX)
Guidelines for product development process for Airport stakeholder (XXXXXX)
Guidelines for Safety Assurance in operation for Airport stakeholder (including the lessons learned feedback loop) (Standard to be defined)
Guidelines for Airport Software Development (XXXXX)
Guideline for Airport Hardware Development (XXXXX)
Guideline for procedure and service development (XXXX)
Development Phase
In Service Operational Phase
AIRPORT stakeholder (See figure 19)

Figre 21- Overall product development and in operation safety assurance standard document organizations for TAS (inter-stakeholder and stakeholder)

4.4.3 Details on the content of development process standard

Let’s come back to the ASCOS standard organization at the level of each stakeholder and at TAS level illustrated in figure 15 and 20. In this organization, the core document that structures the development process is the “Guideline for product development process”. It should be recalled that, In accordance with the ASCOS model for product development detailed in chapter 3.3 and in figure 13, the “guideline for product development process” should describe the project development planning activities and the tasks to perform during the product development process of one given stakeholder. In addition to the planning activities, the 8 following generic integral processes should at least be addressed:

1. Safety Assessment process to show compliance with safety objectives
2. Development Assurance Level (DAL) assignment process to mitigate development errors (extended to errors in the application of normal or emergency operational procedure)
3. Requirement Capture process to assure that all requirement sources are collected
4. Requirement Validation process to assure that requirement list is complete and that each requirement is correct
5. Requirement Implementation process to assure that validated requirement are applied
6. Configuration management process to control the configurations of the systems
7. Process Assurance to assure that the development process follows the principles described in the development document
8. Certification and regulatory authority coordination to standardize the interface with the certification authorities

Each integral process should be structured with a plan, method documents, and technical deliverables.
It is beneficial if each stakeholder develops plans with the same generic structure to avoid overlooking safety related tasks (e.g. safety plan generic structure)

For each type of plan (e.g. safety plan) the details of the implementation of the related activity (e.g. Safety organization, safety tasks and safety management) may be specific to each stakeholder depending on its company organization and product specificities.

The application of the same development standards organization at each level of the total aviation system will lead to the issuing of the same type of applicable documents for product development. These applicable documents are summarized here after:

Product development applicable document	Document family
Safety plan, Validation plan, Verification plan Process assurance plan Safety assurance in operation plan	Process
Safety Master Document	Design
Lessons learned Requirements document for design	Design
Safety validation question list	Design
Safety review question lists	Design
SOI Review question lists	Design
Safety methods for FHA, PASA, PSSA, SSA, ASA, CMA, HEA, PRA, ZSA, IHA, OSA, OPA, IA, Safety Synthesis, safety review organization, Safety assurance in operation, Fault Trees, Event Sequence Diagrams, etc.	Method
Integrated system specific studies (margin and sensitivity studies)	Method
Lessons learned method document	method

Table 1 Product development applicable document

These documents, that are low level applicable standards for product development, will be the primary targets of a “continuous standard improvement” loop based on lessons learned from in operation results.

The improved low level standards will be, if necessary, the starting point for improvement of higher level standards such as recommended practices from SAE or EUROCAE, regulation acceptable means of compliance, regulation items.

4.4.4 Details on the Safety management tasks described in Safety plans

There should be several safety plans in the total aviation system, one at the level of the total aviation system and one at the level of each stakeholder for each development project, etc.

In the total aviation system safety plan it should be considered and described the safety management organization that will coordinate and harmonize the safety activities at the level of the total aviation system and at the level of the interface between stakeholders. This organization will also be in charge of assuring that safety knowledge and safety culture are implemented in each stakeholder organization.

At the level of each stakeholder the safety plan should describe the safety management implemented by the considered stakeholder. It should be recommended that an “Engineering and Safety Group” (ESG) is created to assure coordination of all the tasks described in the plan and assure safety plan application. The stakeholder organization will be in charge of preparing and providing educational courses to enforce the adequate level of safety knowledge and safety management to perform the safety activities described in the safety plan (more details on the Safety management organization are in chapter 7).

4.4.5 Details on the Safety assessment methodology

To perform the safety assessment and safety analysis tasks described in a Safety plan it is necessary to develop recommended methods that should be applied by all the participants. Such a document can be extrapolated from the SAE ARP 4761 (aircraft) and from ED78A (ATM) documents used for safety assessment of aircraft systems and ATM data link systems.

4.4.6 Details on the Validation/Verification plan

For the Validation/Verification plan, after a description of the validation/verification organization and of the Validation/Verification process principles, the plan should particularly identify the tasks associated with the consideration of lessons learned from and in operation experience and the consideration of novelties (technological, organizational, regulation, operational, etc.) and Area of Change.

4.4.7 Details on the requirement capture and requirement Validation/Verification methods

The Validation/Verification method document should particularly describe:

- The methods for safety related requirement capture,
- The methods for validation of safety requirements and associated assumption (completeness and correctness)
- The method for consideration of lessons learned from events in operation in the validation/verification process.
- The novelties (technological, organizational, regulation, operational, etc.) consideration in the Validation/Verification process
- The method to organize safety reviews using “review question lists” covering both technical and quality aspects and adapted to each different type of review (development review or review required by the authorities i.e. SOI review for software and hardware development.
- The review transition criterion

4.4.8 Details on the Development Assurance Level assignment process

In a system, a malfunction of a function is due either to:

- Component failure(s) (hardware random failures: the random failures are subject of qualitative analysis (no single failure) and probabilistic analysis to show their acceptability);
- Error(s) in the development process (error in requirement capture, requirement validation and requirement verification of application); or
- Error(s) in the application of an operational procedure..

The Errors in the application of an operational procedure are mitigated by the quality level in the human factor studies associated to procedure and in the evaluation and testing of the procedure application.

The errors in the development process (errors on requirement completeness and correctness) are mitigated by the quality level of validation and verification activities that are requested in the development process for each function. This level depends on the severity of the safety repercussion in case of error and on the independencies introduced in function architectures. It is measured by the "Development Assurance Level (DAL) associated to each function.

The DAL (Development assurance Level) and the associated assignment process is a key point to mitigate errors that can be made on requirements during the system development process. It is recommended that each stakeholder of the total aviation system uses a "Development Assurance Level" like concept with an assignment process similar to the one described in the ED79A/ARP 4754A.

It is recommended that the DAL concept is extended to operational procedures (e.g. ATM procedures, cockpit crew procedures). If so, the level of Validation/verification/training activities associated to an Operational procedure will be in relation with the associated DAL.

A consistent DAL assignment process using ED 79A/ARP 4754A principles and applicable at total aviation system level and at each stakeholder level should be described in future issue of ED 78A.

4.4.9 Details on Safety Master Document - providing homogeneity in safety assessments and flexibility in regulation application

To perform, at stakeholder level, an efficient safety activities and assure that each sub-stakeholder participant will use the same methods and data in the same way, it is often useful to precise how to apply the regulation and always necessary to define common data that will be used by each of the stakeholder involved in the safety activities. For that it should be developed an applicable document often called "Safety Master Document" which should be written by the applicant at the beginning of any development project and discussed with the authorities for acceptation.

In complex system development, this document is a key point to assure common understanding between safety analysts and homogeneity between the different types of safety assessments performed during product development.

This document is a means to assure flexibility in regulation application by allowing the applicant to describe, if necessary, new means of compliance to regulation and propose them to the authorities for acceptation.

5 Safety standards continuous improvement using feedback from safety events in development and in operation

The aim of this section is to propose a process for elaborating lessons learned from development and in operation events for reuse in the development process of new or modified products. After a recall on the safety assurance process in operation (Section 5.1), this section highlights the following:

- Identification of events to monitor for safety assurance in operation: (notion of safety barriers, CATS risk picture, precursors (see section 5.2 of this document)
- Feedback loop for safety standards improvement (see section 5.3 of this document)
- Future Risk consideration (linked with area of change and with future novelties implementation) (see section 5.4 of this document)
- Principles for an in operation automatic identification of precursors (see section 5.5 of this document)

5.1 General principles and recall on the Safety assurance process in operation

The initial list of events to monitor during operation should be made during the safety assessment process performed during the product development phases and during the elaboration of the safety risk picture (CATS ESD). Safety risks picture made for AoCs (Area of Changes) should also be considered as they permit orienting the search for precursors associated with the considered AoCs. These events are called safety precursors and allow to establish the initial list of parameters to monitor during the "Safety Assurance" process in operation as defined in figure 10 of Chapter 4.2 of this document and as recalled in the figure below.

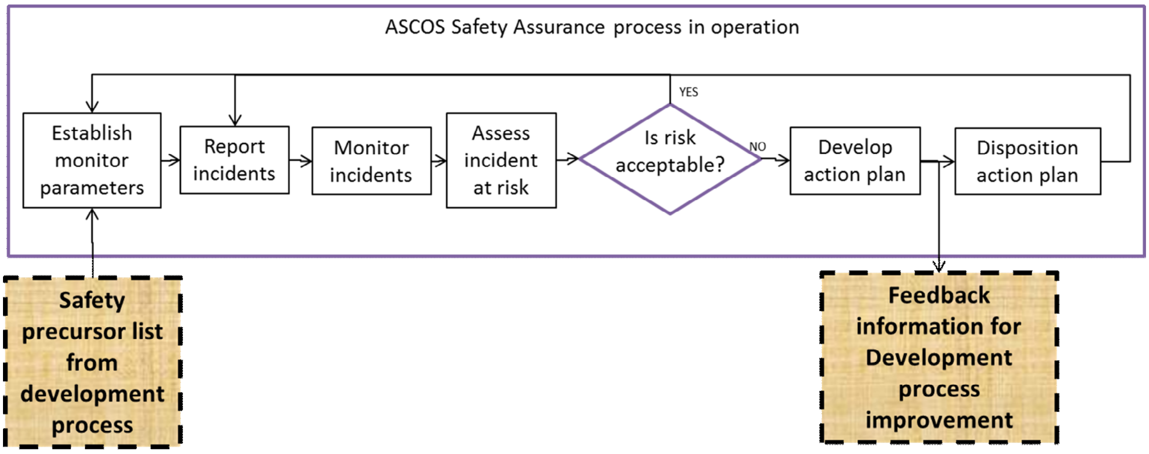

ASCOS Safety Assurance process in operation
Establish monitor parameters
Report incidents
Monitor incidents
Assess incident at risk
Is risk acceptable?
YES
NO
Develop action plan
Disposition action plan
Safety precursor list from development process
Feedback information for Development process improvement

Figure 22 - ASCOS proposed Safety Assurance process in operation and link with development process

5.2 Identification of events to monitor for safety assurance in operation

5.2.1 Safety barriers and precursors

5.2.1.1 General concept

During development and in service phases, a product is facing many abnormal situations due to failures, mishandling, development errors, procedure application errors, maintenance errors, environmental conditions, etc. These situations may be part of a chain of events that can lead to an end event with Hazardous or Catastrophic repercussions.

When an event occurs, the analyses of the event conditions often show that several abnormal situations have occurred before. If these abnormal situations had been identified as precursor and mitigated, the event will have been prevented.

During the development phases of a product, Hazardous and Catastrophic situations are anticipated in safety assessments and mitigations means are implemented in the design: redundancies, back up, monitoring and associated procedure, product lay out (e.g. installation separation), operational procedures, maintenance procedures, etc.

These mitigation means are safety barriers to protect against Hazardous or Catastrophic situations.
These safety barriers may fail leaving the product without protections if the malfunction is not identified and if measures are not taken to restore the situation. These malfunctions of safety barriers are precursors of situations that may lead to Hazardous or Catastrophic repercussions. It is then necessary during development phase to identify safety barriers, associated precursors (malfunctions of safety barriers) and during product operation phases to implement a monitoring for tracking precursors and react as necessary to:

- Keep the mitigation means efficient and keep the final risk at the safety level accepted at the time of certification.
- Learn from precursor root causes and derive lessons to improve product development standards and/or operational standards

5.2.1.2 Recall on Risk and Precursor definition

Here after are reminded the definitions associated with Risk and precursors (ASCOS D3.2).

5.2.1.2.1Risk definition

A risk is characterized by its severity and likelihood.
A “**current/known risk**” is defined by its severity and the current/known likelihood of its components (failures, errors represented by fault trees).
An “**emerging risk**” is defined by

a) The same consequences and Severity as a current/known risk but with a different Likelihood of its components taking into account the influence of new/emerging technologies behavior, work organizations, regulations, operational procedures, change in failure rate, etc.,

b) A new Severity with the same Likelihood of its components,

c) A new Severity with a new Likelihood of its components.

A “**future risk**” is defined as a risk associated with the future introduction of a novelty (e.g. new design, new procedure, and new organization).

5.2.1.2.2Precursor Definition

A precursor is defined as an “identifiable event that may be used as early warning for known or potential hazards”. Such early warnings may be:

- Events identified and currently monitored, for which the potential to degenerate in hazard is known to be significant
- Events known yet, but for which risk to degenerate in hazard may have been underestimated, neglected or even unidentified up till now, unless revealed by an actual occurrence of the hazard

A systematic precursor capture process is an efficient means for enhancing and maintaining risk awareness and for proactive identification of safety actions.

5.2.1.3 Safety barrier and associated precursors

5.2.1.3.1Definition of Safety barriers

Referring to the concept spread out by J. Reason, the notion of Safety Barrier could be seen as the “Swiss cheese slice” he has introduced in his illustrative model. Indeed, these slices are an image of the Safety Barriers in the risk model. However, the analogy with slices of cheese has some limits and does not suffice to define the concept of Safety Barrier, as they shall have key characteristics that cannot be inferred from it.

> A Safety Barrier is a means or feature which efficiently mitigates, prevents or protects a malfunction or combination of malfunctions from worsening into a more serious mishap.
>
> Note1: A key aspect of a Safety Barrier is that it is specific in avoiding a particular malfunction or combination thereof to develop in a more serious mishap. The validity of a Safety Barrier is specific of a particular “malfunction path”. There is no such notion of universal Safety Barrier preexisting to any hazard.
>
> Note2: A second point of a Safety Barrier is that it shall be an efficient mitigation means. The accumulation of mitigation means of little or uncertain efficiency and independence does not constitute a Safety Barrier.

Categories of Safety Barrier can be of a wide range of type and nature, including procedures, redundancies, backups, independence, design process rules, dissimilarities, segregation, airmanship skills, etc.

Some overlap could be claimed between the definitions of 'Safety Barrier' and 'Safety Requirement'[4]. The latter introduces the idea that the risk-mitigation means is compulsory in order for the risk to be acceptable. In such context, a Safety Requirement would therefore induce the implementation of Safety Barrier(s) that has been invoked by a risk-mitigation strategy.

There is a safety risk when a safety barrier fails. The way the safety barrier can fail can be illustrated by fault trees.

Within the ASCOS project, focus will be given on identification of events that could make fail the safety barriers introduced in the design and through procedures and operation and that could be identified and traced as precursors, (i.e. identifiable events that may be used as early warnings for known potential hazards).

5.2.1.3.2Identification of safety barriers and precursors in product design

The development of the system architecture is supported by the process of hazards identification and risks assessment and mitigation. Identification of mitigation means and determination of the Safety Barriers is a core element of this process of mitigating risks. The Safety Barriers retained at the end of the process of hazards identification, risks assessment and mitigation should be finally described as completely as possible over the total aviation system, together with the way they should combine in order to mitigate the risk.

Description of Safety Barriers would be naturally developed in parallel with the description of the scenarios of hazards. For the sake of completeness, a scenario description should be refined until all the underlying assumptions have been exposed. Finally, a careful screening on all these assumptions should give way to the determination of the means or features which would efficiently mitigate prevent or protect the malfunction or combination of malfunctions from resulting in the hazard, i.e. to the determination of the Safety Barriers related to the malfunction scenario.

In accident scenarios inefficiency or malfunctions of Safety barriers should also be considered. The unexpected malfunction or degradation of a Safety Barrier may result in an underestimated level of risk and jeopardize the risk mitigation strategy that has been deployed. So, it is important that the possible malfunctions of a Safety Barrier should also be considered during the design phase of a product and modeled (through fault trees and Event Sequence Diagrams, for example), in order for all the contributors to the malfunction to be readily identified.

Finally, the determination of Safety Barriers and the modeling of their related malfunctions will be a cornerstone in the process of determination of precursors to accidents/incidents described below.

The method for safety barriers and associated precursor identification is described in ASCOS D3.2.

[4] As reference, EC1035/2011 gives a definition of a Safety Requirement that is "a risk-mitigation means, defined from the risk-mitigation strategy that achieves a particular safety objective, including organizational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics".

5.2.1.3.3 Safety Barriers/precursors and stakeholder's safety responsibility

The Global Aviation System is composed of a community of stakeholders having different and complementary roles and responsibilities on the overall safety of the system. By the way, a number of accident reports reveal that they are often the result of the combined contributive malfunctions of different elements pertaining to these different actors of the Global Aviation System. That means that Safety Barriers are most of the time a combination of features or elements that are under the responsibility of these different stakeholders. As a consequence, the mitigation efficiency expected from a Safety Barrier would largely depend on the level of safety awareness and commitment of each and every stakeholder involved. However, the different stakeholders of the Global Aviation System may have different and fairly independent approaches to identify how their current or foreseen activities and processes contribute to the Safety Barriers. In other words, there is not much global approach to ensure overall consistency of Safety Barriers amongst stakeholders

5.2.1.3.4Alerts associated with safety barriers precursors

When an event occurs revealing a failure or a flaw in a safety barrier, it would be useful and beneficial for safety to raise an alert. However the event should be recognized as such. It is therefore important that when Safety Barriers are identified, the identifiable events that may reveal malfunctions -i.e. precursors- are identified, monitored and reported as means of alerting of potential failure or flaw in the Safety Barrier.

Finally, the determination of Safety Barriers, the modeling of their related malfunctions, the identification of the related assumptions and the determination of precursors to be monitored will be a cornerstone in the improvement of the safety risks perceived and shared by all the actors of the aviation system.

5.2.1.4 Safety barriers and precursor representation in global aviation risk pictures

During product development, many safety barriers are implemented in each activity of the main participants of the total aviation system (Aircraft, Airlines, ATM, and Airport).

The identification of the safety barriers will be made first considering each part independently, second by considering the different parts integrated. The safety barriers and the barrier malfunctions (precursors) will be identified and visualized when constructing the Safety risk models (see ASCOS D3.2).

In ASCOS, risks are modeled through Events Sequence Diagrams (ESD) developed using "Causal Model for Air Transport Safety" (CATS) tool for the main risk domains identified in the European Aviation Safety Plan (EASP). In these models, safety barriers as well as precursors that can make fail the safety barriers are incorporated.

The ESD Safety risk model should be representative of the real in service environment. There should be models for the cases where all the different resources of the total aviation system are considered available and models considering that some resources are missing when the system is authorized to work without these resources before reparation (MMEL concept for aircraft).

The assessment of emerging/future risks will be made by updating the ESD with data coming from the events in operation. The result of these assessments may lead to implement mitigation actions if the safety objectives are not met.

5.2.1.5 Safety barrier and precursor prioritization

Some safety barriers and associated precursors are more important than others and their monitoring should be the subject of particular attentions. A Precursor Criticality Level (PCL) can be associated to each precursor depending on the criticality of the situation when the precursor occurs and depending on the number of safety barrier remaining to protect against the feared event.

As example: if the feared event is Catastrophic and if it is mitigated by one safety barrier a PCL1 should be assigned to this safety barrier and to the precursors that can make fail this safety barrier. If the end situation is mitigated by two independent safety barriers, a PCL2 is assigned to each of the safety barrier and to the precursors that can make fail each of these safety barriers

If the feared event is Hazardous and if it is mitigated by one safety barrier a PCL2 should be assigned to this safety barrier and to the precursors that can make fail this safety barrier. If the end situation is mitigated by two independent safety barriers, a PCL3 is assigned to each of the safety barrier and to the precursors that can make fail each of these safety barriers

The following table summarizes the Precursor Criticality Level (PCL) assignment process

Number of independent safety barriers Feared event classification	1	2	3	4 or more
CAT	PCL1	PCL2	PCL3	PCL4
HAZ	PCL2	PCL3	PCL4	PCL4
MAJ	PCL3	PCL4	PCL4	PCL4
MIN	PCL4	PCL4	PCL4	PCL4
NSE	PCL4	PCL4	PCL4	PCL4

Table 2Precursor Criticality Level (PCL) assignment process

The PCL indicator can be used to prioritize the actions to take when precursors occur.

The safety barriers, the associated precursors and their assigned criticality level identified during the development process are transmitted to the safety assurance in operation responsible and to the risk picture responsible for incorporation in CATS diagrams. This will be made using:

- The results of the safety assessment process performed during product development by each stakeholder of the total aviation system. A particular activity may be added in safety assessments process for preparing the list of the significant safety barrier and associated precursor to consider in the CATS diagrams of the total aviation system. Traceability between safety assessments results and CATS diagrams should be kept.

- Operational documentation where are described operational procedures that are often acting as safety barriers. Traceability between operational procedures considered as significant safety barriers and CATS diagrams should be kept.

5.2.2 Collection of precursors associated with emerging risk and associated analysis

The identification at each stakeholder level and at total aviation system level of the safety barriers, the associated precursors to monitor and the PCL allows defining the means to use for collecting these precursors.

Developing a specific taxonomy for precursor event will help extracting these events from development tests result data bases or from in operation event data bases.

When precursors are detected and root cause identified, safety assessments and CATS ESD risk picture should be checked to verify if safety objectives remain met. If not, mitigation means should be developed.

5.2.3 Precursor list updating with in operation events

The monitoring of precursors identified during development process may be, some time, not sufficient to prevent Hazardous or Catastrophic events to occur. When such Hazards occur they should be collected and analyzed for root cause and precursor identification. The impacted CATS diagrams and safety assessments should be reviewed accordingly. If it appears that some precursor events have been overlooked and are missing in the precursor original list, the list should be updated as well as safety assessments and CATS diagrams.

5.3 Feedback loop for safety standards improvement

5.3.1 Feedback process description

The aim of the lessons learned feedback process is to derive, from events in development and in operation, requests for improvements to include in the development process in order to avoid event reoccurrence on new developments. To be applied efficiently these requests for improvements should take the form of requirements (Lessons Learned Requirement: LLR) in order that the application and verification of application is made using the standard requirement management process implemented in the development process.

The process described here after use the results of the European Esprit project REAIMS (Requirement Engineering Adaptation and Improvement for Safety and dependability (1994- 1996)) and the information from the ARP 5150 (safety assessment of aircraft in commercial service, appendix O: lessons learned).

The process proposed for ASCOS is structured in accordance with the following steps:

1- The process starts with the identification, from development test results and from events occurring in operation, of safety significant events (precursors) candidate for further safety investigations.

2- When a safety issue is identified the process continue with investigation for root cause identification and elaboration of mitigation solution to solve the safety issue on products in development and operation

3- The identified root cause identified in step 2 is related to process development activity to generate a Lesson Learned Requirement (LLR) for improvement of development process standards

4- The LLR from step 3 are incorporated in development process standards including process and method documents but also in question lists to use for requirement validation, requirement verification and review activities

The two first steps can be identified as a current safety follow up activities performed by TAS stakeholders on product in operation. These two first steps basic process are illustrated in the following figure:

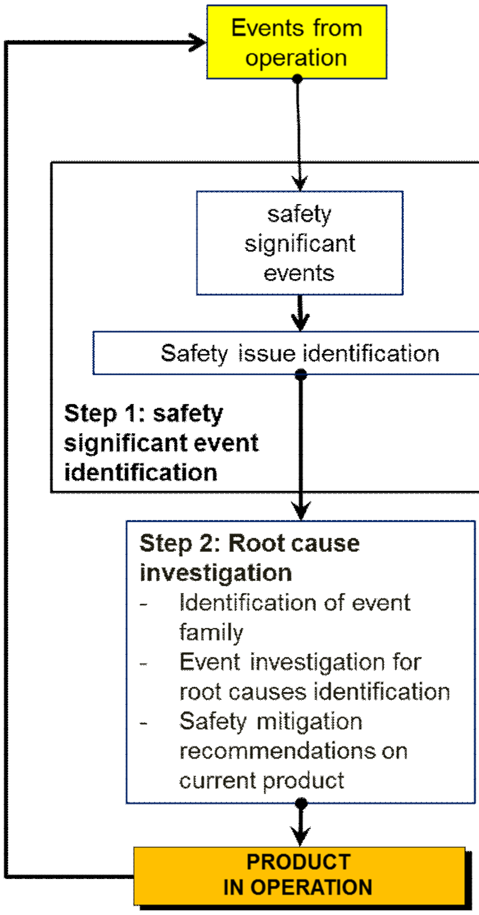

Events from operation
safety significant events
Safety issue identification
Step 1: safety significant event identification
Step 2: Root cause investigation
- Identification of event family
- Event investigation for root causes identification
- Safety mitigation recommendations on current product
PRODUCT IN OPERATION

Figure 23- TAS Basic Safety follow-up of product in operation

The identification during product development of safety barriers and associated precursors list to monitor during operation modify the above basic process as follows. The modifications are highlighted in deep blue boxes:

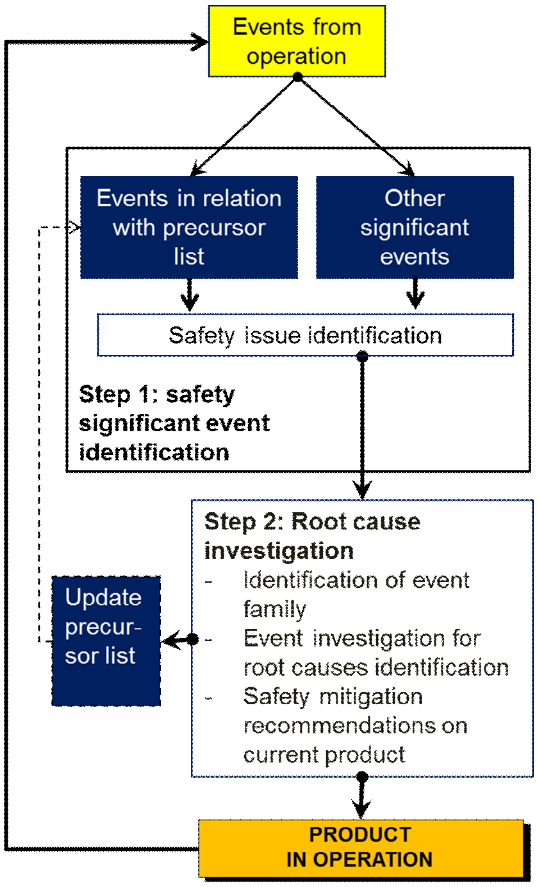

Events from operation
Events in relation with precursor list
Other significant events
Safety issue identification
Step 1: safety significant event identification
Step 2: Root cause investigation
- Identification of event family
- Event investigation for root causes identification
- Safety mitigation recommendations on current product
Update precur-sor list
PRODUCT IN OPERATION

Figure 24- Basic Safety follow up process improved by using a precursor list

Even with the improvements due to consideration of precursors, this loop addresses only product in development or in operation. To capitalize lessons learned and make them applicable via standards during product new development an additional “Lessons Learned” process should be implemented. This process aims at updating development standards, validation/verification question lists and reviews question lists that are used as applicable document during the development process. This process is illustrated in the following figure:

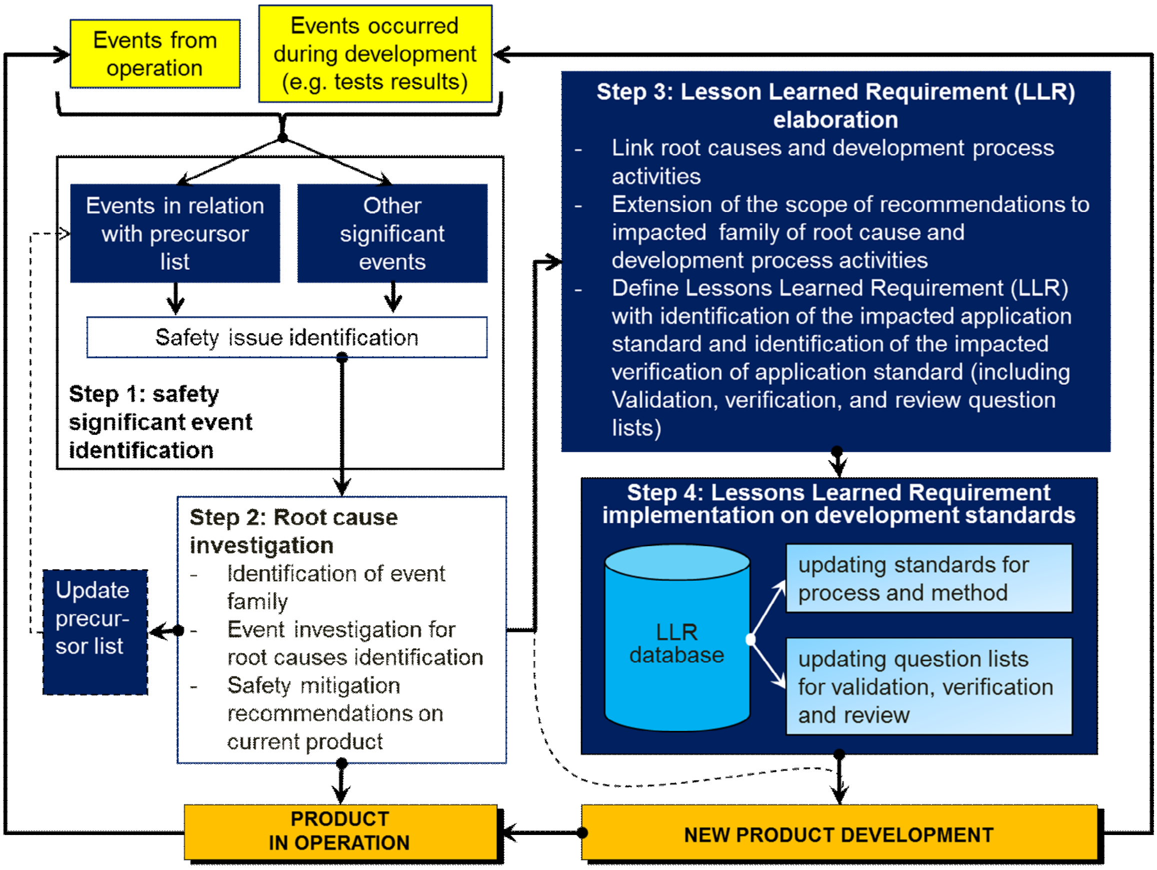

Events from operation
Events occurred during development (e.g. tests results)
Events in relation with precursor list
Other significant events
Safety issue identification
Step 1: safety significant event identification
Step 2: Root cause investigation
- Identification of event family
- Event investigation for root causes identification
- Safety mitigation recommendations on current product
Update precur-sor list
Step 3: Lesson Learned Requirement (LLR) elaboration
- Link root causes and development process activities
- Extension of the scope of recommendations to impacted family of root cause and development process activities
- Define Lessons Learned Requirement (LLR) with identification of the impacted application standard and identification of the impacted verification of application standard (including Validation, verification, and review question lists)
Step 4: Lessons Learned Requirement implementation on development standards
LLR database
updating standards for process and method
updating question lists for validation, verification and review
PRODUCT IN OPERATION
NEW PRODUCT DEVELOPMENT

Figure 25- Complete process for in operation product assurance and for Lessons Learned feedback loop on development standards.

5.3.2 Focus on Lessons learned Requirement Characteristics

Lessons Learned Requirements can be split in two families:

- Requirement that impact standards describing a process or a method.

  When the LLR have been incorporated in the impacted process document or the method document the LLR is automatically applied when the process or method standard is applied.

  The verification of the standard application will be made through the process assurance activities.

- Requirements that impact the product design characteristics.

  This kind of LLR should be the subject of a specific Lessons Learned Requirement list incorporated in the general safety requirement management process for application by the designers. The verification of application should be made during the reviews. For that these LLR should be incorporated in the question lists used to assure review completeness.

For each LLR it should be precised:

- A summary of the event/context of origin,
- An explication on the logic and reason of the LLR
- A description of the LLR

- The identification of the activity and the associated documentation that will assure the LLR application
- The identification of the activity and the associated documentation that will assure the LLR application verification
- A reference to the event(s) of origin to go back to the original event description in case of ambiguity in the LLR interpretation..

Before the LLR are recorded for application they should be the subject of a technical review for acceptation by the specialists of the concerned technical domain that will have to apply the LLR. They also may be reviewed by a manager group to judge acceptable the impacts on non-safety aspects (cost, industrial planning, etc.).

The details of all this Lessons Learned activity should be the subject of specific method document (standard for Lessons Learned elaboration and application).

5.3.3 Lessons learned exchange between TAS stakeholders

The lessons learned management process described in paragraph 5.3.1 should be implemented by each stakeholder of the total aviation system. If ASCOS development process framework developed in chapter 4 is applied by each stakeholders of the TAS, a recommendation to improve the development process of one stakeholder may be significant for the improvement of the others stakeholders development process. Such exchanges should be coordinated at TAS inter-stakeholder level to assure coherency between the stakeholders

5.4 Future risk considerations

In the design of a new product there are always two parts:

- A first part using standard technology/processes/methods where in operation experience exists
- A second part associated with implementation of novelties for which the experience is limited or no experience exists.

The first part takes benefits of the lessons learned loop described in Section 5.3. The second is associated with

- Implementation of novelties in the design (new technology, new architectures, etc.)
- Implementation of novelties in safety management (new organization, new methods, etc.)
- Consideration of new regulation, new operational procedures, new environmental conditions, new interface between TAS stakeholders, new human behaviors, etc.

Due to the lack of experience on these novelties, the only way to assure that enough attention is given to them during requirement capture, validation, verification and reviews is to identify till the beginning of a project development the list of these novelties and for each of them to record:

- The reason for the implementation of the novelty
- The frame of application (limits) and associated assumptions
- The safety impact (positive or negative)
- The anticipated mitigation means in case of adverse effect on safety (impact on safety barriers)

It is recommended that this list is built with the help of the Area of Change (AoC) list from the FAST processes. This list should be used systematically during design and during validation process and safety reviews to assure that no novelty has been overlooked, that all associated assumptions have been identified and validated and that all safety aspects have been considered and mitigated.

6 Principles for an in operation automatic capture of precursors

The aim of this section is to propose feasible process for an automatic capture of safety precursors during Total Aviation System operation in order to improve Safety assurance in operation and safety standards. This process is described in the following steps:

- Description of the existing recording process of system malfunctions in the maintenance computer of the aircraft.
- Definition of a generic taxonomy safety barriers failure oriented with identification of the related risk models and their identified safety barriers (using on board or ground facilities)
- Definition of methods to detect and capture automatically system malfunctions with the use of a taxonomy "safety barrier oriented" and record them in the maintenance computer.
- Extend the methodology to each player of the total aviation system (Airlines, ATM, Airports, Airworthiness and Crew licensing with taking into consideration its specification)

6.1 Event recording process description

It is necessary to note that, besides obvious safety related objectives, the main motivation for development of maintenance related tools is increase of transport efficiency by reducing flight delays, cancellations and time for unplanned maintenances by turning them into planned. It is realized by offering a complex solutions, containing not only autonomous aircraft system condition monitoring, root cause determination or fault isolation, but also through possibility of automatic sending the detected alerts and notifications directly to the operator's ground base in order to enable deploying of necessary resources (people, parts or equipment) before the aircraft arrive, without causing the schedule interruption. Additionally, data can be transmitted via manufacturer's support center (e.g. Boeing Operation Control Center or Airbus Real Time Health Monitoring (AiRTHM) 24/7 service) where they can be amended with airworthiness specialists' comments and tips.

Going into details the heart of the system is Central Maintenance Computer (CMC) or its equivalent unit such as Centralized Maintenance System (CMS), Airplane Condition Monitoring System (ACMS) or Central Maintenance Computing Function (CMCF) being a part of Airplane Health Monitoring (AHM) systems (Boeing) or AiRTHM (Airbus). It receives fault status indications from all aircraft systems, which are equipped with own independent fault detection and reporting modules called BIT or BITE depending on manufacturer. Next, by application of appropriate diagnostic model, received faults are consolidated and processed in order to determine the root cause, isolate and remove the risk of cascade effect. Finally, depending on the class of problem or assessed severity level, identified fault is correlated to flight deck effects such as flight crew alert, display of message on Multifunction Control Display Unit (MCDU) or sending to the ground station in order to support maintenance planning (by recommending repair actions for example). The CMC can also perform ground test of all connected systems. The entire fault history as well as maintenance data are kept for further analysis in form of fault reports. The place of data storing can be on on-board mass storage devices such as MAT hard drive, CIS servers or Quick Access Recorder (QAR). They also can be downlinked via ACARS or wireless local area network or sent by satellite service. Additionally airborne functions can be interacted with maintenance and ground components into CIS-MS providing health management related tasks as a part of CIS.

Besides, detecting faults after they have occurred, the contemporary maintenance and health monitoring systems such as AHM have ability to predict some problems in advance and identify precursors likely to progress into the Flight Deck Effect (FDE) faults. In the case of Honeywell system installed on Boeing B777 and B787, the system component realizing proactive approach is called Aircraft Condition Monitoring System (ACMS). Both in case of Airbus and Boeing aircraft the predictions is based on monitoring of pivotal flight parameters as flight speed, flight conditions, engine parameters, on-board equipment work parameters or other performance factors, interpreted as precursors for potentially dangerous failures or malfunctions. All these parameters as well as such as tire pressure, oxygen pressure, hydraulic fluid, APU or engine oil levels can be chosen as contained in customized set and continuously available for the operator via ACARS.

The real time data transfer between aircraft and ground realized by mentioned at the beginning the Boeing Operation Control Center or Airbus Real Time Health Monitoring (AiRTHM) 24/7 service are currently provided only to operators using the newest Boeing and Airbus products (B787, A380 and A350XWB). But due to significant potential for safety and operation efficiency improvement, it is highly probable that it will be extended with next new aircraft. This perspective, together with expected technological progress in real time aircraft health monitoring leads, to the conclusion that such solutions using tool for automatic precursors' detection and capture with use of ground facilities, should also be considered as very prospective.

Another instrument representing potential for automatic safety related data capture purposes is flight recorder. Currently available devices collect large amount of data concerning numerous flight parameters, which converted into a single stream of digital format are sent to the flight data recorder (FDR) and quick access or direct access recorder (QAR or DAR). Processed with commercially available software represents vast potential for various analyses. Many of aircraft is equipped with memory volume which does not entail the necessity of data transfer after every flight. Additionally, in some cases copy of data does not require physical connection to the computer. Data can be transmitted with use of cellular networks or wireless internet based technologies. The data than can be processed by commercial software or Ground Data Replay and Analysis Station (GDRAS) and analyzed for the detection of exceeding data (when some parameters across the limits), statistical study (in order to compare some parameters with statistical trends) or presence of undesired events including malfunctions. The available information can be also used for the purposes of the Flight Operational Quality Assurance (FOQA), Maintenance Operational Quality Assurance (MOQA) software as well as for extended operator's analyses such as aimed at improvement of performance or service life optimization.

The so called Flight Data Monitoring system (FDM), which can be employed during data analysis, is considered as powerful tool for monitoring and improvement of operational safety. Dedicated to be integrated into the operator's Safety Management System (SMS), FDM have possibility to significantly enhance the efficiency of detection, confirmation and assessment of safety related issues as well as to improve the validation and evaluation process in terms of effectiveness of applied corrective actions.

The specification concerning the type of recorded parameters, its sampling rate, accuracy as well as recording format differs significantly from one operator or manufacturer to another. Mostly due to different aircraft specification and also various standards employed. This fact is expected to be source of difficulties during the process of implementation of continuous monitoring based on common taxonomy as indicated in numerous ASCOS deliverables.

Simultaneously it has to be noted that FDM system should be integrated part of Integrated Vehicle Health Monitoring system (IVHM), which - in contrast to maintenance related functions - would focus on human connected issues concerning mainly exceeding data, compliance with operational procedures and safety relevant actions monitoring (CMC – malfunctions, FDM pilot errors).

Effective use of data collected and recorded by either Central Maintenance System or Flight Data Monitoring enforces standardization. This standardization should enable implementation of indicators necessary for introduction of method for automatic capture of faults using a safety barrier oriented taxonomy for automatic coding. Only valid, accurate and correctly sampled flight parameters can make it feasible. Not all currently employed systems meet those conditions. In addition many of considered as key indicators is not achievable, due to the fact that flight parameters are not recorded with sufficient sampling rate, accuracy or not recorded at all.

Therefore further considerations in this section is based on assumption that change in flight data monitoring and storing aiming at unification is necessary and forthcoming.

6.2 Generic taxonomy - safety barrier failure oriented

The first step toward easy identification and capture of precursors and events preceding the accident is definition of appropriate taxonomy which will be as much as possible coherent both with any commonly used standard taxonomy and barriers identified in ASCOS CATS model. This taxonomy will be used for coding precursors when they occur.

According to Safety Management System Manual issued by ICAO as well as European regulatory documents, the ADREP 2000 and CICTT (CAST/ICAO Common Taxonomy Team) taxonomy principles were selected. The requirement of coherency with CATS risk model entails the need for extension of the CAST/ICAO taxonomy with additional indicators enabling unequivocal assignment to appropriate CATS risk model. In the further part of the document, the new taxonomy is entitled the CICTT/ASCOS taxonomy.

Implementation of the process entails three steps:

- Failure detection. It can be realized with use of health monitoring systems detecting aircraft component failures or, in some range, the human errors (e.g. pilot or controller) or crew recognizing improper functioning of a system (e.g. ground service related). Requirement of automatic capture/ coding of precursors in many cases leads to the necessity of extension of system's ability to detect the failures by equipment with new-type sensors and instruments. It can be a challenge, especially in area of human errors related to tasks strictly dedicated to human domain (e.g. spatial disorientation or PNF involvement in monitoring).
- Assignment to appropriated occurrence category, according to new extended CICTT/ASCOS Taxonomy.
- Identification of linkage with relevant ASCOS risk model.

The new CICTT/ASCOS taxonomy should:

- Indicate on the flight phase the precursor event occurred.
- Classify the errors related to system malfunction or failure, flight crew, air traffic controller, maintenance and ground service.
- Be extended with more detailed designation in order to enable easy linkage with ASCOS risk model and avoid ambiguity.

Presented in ASCOS risk model, safety barriers failures expressed in particular *Base Events* are considered as precursors for *End Event* for all considered risk models. In below text the term event should be understood as Base Event and precursor at the same time.

Example 1. Anti-ice or de-ice function failure (according to CICTT/ASCOS taxonomy):

SCF–NP–MISC–ANTICEFL
Where:
SCF – System/component failure or malfunction
NP – non-power plant
MISC – miscellaneous system
ANTICEFL - Anti-ice or de-ice function failure.

The occurrence defined in such manner can be linked with four ASCOS risk models related to four different accident scenarios. The complete designation enabling unambiguous linkage with ASCOS risk model entails extension with indicator related to the flight phase and detailed component suffering pointed dysfunction.

New comprehensive designation with relation to anti-ice or de-ice function failure should be as follow:

a. **TO–[ICE]–SCF–NP–MISC–ANTICEFL–LIFTSURF**

Where:

TO – designation of the flight phase (TAKE-OFF)

[ICE] - Designation of occurrence category according to CICTT (if icing conditions occurred)

LIFTSURF – indication of component with relation to which anti-ice or de-ice function failure is detected (lift generating surfaces ice protection system).

Such defined occurrence can be unambiguously linked with barrier - Pre-Service De-icing Procedure in ASCOS ESD 6 - Aircraft takes off with contaminated wing risk model.

b. **ER–[ICE]–SCF–NP–MISC–ANTICEFL–LIFTSURF**

Where:

ER – Designation of the flight phase (EN-ROUTE)

Such defined occurrence can be unambiguously linked with barrier - Anti-icing system integrity in ASCOS ESD 15 – Ice accretion on aircraft risk model.

c. ER–[ICE]–SCF–NP–MISC–ANTICEFL–PITOT

Where:

PITOT – Pitot static ice protection system.

Such defined occurrence can be unambiguously linked with barrier - Integrity of main flight control instrument (ASI, ADI, PFD) in ASCOS ESD 16 – Flight instrument failure risk model.

d. ER–[ICE]–SCF–NP–MISC–ANTICEFL–ENGIP

Where:

ENGIP – Engine ice protection system.

Such defined occurrence can be unambiguously linked with barrier – Single/Dual engine integrity in ASCOS ESD 18 – Single engine failure risk model.

Example 2. The event of lack of pilot reaction in situation of loss of control after rejected take-off

Many of accident occurrences are directly resulted from flight crew errors and are free of any systems malfunctions or structural failures. In the contrary to system component failure category which quite precisely classify most of equipment failures, the ADREP 2000 and CICTT taxonomies do not cover such occurrences unless they turn into accident or incident able to be classified as e.g. LOC or GCOL. Lack of (possibility for) automatic capturing of all flight crew errors (which often do not directly affect the safety but can be precursors for e.g. mentioned occurrence categories) is serious obstacle in real safety improvement implementation. Efficient pilot error detection process elaboration is a challenge for future, but undoubtedly it is necessary to define the taxonomy covering this issue especially if it is identified as critical element in many safety risk models. The below example presents taxonomy reflecting the event of lack of pilot reaction in situation of loss of control after rejected take-off (specified in ASCOS ESDs no. 1 to 5, 9 and 10).

a. RTO-LOC-G-FCE-LCTRL

Where:

RTO – designation of the flight phase or last important event (here Rejected Take-off)

LOC-G – occurrence category appeared during the flight phase (here Loss of Control on Ground)

FCE – the reason for the occurrence category (here flight crew error)

LCTRL – type of the reason (here: lack of control on the aircraft by flight crew).

b. AL-ATM-ATCOER-IGN-FCWRN

Where:

AL – designation of the flight phase (here approach and landing)

ATM – occurrence category appeared during the flight phase (here air traffic management)

ATCOER – the reason for the occurrence category (here air traffic control officer error)

IGN – type of error (here: ignoring)

FCWRN – detailed error (here flight crew concerns in terms of trajectory commanded)

Occurrence defined in such manner can be unambiguously linked with barrier – on-board monitoring in ASCOS ESD 35 – Flight crew decision error / operation of equipment error risk model.

c. GM-[GCOL]-GSE-EQMOV

Where:

GM – designation of the flight phase (here ground movement: taxiing, marshalling and other not necessary restricted to aircraft)

GCOL - occurrence category appeared during the flight phase (here: ground collision if appeared)

GSE – Ground service error – where it was recognized that safety barrier failure was resulted with inappropriate act of flight crew

EQMOV – type of error (here equipment movement)

Occurrence defined in such way can be unambiguously linked with barrier – Ground collision avoidance in ASCOS ESD 36 – Ground collision imminent risk model.

As described above, the new safety barrier failure oriented taxonomy CICTT/ASCOS should be detailed and extended in comparison to CICTT taxonomy.

- Detailing should aim at deeper failures and errors classification. It is necessary in order to link occurrence or precursor appeared with appropriate safety risk model.
- Extension should allow for better human error classification. It would be first step in automatic identification of human error as precursor for various occurrences.
- Flight phase indicator should be an inseparable part of new occurrence designation system.

6.3 Automatic capture/coding and recording

The topic of automatic capture/coding and recording of system malfunctions which have potential to be a precursor for more serious occurrences is already quite widely explored. As described in section 5.5.1, the leading aircraft manufacturers increasingly better understand the advantages of predictive approach for maintenance and reliability of big commercial aircraft and focus their efforts on developing more and more complex and autonomous health systems. But at the same time it has to be kept in mind that requirement of maximisation of positive impact resulted from harnessing the proactive approach entails the Total Aviation System perspective and common methodology in the entire process.

But also the difficulties related to the event capture/coding process have to be kept in mind. As indicated ASCOS D2.3, current technical possibilities in area of homogenous data collecting are very limited. Different specification of aircraft resulting from their configurations and performances as well as various coding methods lead to practical disability of using what is provided by air operator data as a basement for common process. Despite the visible and potential difficulties as the most powerful tool for any occurrence detection the FDM system (or equivalent able to process, store and alternatively send data via ACARS system) should be considered. Besides large opportunities in risk event detection it also can provide data allowing for system malfunction identification.

The requirement of malfunction coding with accordance to safety barrier failure oriented taxonomy defined in the previous section leads to the need for more detailed information provided by the aircraft systems when compared to CICTT or ADREP 2000 taxonomy. The set of example symptoms allowing for precise event identification are presented in the table 1 (an example) as well as in the Annex 1 (all ASCOS ESDs). It should be additionally translated into strictly technical system parameters as signal level, signal amplitude or others dependent on system specification. All critical aircraft systems, especially in modern aircraft are equipped with their own diagnostic system providing central maintenance computer with information about problems when they occur. Many failures included in ASCOS risk model touch the systems or situations which are not covered by capabilities of currently available diagnostic/warning systems or concern the failure of those diagnostic/warning systems. Therefore, as a critical element, enabling automatic precursors capture/coding, new failure detection methods should be considered. It is assumed that they should be based on potential (current and expected to appear in near future) possibilities of aircraft maintenance computers. It in turn entails the following requirements and assumptions:

- Extension of diagnostic skills of currently available aircraft health monitoring systems or maintenance computers by equipping them with additional instruments and sensors enabling detection of new phenomena identified as having potential for being a precursor should be considered as unavoidable.
- Large number of precursors is related with human errors. For some of them it is possible to propose methods to efficiently detect them and code according to new safety barrier oriented taxonomy. Beside mentioned extended possibilities of aircraft computer (here by tracking pilot actions and comparing them to the reference models) there is need for closer linkage and cooperation between various aviation domains. For example: parallel and simultaneous communication of ATCO with flight

crew and ATM system with aircraft FMS allowing for supervision of ATCO and flight crew actions and decisions. Some benefits are expected to appear due to SWIM (System Wide Information Management) implementation (see 5.5.4 section).

- In some cases deferred detection of precursor event is less problematic (or more reliable or less cost demanding) than automatic, in-operation detection of occurrence resulted from it. In addition unerring safety barrier failure detection can be impossible without information about the precursor appeared in other flight circumstances such as during maintenance, or even design or manufacturing of aircraft components. The structural failure can be given as an example. The similar situation can be observed in terms of some pilot errors. The precursor appeared during training on simulator can provide necessary tips for successful safety barrier failure identification. In both cases automatic capture/coding of precursor event process has to be proceeded by analysis of specific data gathered during all aircraft's life cycle phases as well as during pilot training. Therefore:
    - Design process captured by certification. Correct detection and capture/coding of in-flight precursors events as well as related safety barrier failure entails the need for deeper data about design quality. They can be acquired by e.g. indication: whether all (if not how many) recommended practices were applied or employed during design of given structural component; what is real safety margin in terms of component material strength and fatigue both theoretical and supported by tests. Additionally aircraft maintenance computer should be equipped with all critical structural components datasheets containing mentioned information.
    - Manufacturing process captured by quality control. Here the highest weight should be assigned to repeatability in components production resulted with different material specification. Similarly to design process also all considered as potentially critical aircraft components specifications resulted from manufacturing quality should be included in structural components data sheets and be available for aircraft maintenance computer.
    - Maintenance. Currently the quality of maintenance process is supervised by airworthiness specialists signing the appropriate papers. This activity as being a typical human domain can be a source of many precursor events able to turn in serious occurrences during aircraft operation. In addition proper monitoring of this process represents significant potential in delivering the tips for aircraft computer enabling error free, automatic detection and capture/coding of in-flight precursors and safety barrier failures. Therefore it is considered as necessary to harness aircraft maintenance computer or other ground located entity to monitor the aircraft maintenance process and detect and code the events able to impact the safety.
    - Flight crew training. Data gathered during last phases of pilot training on simulator or in flight should be used to elaborate pilot personal skills profile. Validated profile extended with experience related data and pilot's strengths and weaknesses could be useful for correct identification of source of failure or flight crew related errors (in the cases of lack of any hard indications).
- More complex and dynamic events such as fire on board, cracks in pressure boundary or main aircraft structure failure can be extremely difficult to be precisely identified. In some cases a couple of most

probable variants would be coded by the maintenance computer. The selection of the correct one would be conducted / supported by the system operator.

- It is possible that proposed methods do not exhaust given events/precursors. In many cases they would need for deeper reliability analysis. Especially in terms of scenarios concerning simultaneous appearing of two and more events.
- Also other precursors identified in ASCOS D2.3 should be taken into consideration. Although they are not named in any ASCOS CATS risk model it is obvious that they have potential to significantly impact the safety. The most important seems to be these related to pilot work quality and his current psychomotor fitness – manifesting itself by adherence to procedures and tiredness resulted from example from work overloading.
- CATS/ASCOS risk model as being, an envelope of aviation accidents and a picture of history based on aviation experience in area of accidents does not contain all currently or lately introduced safety barriers. It has to be noted that presented model, extended with dedicated taxonomy do not represent current aviation safety picture and both the model as well as taxonomy should be considered to be continuously updated. In addition the increasing automation range and relying on computer would enforce increasingly deeper ASCOS model compatibility with central aircraft computer risk model as playing more and more critical role in area of entire system reliability.

In many cases, implementation of appropriate procedures, and tools allowing for process control in other aviation activities which have contact with aircraft (e.g. airport ground service) would lead to significant increase of the operational cost (cost of new handling equipment). Therefore it is suggested that cost-benefit analysis should be performed in order to answer the question about reasonability.

The example in Table 3 presents new safety barrier oriented taxonomy and linkage with the ASCOS risk model together with proposed precursor detection methods. A complete set of examples can be found in the Appendix.

Beside safety barrier failure detection and coding it is also worth to collect experience about events where safety barrier successfully broke the event sequence leading to unsafe situation. Every such case would be specified by appearing of precursor followed by decline or disappearance of indication of deviations (pointing on system/component/human failure). Detailed successful barrier working can be assigned to one or more last actions made by automatic system or human.

Barrier	Description	Possibilities for braking the barrier – Base event	Code	Possible occurrence (CICTT)	Designation (CICTT)	Flight phase indicator	Proposed method for failure detection (trigger logic)
1.Correct configuration of aircraft for take-off	Proper conducting of procedure concerning setting of appropriate aircraft configuration for take-off	Unsuccessful TO configuration checklist	TO05B111	Flight crew error (FCE) - Lack of configuration checklist	**TO-FCE-LCNFCHCK**	Phase 1: Landing gear compression longer than 10min and at least 1 from: 1. Altitude equal 0ft AGL, 2. Thrust taxiing mode.	- Negative cabin voice record analysis for key words (configuration checklist) - OR Indicated flaps & slats positions differ than expected / suggested (calculated for current aircraft specifications and external conditions) - OR Negative cabin voice record analysis for key words (verification of FMC input)
		Unsuccessful Checklist Verification	TO05B112	FCE – unsuccessful configuration checklist	**TO-FCE-LCHCKLVER**		
		Flap & slat positions entered into FMC incorrectly	TO05B12	FCE – incorrect operation of FMC - flap and slat position entering	**TO-FCE-FMC-INCOPER-INCFLSLENT**		
		Verification not conducted	TO05B21	FCE – lack of verification of flap and slat position entered into FMC	**TO-CFE-LVRFER-FMC-FLSLSET**		
		Verification unsuccessful	TO05B22	FCE – unsuccessful verification of flap and slat positions entered into FMC	**TO-CFE-VRFERF-FMC-FLSLSET**		
2.Take-off configuration warning	The flight crew is provided with the alert	Unsuccessful Manufacture	TO05B311	Warning loss – manufacture findings	**TO-SCF-NP-AVION-WRNLS-TOCW-MFF**	Phase 2: At least 2 from: 1. Speed above ~35kts	- Take-off roll acceleration values different than expected

Barrier	Description	Possibilities for braking the barrier – Base event	Code	Possible occurrence (CICTT)	Designation (CICTT)	Flight phase indicator	Proposed method for failure detection (trigger logic)
	concerning incorrect aircraft configuration for take-off			Automatic protection functions failures – manufacture findings	**TO-SCF-NP-AFC-AUTOPROTFL-TOCW-MFF**	and not decreasing 2. Altitude: 0 - 50ft AGL, 3. Application of take-off power	(calculated for current aircraft specification and applied engine power as well as external conditions) for take-off roll
		Unsuccessful Maintenance	TO05B312	Warning loss – maintenance findings	**TO-SCF-NP-AVION-WRNLS-TOCW-MF**		
				Automatic protection functions failures – maintenance findings	**TO-SCF-NP.-AFC-AUTOPROTFL-TOCW-MF**		
		Unsuccessful Operation	TO05B313	FCE – unsuccessful operation of TOCW System	**TO-FCE-INCOPER-TOCW**		- OR TOCWS not active OR not reset
		Unsuccessful Manufacture	TO05B321	Electrical power system failure - TOCWS related – manufacture findings	**TO-SCF-NP-ELEC-TOCW-MFF**		- OR TOCWS not active AND other aircraft system not active (dividing the same bus)
		Unsuccessful Maintenance	TO05B322	Electrical power system failure - TOCWS related – maintenance findings	**TO-SCF-NP-ELEC-TOCW-MF**		

Barrier	Description	Possibilities for braking the barrier – Base event	Code	Possible occurrence (CICTT)	Designation (CICTT)	Flight phase indicator	Proposed method for failure detection (trigger logic)
		Aircraft takes-off with incorrect configuration	TO05B33	Warning loss	**TO-SCF-NP-AVION-WRNLS-TOCW**		- OR TO roll and flight parameters indicate on not optimal aircraft configuration
3.Execution of take-off rejection being a consequence of TOC problems	Proper decision of the crew concerning termination of take-off procedure	Pilot Misdiagnosis	TO05B411	FCE – misdiagnose the problem occurred during take-off and rejected take-off above V1	**RTO-FCE-MISD-RTOABV1-INCTOC**	Phase 3a: Following Phase 2 AND Braking application and at least two from: 1. Speed above V1 and not increasing, 2. Altitude – 0ft AGL, 3. thrust idle or reverse mode	- Take-off rejection after reaching the V1 speed
		Pilot Misjudgement	TO05B412	FCE – misjudgement in terms of necessity of rejected take-off above V1	**RTO-FCE-MISJ-RTOABV1**		
		Take-off rejected correctly when below V1	TO05B42	Take-off rejected correctly	**RTO-INCTOC**	Phase 4. Following Phase 2 AND Braking application and at least two from: 1. Speed below V1 and not increasing and at least one from: 1. Altitude – 0ft AGL, 2. thrust idle or in	- OR Take-off rejection at speed below v1
4.Effective braking after execution of take-off rejection being a consequence of TOC	Parameters of braking systems and devices included into assumed / expected range	Insufficient Runway Length	TO05B51	Runway too short due to poor surface condition (ice or wet)	**RTO-ADRM-INSRWYL**		- Runway excursion AND braking devices work correctly AND braking performed correctly. - OR Deceleration parameters lower than expected (calculated for current conditions) AND/OR
		Brakes not functioning correctly	TO05B52	Automatic braking loss	**RTO-SCF-NP-AFC-ABRKLS**		
				Automatic braking operation error	**RTO-SCF-NP-AFC-ABRKERR**		

Barrier	Description	Possibilities for braking the barrier – Base event	Code	Possible occurrence (CICTT)	Designation (CICTT)	Flight phase indicator	Proposed method for failure detection (trigger logic)
problems				Brake system failure	**RTO-SCF-NP-LG-BRKFL**	reverse mode	braking asymmetry AND all braking devices applied on time and correctly - OR thrust reverser not deployed - OR execution of braking procedure conducted by the flight crew differs significantly from the assumed as reference model.
				Reverser / beta malfunction - failure to deploy	**RTO-SCF-PP-RFD**		
		Brakes not applied correctly	TO05B53	FCE – brake application error	**RTO-FCE-BRAKAPP**		
5.Stall avoidance after take-off with unrevealed incorrect take-off configuration	Flight crew avoid aircraft stall resulted with unrevealed incorrect take-off configuration	Stall Unavoidable	TO05B61	Loss of control in flight during take-off in result of incorrect configuration	**TO-LOC-I-INCTOC**	Phase 3b. Following Phase 2. AND Speed above V1 and not increasing, and at least two from: 1. Altitude above 0ft AGL, 2. landing gear not compressed, 3. thrust in take-off mode.	- Flight parameters indicate on near stall AND lack of icing conditions - OR Actions taken by the flight crew do not cover procedure assumed as optimal for given conditions - OR Flight parameters (speed, configuration, AoA) indicate on near stall condition AND lack of stickshaker warning AND lack of icing condition
		Pilot ignores stickshaker	TO05B622	FCE – ignoring of stickshaker warning	**TO-FCE-IGN-STICSHKRWRN**		
		Stick shaker failure	TO05B6211	Warning loss	**TO-SCF-NP-AVION-WRNLS-STICSHKR**		
				Automatic protection functions failures	**TO-SCF-NP-AFC-AUTOPROTFL-STICSHKR**		

Barrier	Description	Possibilities for braking the barrier – Base event	Code	Possible occurrence (CICTT)	Designation (CICTT)	Flight phase indicator	Proposed method for failure detection (trigger logic)
		Stall AOA too low	TO05B6212	Automatic protection functions failures	**TO-SCF-NP-AFC-AUTOPROTFL-STICSHKR**		- OR Flight parameters indicate on stall AND AoA lower that necessary for stickshaker activation AND lack of icing conditions
6. Recovery of control after stalling being a result of unrevealed incorrect configuration	Flight crew recover the aircraft after stall being a result of unrevealed incorrect take-off configuration	Uncontrollable	TO05B71	Aircraft incontrollable in result of stall	**TO-LOC-I-STALL**		- Flight parameters indicate on near stall AND lack of icing conditions
		Lack of control	TO05B72	FCE – lack of reaction of flight crew on aircraft stall	**TO-LOC-I-FCE-LCTRL**		- OR Inconsistency between flight crew input to aircraft control and identified as optimal for given situation (defined and coded in aircraft system)
		Incorrect Control	TO05B73	FCE – incorrect flight crew input to aircraft control	**TO-LOC-I-FCE-INCTRL**		
		Insufficient control	TO05B74	FCE – insufficient flight crew input to aircraft control	**TO-LOC-I-FCE-INSCTRL**		

Table 3 Possible methods for automatic precursor's detection and coding in accordance with safety barrier failure oriented taxonomy ASCOS ESD 5 - Take off with incorrect configuration

6.4 Total Aviation System approach

The example of ESD 5 'Take-off with incorrect configuration', as well as others included in the Annex 1, indicate that failures or precursors identification, detection and automatic capture/coding with use of aircraft maintenance computer is relatively easy and currently restricted only by:

- limited computational power of aircraft systems,
- limited number of available sensors and instrument allowing redundancy in precursor detection, especially in situation of failure one of them.

Additionally, knowledge and experience gathered in aviation allow for quite precise modelling of even more complex phenomena in area of aerodynamic, flight mechanic and thermodynamics in order to efficiently identify the disparities (precursors). Therefore it can be assumed that this technology development ultimately aiming at enabling autonomous operations in future will be able to be harnessed for operation monitoring first. Beside aircraft systems condition/health it will allow also for flight crew actions supervision. In addition unerring automatic safety detection and capture/coding of in-flight precursor event can be supported by data concerning the design manufacturing quality.

As the safety in aviation is not limited to aircraft and many failures origin in other aviation domains some standards unification is necessary. Automatic detection and coding of precursors occurring outside the aircraft can only be realized by enabling of continuous computer/automatic monitoring of all relevant activities concerning both correct functioning of supporting systems as well as proper and error free work of human. In ATM domain it can be achieved by:

- Separate ATCO monitoring system interpreting controller decisions and looking for system errors and non-optimal decisions. Systems based on solutions employed in STCA system would be satisfactory.
- Such a system can be supported by aircraft computer. Sent via controller-pilot data-link communication (CPDLC) clearance would be analysed by Flight Control System for inconsistency with data computed on base of on-board flight instruments (e. g. in cases of CFIT). Beside possibility of ATCO decision verification it also would allow for easier automatic detection and capture/coding of relevant precursors (e.g. related with flight instrument malfunctions).
- The controller training and licensing processes as being conducted with use of simulators and real work create ability to collect related data allowing for building the individual controller skills profile. Controller's areas of weaknesses as a collection of potential precursors together with data concerning experience can serve to more reliable detection and capture/coding of events being an evidence of safety barrier failure.

On airport by:

- CCTV based monitoring of ground service equipment movement. Properly located cameras attached with dedicated software would also control and track the vehicle and workers position.
- The equipment failure and malfunction should be monitored on base of vehicle operators reporting. Providing the devices with automatic systems would be too expensive and should be excluded from consideration.
- Using aircraft systems for monitoring of both aircraft and other ground service equipment (only when separation is infringed). It would allow for avoiding large costs related with capturing of airside activity not directly related with aircraft traffic safety.

In the light of the above the envisioned input of technology advance and ATM information management improvement resulted from SWIM (System Wide Information Management) implementation should also be considered as having significant impact on real possibilities of automatic detection and capture/coding of related precursors. It will be achieved by introduction of SWIM related elements. Especially:

- Standards. That is ATM information model representing the standard definition of all ATM information, through harmonized conceptual and logical data models. Practically AIRM (ATM Information Reference Model) will enable automatic reading of information messages such as NOTAM or weather data by the aircraft system and using them for automatic detection and precursor capture/coding purposes.
- Infrastructure. The SWIM Technical Infrastructure (SWIM-TI) over which different services are provided (ATM data distributed, shared and consumed (ground/ground and air/ground)). The SWIM Air/Ground TI will allow aircraft to access ground-based SWIM, will provide it with services complementing the existing data-link applications (e.g. CPDLC) and will enable information sharing between aircraft and multiple ground SWIM enabled systems. It will create a possibility for redundant real time data storing and processing as well as will allow for in-flight precursors detection and capture/coding on base of on-ground facilities.

SWIM will enable the management of ATM information and its exchange between qualified parties via interoperable services. It is highly expected that solutions implemented within the framework of SESAR through standardization and unification ATM related systems will deliver many very usable means allowing for more efficient and reliable process for automatic detection and capture/coding of precursor events concerning both aircraft, ATM and aerodrome domains.

In terms of airworthiness:

- Employment of ground located facilities or/and aircraft maintenance computer as well as built-in test equipment of every aircraft/system components to track and monitor the maintenance process conducted.
- Additionally the monitoring and supervising process can be enriched by harnessing automatic health monitoring procedures aiming at verification of maintenance work results.

Flight crew licensing

- As indicated above, the pilot training and licensing processes supported by flight simulators and real aircraft create ability to collect related data allowing for building the individual pilot skills profile. Pilot's areas of weaknesses as a collection of potential precursors together with data concerning experience can serve to more reliable detection and capture/coding of events being an evidence of safety barrier failure.
- Significant differences detected during flight (between individualized pilot skills profile and airmanship quality) can in turn help to detect pilot incapacity resulted from illness or tiredness.

Unerring cause identification and capture/coding – concerning the reason for system/component failure or pilot/ground service/ATCO error is highly dependent on development of automation technologies able to track, monitor and supervising of various processes. In many areas is still a challenge. In addition multi-domain character of many accident sequences requires close cooperation between different domains of Total Aviation System. Especially in terms of definition of compatible interfaces for unconstrained information transfer within the TAS. It is critical element for successful implementation of efficient and reliable automatic precursors capture/coding process in aviation.

7 Management of safety activities for Total Aviation system

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

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

Of primary target are project breakdown structures. These activities should be harmonized and coordinated at the highest level. Of most importance is the identification of safety standards to apply to answer to the argument tree developed in accordance with ASCOS D1.3 recommendations. These safety standards should formalize development processes for Safety assessments, DAL assignment, requirement capture, requirement validation, requirement application verification, project organization/documentation, deliverables management, schedule management, process assurance, configuration management. Of most importance are also the "Safety plans" and the safety requirement validation plan, without which there will be no assurance of any safety method application.

Although the operational reliability and the integrated logistic support activities are not strictly speaking part of the safety and certification, these activities can be integrated within the same framework as safety activities To assure a good interface management between the different stakeholders of a project, a sound and seamless engineering, the continuity of safety assessment practices and the seamless application of the rules, all the activities described in previous chapters should be promoted, initiated, coordinated and monitored at:

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

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

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

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

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

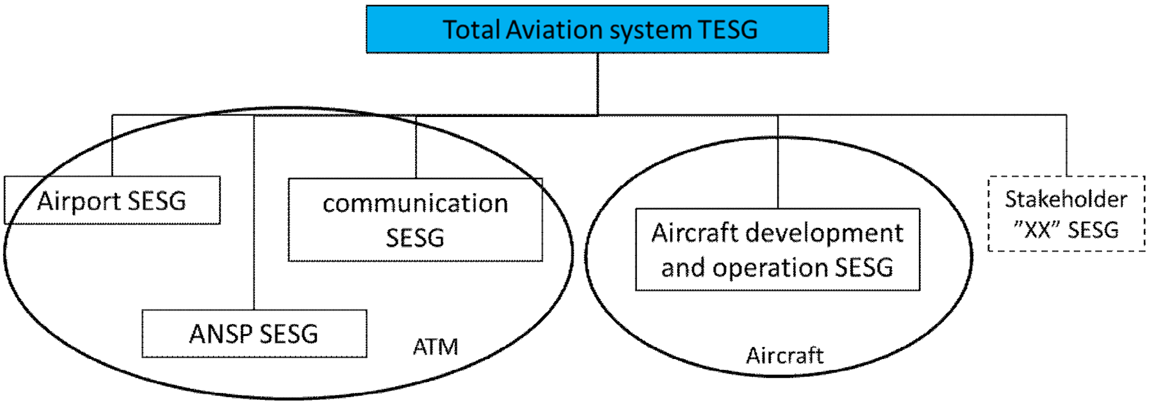


Figure 26- Safety management organization at TAS inter-stakeholder level and at stakeholder level

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

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

1. Identify and promote coherent safety standards framework to apply at inter-stakeholder level and at each stakeholder level for product development, interface management, safety assessment methods, software item development, electronic hardware item development, procedure and services development (including human factor)
2. Develop a safety plan and methods for the inter-stakeholder safety activities
3. Assure coherency between the tools used by the different TAS stakeholders
4. Promote safety culture and assure that safety training courses are available and given to safety involved people
5. Assure that lessons learned processes are established within each stakeholder organization
6. Identify safety lessons learned from previous accidents and provide visibility to each stakeholder
7. Establish and communicate the principles and data to apply to assure coherency between the safety assessments performed by each stakeholder
8. Assure compliance with ICAO SMM and European Aviation Safety Plan (EASP)
9. Identify inter-stakeholder accident scenarios with associated "Event Sequence Diagrams" (ESD)
10. Identify Area of Change to consider with associated future accident scenarios and ESD
11. Establish and allocate the safety objectives and the studies to perform by each stakeholder that contribute to the inter-stakeholder ESD
12. Monitor the completion of each stakeholder contribution to inter-stakeholder ESD

13. Perform inter-stakeholder Common Mode Analyses and evaluate Common Mode Analysis from each stakeholder
14. Issue total aviation system safety results
15. Coordinate with TAS certification authorities
16. Monitor the TAS level lessons learned and standards improvement process

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

1. A safety assurance plan describing the Safety Management Strategy and associated tasks for in operation safety assurance. This plan should be compliant with the TAS Safety Management Process Guide and with the regulation applicable to each individual organization. The safety assurance plan should particularly identify all the tasks associated to dissemination of safety information between the TAS stakeholders through the TAS level ESG (TESG). This plan may be structured around the activities recommended in:
    a. The ARP 5150 for aircraft Safety Assessment in operation
    b. The "Management of risk: Guidance for Practitioners" published by TSO (The Stationary Office) on behalf of Office of Government Commerce and applied by some ATM bodies
2. The safety methods to perform the tasks described in the safety plan

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

The organization principles at TAS level and stakeholder level developed above should be incorporated in the revised ED 78A

8 Conclusions and recommendations

A seamless certification process at total aviation system implies coordination and coherency between the different stakeholders of the TAS. This coordination and coherency should be reflected in the safety standards used by each stakeholder of the TAS and in the TAS Safety organization.

Safety standards harmonization

Depending on the different stakeholders of the TAS and on the field of application, the set of applicable safety standards is often not complete not coherent and often does not refer the internationally agreed processes or methods. This situation leads to difficulties in communications with the certification authorities and between the TAS stakeholders and may lead to overlook inter stakeholder safety issues.

To improve this situation, this study promotes the application of a “common safety standard framework” by each of the TAS stakeholder that will help to avoid certification bottlenecks, to avoid identifying certification safety issues late in the certification process and to give confidence and transparency to the certification authorities on the safety process that is applied by each stakeholder during product development as well as during operation.

To be coherent in interface, the ED78A standards used for TAS level and ATM stakeholder level and the standard used at other stakeholder level (for example the ARP4754A/ED79A standard used at aircraft stakeholder level) should be revisited in order to make them consistent in term of requirement validation, requirement exchange, DAL assignment.

In the aircraft development standard (ARP 4654A) the failure/error severity repercussion should be extended for consideration of aircraft failure/error repercussion on ATM operations.

Safety standards continuous improvement

If safety standards are disconnected from the in operation experiences they may become obsolete and may not be able to address all safety situations. To solve this issue, safety standards should be continuously the subject of review for improvement considering the results of their application on product certification performances and on in operation safety behavior.. This improvement activity will assure the permanent adaptation of the standards to the safety and certification needs while maintaining a seamless certification process.

Feedback loop for safety standards improvement

The safety Standard improvement is based on implementation of a feedback loop between the safety event in operation t and the development/design process. To be efficient this feedback loop needs to

- Identify the safety event to monitor. This may be done through the identification during the development process of a Safety Precursor list
- Capture safety events, particularly those associated with safety precursors

- Identify root causes and define the mitigation strategy to implement in the development process to avoid reoccurrence
- Translate the defined mitigation strategy in Lessons Learned Requirement (LLR) for application and safety standards improvement.

Feedback loop request

The request for this feedback loop and the associated management principles should be incorporated in the IR / AMC / GM from RMT 469/470 working group and developed in the safety assurance standards used at the level of each stakeholder (e.g. ED79A/ARP 4754A and ARP 5150A for aircraft manufacturers).

Safety precursor automatic capture and identification

To improve the safety assurance in operation and the collection of safety precursors it is possible to envisage the implementation of automatic means to detect and capture safety precursor occurrence. These possibilities are developed in Chapter 6.

TAS safety management organization:

Each stakeholder of the TAS is participating to the overall safety performance at TAS level. These stakeholder activities are interconnected and the lack of a clearly identified management structure at TAS level may lead to overlook safety issues, generate certification bottlenecks, induce non coherency between TAS stakeholder safety activities.

This study recommends the implementation of a TAS safety management organization to assure a coherent and seamless certification activities at TAS level, to drive inter stakeholder safety activities and enforce coherency between the stakeholder safety standards. This TAS safety management organization will be based on an Engineering and Safety Group (ESG) at total aviation system inter-stakeholder level (TESG) and of an Engineering and safety group at the level of each stakeholder (SESG). This organization will assure implementation of a common safety standard framework between the TAS stakeholders with safety standard harmonization, the application of a harmonized Lessons Learned feedback process for safety standards improvement. It should be the interface with ICAO/EASA for application of the SMS and State Safety Plan as defined by the ICAO/EASA.

The organization principles at TAS level and stakeholder level developed above should be incorporated in the ED 78A and in standards used at stakeholder level (e.g. ED79A/ARP 4754A)

Development and safety assurance standards updating actions

- **For inter stakeholder level**, improving the IR / AMC / GM from RMT 469/470 working group and the ED78A following EUROCAE WG91 comments to define the inter stakeholder activities and ask the use of a common standard framework for development activities and for safety assurance activities of each TAS stakeholder

- **For the aircraft stakeholders**: updating of the current development and safety assurance standards taking the opportunity of:
  - The current reopening of the ED79A/ARP 4754A by EUROCAE WG63 and SAE S18 committee to produce an issue B
  - The current reopening of the ARP 5150 (Aircraft Safety assurance in operation) by EUROCAE WG63 and SAE S18 committee to produce an issue A.
- **For the other stakeholders**: start a standard identification activity and develop/update standards to be compliant with the updated ED78A directives and coherent with other TAS stakeholders

Appendix A Recommended action list

The table below summarizes the activities to implement at TAS level (inter-stakeholder) and at each stakeholder level to improve safety standard organization by:

- Setting a common safety standard framework and developing coherent safety standards applicable at inter-stakeholder level and at each stakeholder level
- Implementing a continuous safety standard improvement loop based on a safety precursor capture and on application of lessons learned from in operation events. Consideration of implementation of a safety precursor automatic capture/coding system
- Implementing at inter-stakeholder level a safety and engineering activity to coordinate stakeholder safety activities and integrate safety stakeholder results at TAS level

The details of these actions are summarized in the following table

Action REF	Action description	Action owner	Chapter ref for explanation
	1- Safety standards organization		
1.1 Safety standard framework	1.1.1 consider in IR / AMC / GM deliverables from RMT 469/470 WG the model illustrated in ASCOS D3.5 figure 15 (slide 16 and 17 of this presentation) to implement a common safety standard framework applicable at each TAS stakeholder level and covering both product development and in operation safety assurance 1.1.2 Extend the application of the ED78A to other development activities than Data Link	RMT 469/470 WG EUROCAE WG 53/ WG 91	4.4

1.2 Safety standards development	1.2.1 Consider in IR / AMC / GM deliverables from RMT 469/470 WG and in ARP4754A/ED79A consistency in term of requirement exchange, requirement validation, DAL assignment and failure/error severity classification. 1.2.2 Implement the ASCOS Standard framework and Develop/identify and implement, at the level of each stakeholder, a coherent safety standards for: - Product development - Safety assessment/analysis applicable methods - Software Item development - Hardware item development, - Procedure and service development - Safety assurance in operation For aircraft stakeholder: review ARP 4754A/ED 79A, ARP 5150. For other TAS stakeholders: identify standards and make them coherent with revisited ED 78A directives	- RMT 469/470 WG SAE S18/ EUROCAE WG 63 SAE S18/ EUROCAE WG 63 To be defined	4.2 - 4.3 - 4.4
2- Safety standard continuous improvement loop using a safety precursor approach –			
2.1 Safety precursor identification at TAS level	In IR / AMC / GM deliverables from RMT 469/470 WG for TAS (inter-stakeholder) level implement a process for safety precursor identification based on CATS Event Sequence Diagrams (ESD)	EUROCAE RMT 469/470 WG	5.2
2.2 Safety Precursor identification at stakeholder level	At each stakeholder level Develop a process for safety precursor identification during product development/implementation phases (results from safety assessments) using safety assessment results and CAT Event Sequence Diagrams (ESD) (for aircraft stakeholder update ARP 4754A/ED 79A, ARP 4761/ED and ARP 5150	SAE S18/ EUROCAE WG 63	5.2
2.3 Safety standard continuous improvement	In IR / AMC / GM deliverables from RMT 469/470 WG implement a process for a continuous safety standard improvement loop based on lessons learned from in operation events	- RMT 469/470 WG SAE S18/ EUROCAE WG 63	5.3

2.4 future risk consideration	In IR / AMC / GM deliverables from RMT 469/470 WG and in ARP 5150 implement a process for future risks identification and mitigation	RMT 469/470 WG SAE S18/ EUROCAE WG 63	5.4
2.5 Precursor automatic capture/coding	In IR / AMC / GM deliverables from RMT 469/470 WG and in ARP 5150 promote a process for automatic detection and capture/coding of the precursor events when they occurs	RMT 469/470 WG SAE S18/ EUROCAE WG 63	6
3- Safety management at TAS (inter-stakeholder) level			
3.1 Safety management at TAS (inter-stakeholder) level l	In IR / AMC / GM deliverables from RMT 469/470 WG implement a safety management group to: - Enforce the activities and processes recommended in action item 1.1 to 2.5 in this table - Assure and Coordinate development of CATS Event Sequence Diagrams at TAS level (CATS ESD) - Coordinate stakeholder safety activities - Integrate stakeholder safety activities at TAS level - Manage relations with certification and operational authorities and with ICAO	RMT 469/470 WG	7

Table 4 Action List