SEVENTH FRAMEWORK PROGRAMME

WP3 Final Report
Safety Risk Management

S. Bravo Muñoz, J.P. Heckmann (APSYS), J.P. Magny (JPM), A.L.C. Roelen, L. Speijker (NLR), H. Udluft (TU Delft), M. Sanchez Cidoncha (Isdefe), B. Dziugiel (IoA)

ASCOS
safety certification

This document provides the Final Report for Work Package 3 “Safety Risk Management” of the EC Project ASCOS (Aviation Safety and Certification of new Operations and Systems).

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

Grant Agreement No.	314299
Document Identification	D3.6
Status	Approved
Version	1.2
Date of Issue	31-08-2014
Classification	Public

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	S. Bravo Muñoz	24/06/2014	All	Version for approval by PMT
1.1	L.J.P. Speijker	20/08/2014		Update by ASCOS coordinator
1.2	L.J.P. Speijker	31/08/2014		PMT comments processed

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	R. Wever, J.J. Scholte	10/06/2014
TU Delft	R. Curran	10/06/2014
Isdefe	M.M. Sanchez	10/06/2014
Thales Air Systems	B. Pauly	10/06/2014
CAAi	T. Longhurst	10/06/2014
Deep Blue	L. Save	10/06/2014
Institute of Aviation	A. Iwaniuk, K. Piwek	10/06/2014
APSYS	J.F. Delaigue, Jean Pierre Heckmann	10/06/2014
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	24/06/2014
NLR	L.J.P. Speijker	31/08/2014

Document Distribution

Organisation	Names
European Commission	M. Kyriakopoulos
NLR	L. Speijker, A. Rutten, M.A. Piers, P. van der Geest, A. Roelen, J.J Scholte, J. Verstraeten, A.D. Balk, E. van de Sluis, M. Stuip
Thales Air Systems GmbH	G. Schichtel, J.-M. Kraus
Thales Air Systems SA	B. Pauly
Airbus Defence and Space APSYS	S. Bravo Muñoz, J.P. Heckmann, M. Feuvrier
Civil Aviation Authority UK	S. Long, A. Eaton, T. Longhurst
ISDEFE	M. Martin Sanchez, I. Etxebarria, M. Sánchez
CertiFlyer	G. Temme, M. Heiligers
Avanssa	N. Aghdassi
Ebeni	A. Simpson, J. Denness, S. Bull
Deep Blue	L. Save, 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
ACFT	Aircraft
AMC	Acceptable Means of Compliance
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AoC	Area of Change
ARP	Aerospace Recommended Practice
ASRS	Aviation Safety Reporting System
A-SMGCS	(Advanced-Surface Movement Guidance and Control System
ASPA-IM-S&M	Airborne Spacing – Interval Management - Sequencing & Merging
ATSAW-ITP	Airborne Traffic Situation Awareness - In-trail procedure
ASCOS	Aviation Safety and Certification of new Operations and Systems
ATC	Air Traffic Control
ATM	Air Traffic Management
ATM-NEMMO	ATM Network MacroMOdel
CAST	Commercial Aviation Safety Team
CATS	Causal model for Air Transport Safety
EASA	European Aviation Safety Agency
ESARR	EUROCONTROL Safety Regulatory Requirements
EHAM	Amsterdam Schiphol Airport
E-OCVM	European Operational Concept Validation Methodology
ESD	Event Sequence Diagram
ESSI	European Strategic Safety Initiative
FAA	Federal Aviation Administration
FAST	Future Aviation Safety Team
FCL	Flight Crew Licence
FDM	Flight Data Monitoring
FHA	Functional Hazard Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FOQA	Flight Operations Quality Assurance

FT	Fault Tree
HAZOP	HAZard and OPerability study
HTRR	Hazard Tracking & Risk Resolution
IFPS	Integrated Initial Flight Plan Processing System
JPM	Jean-Pierre Magny
LCC	LCC (Life Cycle Costs)
LEMD	Madrid Barajas Airport
LLR	Lessons Learned Requirements
MRO	Maintenance Repair Overhaul
NLR	National Aerospace Laboratory of the Netherlands
PDARS	Performance Data Analysis and Reporting System
PI	Performance Indicator
PIC	Pilot In Command
QAR	Quick Access Recorder
ROI	Risk Opportunities Issues
SAM	Safety Assessment Methodology
SADT	Structure Analysis and Design Technique
SB	Service Bulletin
SMS	Safety Management System
SRC	Safety Regulation Committee
SESAR	Single European Sky ATM Research
SWIM	System Wide Information Management
TCAS	Traffic Collision Avoidance System
TO	Take Off
TOPAZ	Traffic Organization and Perturbation Analyzer
TOWS	Take Off Warning System
TSB	Transportation Safety Board

This page is intentionally left blank

Executive Summary

The main goal is to develop a total aviation system safety assessment methodology, with supporting safety based design systems and tools, for handling of current, emerging and future risks. This safety assessment needs, not only to address the new risks, but to be adapted to the whole Total Aviation System. This goal can be divided into two main objectives, a successful identification of risks prior to the accident and the creation of a safety methodology seamless for all TAS stakeholders.

The first objective is to develop a process of future risk identification that could be usable by all TAS stakeholders. It is proposed that CATS model can represent all major aviation safety risks. The base elements of CATS model can be linked to precursors that enable the safety practitioner to identify the emerging and future risk. It is possible as well to create safety requirements and safety objectives for certification purposes related to novelties. WP 3 creates a software tool that can be used for this purpose; the safety analysis can as well be enlarged with the impact on the performance network by combining the tool ATM-NEMMO with the CATS diagrams. In this way it is possible to have an overview of the safety impact of the introduction of a novelty in the TAS.

A second objective for WP 3 is to propose the safety methodology common to all TAS stakeholders that could take benefit from the identification of emerging and future risks. The process starts with the identification of the standards to apply for system development and system assessment in operation. The safety studies supporting these standards are fed with the precursor identification. (During development an in operation) It ends up with a feedback loop to improve these standards using a continuous improvement process from lessons learned from operation.

This page is intentionally left blank

Table of Contents

List of Figures

List of Tables

1 *Introduction and background*

1.1 Background and scope

The aviation world has rapidly developed since the age on when a single pilot could cross the skies with the simple support of clock, a compass and a radio. Nowadays the air traffic is a service supported by several stakeholders, e.g airlines, ANSP and aircraft constructors, and each of them has a particular role and consequently a particular impact on safety. No matter how different these stakeholders may be, they focus on the same final objective, to ensure an efficient and safe air traffic service. Besides the complexity of the aviation network, the XXI century seems to bring new challenges in terms of human aspects (e.g. a widespread of the aviation outside the western world) and in terms of technological improvements (e.g. higher level of automation in aircraft), and thus aviation stakeholders will become more interrelated and the safety will become a seamless objective share commonly by all stakeholders.

ASCOS WP1 addresses this complex world by proposing a complex question: Is the current regulatory framework adapted to the future changes in the aviation world? The answer is that the current framework needs being modified. WP 1.3 concludes that, as there is not a single certification approach that can be applied universally within the TAS, it is recommendable "*to use a logical argument for the certification of any change to the TAS and supporting the overall top level claim that the change is acceptably safe claim that the change is acceptably safe. The argument is decomposed into supporting claims until the claims can be directly"* supported by current standards." *Where existing standards are insufficient, this will support the definition of new specifications to support the introduction of novel technology or concept"* [12]. ASCOS WP1 proposes a new certification approach, which consists of the following stages:

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

The success of this approach depends, among other factors, on a sound understanding on how safety is implemented among stakeholders and how engineering and associated safety analysis are performed in a coordinated way with due consideration of emerging and future risks and of all interactions between systems. WP2 is focused on developing a methodology for a Continuous Safety Monitoring for all stakeholders. This methodology is based on the use of Safety Performance Indicators that are monitored and compared with a previous baseline risk picture. WP2 proposed as well CATS as an effective tool to support this process.

With the support of the WP2 and keeping in mind the certification approach proposed in the WP1, the WP3 can address its objective; to define a total aviation system safety assessment methodology and implementation conditions for handling of current, emerging and future risks supported by safety based design systems and tools.

1.2 Objectives

The main goal of WP 3 is to create a total aviation system safety assessment methodology that enables the stakeholders of the TAS to analyze the safety a whole and to handle the current, emerging and future risks in such a way that could be used in the certification process. WP 3 is divided into five work packages with specific objectives for each of them:

WP 3.1 Aviation Safety Methodology: The WP 3.1 objective is to summarize the existing know-how in the risk identification and to develop an advanced process for the identification of precursors that could be used to foresee the safety issues driven by the introduction of novelties in the Total Aviation System. WP 3.1 recommends as well several areas of improvement for a global safety methodology and its implementation within the Aviation Total System.

WP 3.2 Risk models and Accident Scenarios: The objective of WP 3.2 is to create an approach to risk modeling from the CATS model that could represent the precursors related to the future and emerging risk identified in WP 3.1. WP 3.2 creates accident scenarios in the form of Event Sequence Diagrams in combination with Fault Trees.

WP 3.3 Tool for risk assessment: The objective of WP 3.3 is to develop a software tool that embodies the risk models developed in WP 3.2. WP 3.3 enables the safety practitioner to create safety objectives and safety requirements for certification purposes.

WP 3.4 Tool for Overall Safety Impact: The objective of WP 3.4 is to assess the safety impact of introducing new safety enhancement systems and/or operations in the total aviation system. WP 3.4 addresses the interaction of the performance network (capacity, predictability, etc) with the safety risk model developed in WP 3.2.

WP 3.5 Total Aviation Safety System Standards: The objective of WP 3.5 is to answer to the areas of improvement identified in WP3.1 by proposing a system safety assessment methodology and improvements on the safety standards in order to address the total aviation systems. This total aviation system safety assessment methodology and safety standards improvements methodology uses the inputs from previous packages in WP 3, WP3.5 takes on board the precursors identification process developed in WP3.2 and the tools WP3.3 §WP3.4. . The WP 3.5 deliverable proposes a Total Aviation System common safety standard framework for product development and for product follow up in operation. It establishes a comprehensive and logical process to improve the total aviation system safety standards with a continuous feedback considering experience in operations. These improved aviation system safety standards can answers the claims stated in D1.3.

1.3 Approach and methodology

The WP 3 can be summarized as follows:

WP 3.1 considers the major concerns identified in WP 1.1 [8]. The WP1.1 presents an identification of shortcomings and bottlenecks in the current regulations and certification processes. It leads to recommend to analyze the existing European certification and rulemaking processes and:

- To analyze the issue of lack of clear accountability for regulated entities in current certification and rulemaking processes;
- To analyze the issue of inappropriate actual requirements due to technological changes and emerging risks; can we identify inappropriate actual requirements?

The second concern expressed by WP1.1 is taken on board of WP 3.1 which proposes a process to perform safety assessment on emerging and future risk.

WP 3.1 performs a synthesis of existing know how on (predictive) risk identification conducted through literature research and feedback from safety research panels or advisory groups. Experience gained with the FAST, ESSI, and its connection with the Commercial Aviation Safety Team (CAST) provides a fundamental basis for defining conditions for implementation of a methodology suitable to deal with the Total Aviation System.

As a result, WP 3.1:

- Establishes an advanced process for the identification of precursors of (emerging) risks.
- Develops of a list of emerging risks, and sets up a system for continuously updating this list. This sub-task is mainly based on work done within the FAST team.
- Proposes specifications for a safety assessment methodology and certification practices that includes assessment of emerging risks and fully integrated within standard program management rules applicable to any project.
- Issue recommendations for a seamless application of methods within all aviation domains (Total System) with particular emphasis to increasingly interfaced aviation systems such ground and airborne systems
- Establishes a bridge with WP6.2 & WP6.4 presentation of return on investment of proposed methods.

The objective of **WP 3.2** is to create a risk model that is able to identify the unique sequence of event that may result in hazards (precursors). WP 3.2 starts from the existing model of CATS and incorporates the concepts of precursors and emerging/future risk developed in WP3.1 and the experienced gained in FAST to build a predictive risk model for the Total Aviation System. WP3.2 concludes explicit safety culture and safety management representation in the model is currently not possible, and proposes to represent these aspects by modification factors applied to the base events of the risk model.

Actual quantification of the ASCOS risk model is done in WP 2.2 [11] and when the risk model is being applied in the case studies (WP 4). The ASCOS risk model can be used to integrate information on all available safety performance indicators (developed in WP 2.1 [9]) into a single risk picture. Alternatively, the individual ASCOS risk model elements can potentially be used as safety performance indicators.

WP 3.3 develops a software tool that embodies the risk models and representations of the accident scenarios as developed in WP3.2. The tool enables the safety practitioner to represent a scenario that comprises the whole aviation system. The safety practitioner can modify this scenario to represent the safety impact of the introduction of a novelty. It is possible to identify the precursors and the safety barriers, and to obtain quantitative safety objectives and safety requirements.

WP 3.4 proposes a tool, ATM-NEMMO, which models the performance of a traffic network. In order to do this WP3.4 introduces the concept of safety performance indicators (as it is presented in D2.1 [9]) The safety practitioner can model the impact of any novelty in terms of global performance and to identify the potential areas of safety impact. These outputs, in terms of incorporating ATM network performance related factors, are introduced in the risk model tool developed in WP 3.3. In this way the risk model is refined and the estimation of safety risks considers as well the global networks effects.

WP 3.5 (Starting from the results of ASCOS WP3.1 and WP 3.2) proposes a Total Aviation System common safety standard framework for product development and product follow up in operation. In this sense the safety standard proposed are used to support the claims of the Certification Approach proposed by D1.3 [12]. It establishes a comprehensive and logical process to improve the total aviation system safety standards with a continuous feedback considering experience in operations, following the approach described in D3.2. The ASCOS WP3.5 results are compliant with the ICAO Safety Management Manual (SMM)[18] recommendations and with international safety recommended practices from SAE and EUROCAE organizations.

1.4 Structure of the document

This document is divided into seven sections:

- Chapter 1 presents an overview of the document.
- Chapter 2 presents the WP 3.1: Aviation Safety Assessment Methodology.
- Chapter 3 presents the WP 3.2 : Risks Models and Accidents Scenarios.
- Chapter 4 presents the WP 3.3: Tool for Risk Assessment.
- Chapter 5 presents the WP 3.4: Tool for Overall Safety Impact.
- Chapter 6 presents the WP 3.5: Total Aviation System Safety Standards.
- Chapter 7 presents the conclusion of WP 3.

2 *Aviation Safety Assessment Methodology*

2.1 Introduction and objectives

The Flightpath 2050 Vision for Aviation specifically aims for a holistic, total system approach to aviation safety, integrated across all components and stakeholders. This will be supported by new safety management, safety assurance and certification techniques that account for all system developments. There is a need for new safety based design systems and supporting tools that address the total aviation system, while being able to anticipate on future and emerging risks that may exist in a future aviation system that will differ from today's aviation system. A new approach towards certification – that considers the impact on safety of all elements of the aviation system and the entire system life-cycle in a complete and integrated way – will be beneficial for further safety improvement. An improved safety assessment method, which deals with the total aviation system, could provide the means to deal better with these changes in aviation and the associated needs.

Within aviation, a wide variety of safety assessment methods is available. There are many similarities and redundancies but often these methods are focusing on one specific domain or on one specific part of the life-cycle of an operation system. From a safety and cost benefit perspective, it will be a significant advantage if safety methods (and supporting tools) can be used in the different domains, are able to address changes all along program's life cycle, from early design phases to operations, and support continuous safety monitoring, while being fully coordinated within management activities. The specific objectives of the WP3.1 study are:

- To perform a synthesis of existing know how on (predictive) risk identification methods;
- To develop an advanced process for the identification of precursors of (emerging) risks;
- To develop a list of emerging risks, and propose a procedure for continuously updating this list;
- To support the ASCOS proposed certification approach with appropriate safety methods.
- To analyse Total System implementation constraints and issue recommendations accordingly.

First, the needs and selection criteria for a total aviation system safety assessment methodology will be defined. Promising (already existing) safety methods – that may be used as building blocks – will be identified. The initial idea is to combine the Future Aviation Safety Team (FAST) methodology (endorsed by EASA as FAST/EME1.1 methodology) with the quantitative safety method used in the Causal model for Air Transport Safety (CATS), which covers all possible types of accidents in the total aviation system. FAST developed an approach to discovering aviation futures which uses the concept of 'Areas of Change', considering that the future may produce unanticipated hazards. FAST is able to provide risks pictures of the future to all program phases to any safety, engineering and program actor in all aviation systems and at the end to certification. However, improvements and more detailed guidance material for these safety methods may be necessary, when needs and criteria are better defined. Therefore, other key safety methods will also be considered. Next, existing methods for detection of precursors of risks will be evaluated and an improved process for identification of precursors for future and emerging risks will be defined. This is followed by updating an existing repository of "Areas of Change", which was developed by the FAST, and which enables the identification of emerging risks and associated hazards. A process for continuous updating of the repository of "Areas of Change" and a list of emerging risks is proposed. Finally, recommendations and guidance is provided.

2.2 Terminology

A "**current/known risk**" is defined by its severity and the current/known likelihood of its components (failures, errors represented by fault trees) accepted in the certification process.

An "**emerging risk**" is defined as a familiar risk that is increasing or a new risk that becomes apparent in new or unfamiliar conditions.

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).

2.3 Summary Results

A summary of the needs of a Total Aviation System (TAS) safety assessment methodology is provided in Table 1. These needs also aim to serve as criteria for selecting appropriate methods for the methodology. The needs have been identified by reviewing sources on candidate needs and inputs from the ASCOS partners and by consecutive consolidation. Each need is described in more detail in ASCOS D3.1 [1].

Table 1 Overview of needs

Overview of needs	
A.	The methodology has to address the Total Aviation System (TAS) and to provide the means to address all the interfaces and the interactions between the different aviation system domains
B.	The methodology should make use of more integrated supporting tools for safety assessment
C.	The methodology has to address current and future risks
D.	The methodology has to be appropriate for supporting the certification process developed in WP1
E.	The methodology has to address all lifecycle phases
F.	The methodology has to be appropriate for developing safety assessments of good quality
G.	The methodology has to make use of inputs from experts with appropriate qualifications
H.	The methodology should adopt stakeholders' wishes

Safety assessment methods have been developed over a number of years in a variety of different branches of industry. There is an enormous variety of risk assessment conceptual frameworks, methodologies, and methodologies catalogues. Three catalogues of safety methods that exist are:

- Safety assessment methods database [19]. This document gives an overview of about 800 techniques, methods, databases, and/or models that can be used during a Safety Assessment. Besides a summary of the aim, description, domain (e.g. nuclear, chemical, air traffic management, aviation, aircraft development, computer processes), application (i.e. applicable to hardware, software, human, procedures, or to organisation) of the method, it describes for which safety assessment stage (i.e. scope the assessment, learning the nominal operation, identify hazards, combine hazards into risk framework, evaluate risk, identify potential mitigating measure to reduce risk, safety monitoring and verification, and/or learning from safety feedback) a particular safety method could be used.
- ATM safety techniques and toolbox [20]. This document comprises 27 techniques that can be used to evaluate and improve safety in ATM. It outlines a simplified eight-stage safety assessment approach and then provides details about the safety assessment techniques. It explains where the technique comes

from, its maturity and life cycle stage applicability, the process and data requirements, and practical and theoretical advantages and disadvantages. The overall approach biased towards concept design and development, but most of the techniques can also be applied to existing systems.

- Guide to methods and tools for airline flight safety analysis [21]. This document provides summaries of 57 methods and tools that can be used to analyse flight safety data including event reports and digital flight data. These methods and tools are organized into three areas: flight safety event reporting and analysis systems, flight data monitoring analysis tools, and specific purpose analytical tools.

In response to a request from EASA, Future Aviation Safety Team (FAST) conducted a review of safety risk analysis methods, in order to devise a methodology to assess (as well as anticipating and mitigating) future risks. Criteria to rate about 30 identified applicable methods, according to its ability to provide insight into the future hazard/risk identification objectives, have been developed and applied. The resulting FAST/EME1.1 method, which describes a proposed process of carrying out a future risk assessment, is initially targeted at commercial entities and governmental organizations. Nevertheless, application to newly proposed changes (e.g. operations, systems, products, processes) in the aviation system seems also possible. The FAST method is built on three critical elements: a credible depiction of the future, a description of scenarios that will result in a number of hazards by looking forward in time, and a set of tools to execute the risk analysis that will produce credible results (while using e.g. credible data, addressing human factors influences).

The FAST Method is aimed at identifying future hazards that have not yet appeared because the changes within the aviation system that may produce these hazards have not yet taken place. The method process flow consists of 12 steps; 1) Be responsible for implementation of global aviation system changes; recognize your need for systematic prediction of hazards associated with changes and to design those hazards out of the system or avoid or mitigate the hazard; 2) Clearly define scope of expert team study; 3) Assemble an expert team; 4), 5) and 6) Communicate with FAST and Customer to understand the complete task; to understand pertinent Areas of Change (AoC); to determine key interactions; 7) Refine the visions of the future; 8) Compile the hazards; 9) Determine the watch items; 10) Compile recommendations; 11) Inform FAST regarding results; 12) Inform customers regarding results. The FAST method introduces safety assessment of a scoped future system in its future context, using a scenario-based approach and enriched safety assessment methodology.

Examples of accident sequence models are the Integrated Risk Picture (IRP) of Eurocontrol and the Causal Model for Air Transport Safety (CATS) of the Dutch Civil Aviation Authority. These models are based on phenomenological knowledge and operational experience and are quantified with operational performance data and expert judgment. Event sequence models like IRP and CATS can be used to integrate information on all available safety performance indicators into a single risk picture, are predominantly constructed of active failure events, and do not contain many latent failure events. The fact that accident sequence models are mainly quantified from (past) operational data means that event sequence models are a source of lagging indicators as they capture failure results from a past time period and characterize historical performance.

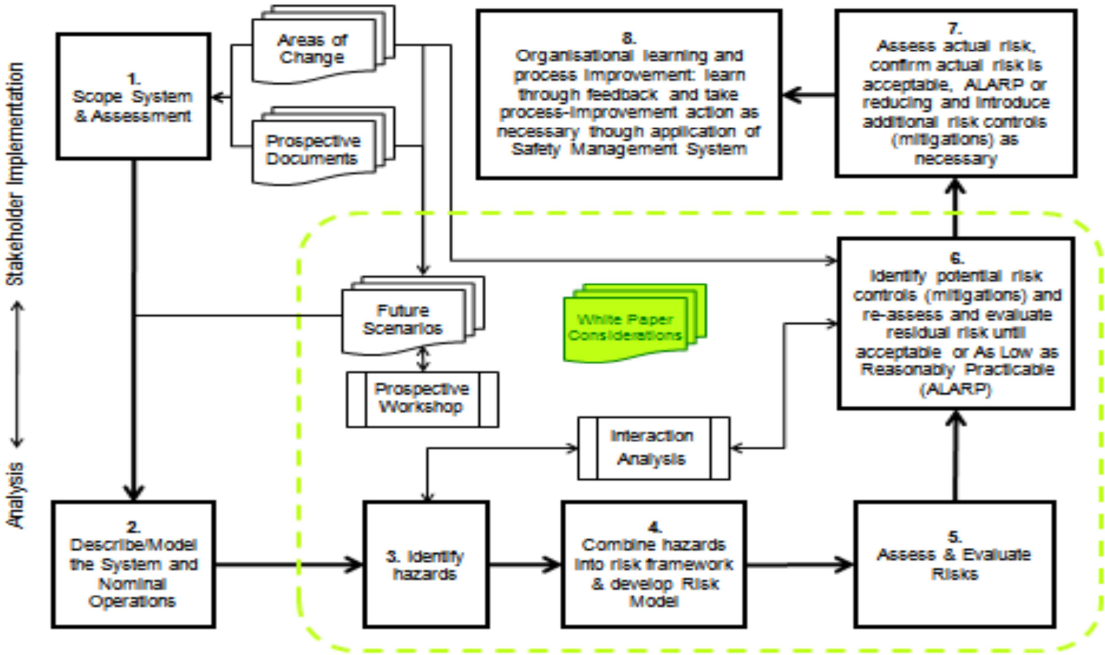
Stakeholder Implementation
Analysis
1. Scope System & Assessment
Areas of Change
Prospective Documents
8. Organisational learning and process improvement: learn through feedback and take process-improvement action as necessary though application of Safety Management System
7. Assess actual risk, confirm actual risk is acceptable, ALARP or reducing and introduce additional risk controls (mitigations) as necessary
Future Scenarios
White Paper Considerations
6. Identify potential risk controls (mitigations) and re-assess and evaluate residual risk until acceptable or As Low as Reasonably Practicable (ALARP)
Prospective Workshop
Interaction Analysis
2. Describe/Model the System and Nominal Operations
3. Identify hazards
4. Combine hazards into risk framework & develop Risk Model
5. Assess & Evaluate Risks

Figure 1 Future Aviation Safety Team (FAST) methodology

A combination of safety methods and tools will likely be necessary is necessary to meet the identified key needs. The idea is to combine the FAST methodology with the quantitative safety method used in the CATS, which covers all possible types of accidents in the total aviation system. The approach is to bring this approach to a next level by considering the concept of 'areas of change' in a certification framework. FAST is able to provide risks pictures of the future to all program phases to any safety, engineering and program actor in all aviation systems and at the end to certification. Therefore, a logical step forward is to investigate if and how the FAST and CATS methods may be incorporate into safety standards developed by EUROCAE/SAE.

The Future Aviation Safety Team (FAST) methodology, endorsed by EASA under EASp Action EME 1.1, has identified and maintains a repository of Areas of Change (AoC). It should be noted that:

- FAST provides a Risk Picture of the future to **all actors** during the entire life cycle
- The present list of emerging risks presented comes out of FAST
- The AoC list provides indications where to searching for precursors (launch a survey confirming where are precursors and measure how severe and spread out is the hazard.
- The corresponding risk picture taken of in most engineering and safety activities concerns design justification of systems robustness to new risks therefore certification demonstrations.
- It is possible to enrich the analysis and efficacy of risk control measures taken by answering the question: "Will the safety enhancement resist to emerging risks?"

Within ASCOS, adaptations to the existing list of FAST AoCs have been made. This was deemed necessary to remove inconsistencies. A cross reference table that indicates how the AOCs are affecting the different domains of the aviation system has been developed as well. The full details are contained in reference [1].

2.4 Conclusions and Recommendations

The ASCOS methodology study:

- Has defined the conditions (needs and criteria) for implementation of a safety assessment methodology suitable to deal with the total aviation system and the entire life-cycle. This definition includes the means to address all the interfaces and interactions between the different domains and associated safety assessment processes, presented here as a total system approach.
- Performed a synthesis of existing know how on predictive risk identification and confirmed the added value of the FAST/EME1.1 methodology as an augmentation process of existing methods.
- Developed an advanced process for the identification of precursors of (emerging) risks
- Developed a list of emerging risks, and proposed a procedure for continuously updating this list;
- Proposes introduction of additional program management recommendations into standards intending to ensure implementation of recommended methods,

Risk and safety management shall be a seamless process throughout programs' life cycle within and between all aviation domains. Rather than developing a new method from scratch, existing methods are evaluated in order to identify promising (combination of) methods that meet the above requirements and can be embedded in a certification scheme tied up to engineering safety analysis. This justifies selection of:

- Causal Model of Air Transport Safety (CATS), promoting the prevention of aircraft accidents through better understanding of aviation risks in terms of causes and magnitude.
- Future Aviation Safety Team (FAST) methodology (FAST/EME1.1), permitting to identify and take care of future and emerging risks.
- Program management dispositions, without which it may be difficult to follow a total system approach and systematically apply safety analysis, risks mitigations and proper decision making.

The following key recommendations are given:

- A total aviation system approach, as followed in the Causal model for Air Transport Safety (CATS), with its capacity to bring a better perception of all possible accident and accident avoidance scenarios is showing benefits and is recommended to be integrated within safety methods and processes.
- Safety methods should be an explicit part of the early phases of program management and promoted accordingly, so as to devote more safety effort in early program phases, in combination with engineering and certification, the latter considered as direct product from design justifications.
- Identifying precursors and emerging risks is important in safety assessment processes. Precursors detection methods are recommended to become part of a standard or, at least, a handbook.
- Precursors' detection and organization dispositions should be part of Integrated Logistics Support (ILS) dispositions as defined at program's level.
- Improved detection of precursors can play a role in enhancing continuous safety monitoring activities.
- Promote the creation and/or updates of standards towards a total aviation system safety approach.
- Encourage participation to the SAE and/or EUROCAE Working Groups, permitting to upgrade the relevant SAE/EUROCAE standards accordingly with the methods and tools developed in ASCOS.
- Provides material for the WP6 demonstration of the important ROI (Return On Investment).

3 Risks Models and Accidents Scenarios

3.1 Introduction and objectives

The current state of the art for the certification of aeronautical products is basically reactive in the sense that changes in certification requirements are often made as a reaction to major accidents or as a reaction to technological advances. A key step in the proposed improved certification process (which is the main overall objective of ASCOS) is an improved hazard identification process, including a 'predictive' approach, aimed at discovering future hazards that could result as a consequence of future changes inside or outside the global aviation system and then initiating mitigating actions before the hazard is introduced.

This is to be achieved by representing current and future risks in accident and accident avoidance scenarios in such a way that it can be used in the certification process. The objective is to provide an integrated approach to risk modelling in which human factors and cultural aspects are considered in connection with technical and procedural aspects and with specific emphasis on the representation of emerging and future risks.

The work comprises the following:

- Representation of safety of the current aviation system in accident scenarios.
- Representation of emerging and future risks in accident scenarios.
- Representation of safety culture and safety management in accident scenarios.
- Quantification of accident scenarios.

The current state of the art in aviation system wide risk modelling and tools is provided by the EUROCONTROL Integrated Risk Picture (IRP), SESAR Accident/Incident Model, FAA's Integrated Safety Assessment Model (ISAM), and the Dutch Causal Model for Air Transport System (CATS), which all have a comparable structure. Aviation accidents are represented as event sequences with different possible causal factors. The CATS model approached this complexity by developing 33 separate accident scenarios for each accident category in commercial air transport. These scenarios are represented as Event Sequence Diagrams (ESDs) and Fault Trees (FTs). The FTs provide a logical structure showing how causal factors could combine to cause an event of the ESD. The ESD shows how combinations of these events may result in an accident. The IRP and AIM and follow a similar approach, but with a focus on ATM. Using the AIM, a risk picture for SESAR is being developed to represent the combined effects of the set ATM changes that are expected to be in place by 2013, 2017 and 2020. ISAM is based on CATS and AIM and allows users to evaluate air traffic, airport and air vehicle systems and operators' individual and integrated impacts in the context of NextGen implementation. The ASCOS risk model study is based on the incident/accident risk model CATS, which represents the total aviation system.

To represent future and emerging risks, the WP3.2 study builds on work performed by the Future Aviation Safety Team (FAST), which developed an approach to discovering aviation futures using the concept of 'Areas of Change'. These possible futures might interact with the change under analysis, producing unanticipated hazards or rendering existing safety barriers less effective. Next step is to define precursors, i.e. identifiable events that may be used as indicators for hazards. These precursors will then be related to elements of the risk model. The representation and the evaluation of the emerging/future risks using CATS can be done if CATS model elements are linked to precursors and if a dedicated capture process is defined for these precursors.

3.2 Terminology

A “**Fault Tree (FT)**” is a graphical representation that uses Boolean operators to identify the chain of events leading to a specific fault or failure.

An “**Event Sequence Diagram (ESD)**” is a modelling tool for developing possible risk scenarios, enabling visualization of the logical and temporal sequence of causal factors leading to various states of the system.

A “**base-event**” is a failure, error or procedure deviation that can lead to an infringement of the safety barrier and to a specific fault in a fault tree.

An “**initiating event**” represents the start of the main accident scenario in a ESD. The initiating event also has causes that are represented in a fault tree.

A “**pivotal event**” is one the series of events leading to an accident in a ESD. It represents a possibility for the safety occurrence to develop into an accident, or a possibility that the accident is avoided.

3.3 Results Summary

Every historic accident, and every accident still to come, has a different sequence of events and a unique set of circumstances. To study accidents, and their prevention, it is paramount however that accident sequences are also described at a more generic level so that generic problems can be identified and solved. Therefore unique sequences of events must be categorized into distinctive scenarios that characterize a certain type of accident. A set of such generic scenarios form a model, and are a simplified representation of a complicated and unique reality. By carefully analysing historic accidents and describing the scenarios, this representation of reality can be made sufficiently detailed to give an adequate description of the total aviation system.

The approach in ASCOS is to base the risk model on the Causal Model for Air Transport Safety (CATS) that has been developed earlier by a consortium led by Delft University of Technology and funded by the Dutch government. The CATS model describes accident scenarios and accident avoidance scenarios as event sequence diagrams (ESDs) and fault trees. For the purpose of the ASCOS accident model some qualitative changes have been made to the CATS ESDs to incorporate the lessons-learnt of the last couple of years in which CATS has been used and studied. These changes include different naming of events, different definitions, addition or deletion of events, and combining of ESDs.

The event sequence diagrams provide a qualitative description of the accident scenarios. They can be quantified by assigning a probability of occurrence of each of the different pathways in the scenarios. These probabilities can be determined from past air safety data, from expert opinion or by calculation using other events in the models for which the probability is known. The preferred way to quantify events is by using historical safety data.

The ASCOS accident model includes a fault tree for each initiating event, and for most pivotal events. The ASCOS fault trees are based on the fault trees used in CATS. Again, lessons-learnt are applied to modify the fault trees to match the requirements of ASCOS. Furthermore, because there are differences between the

ASCOS ESDs and the CATS ESDs, there are ESD elements unique to ASCOS. For these elements new fault trees have been defined. Where possible element of existing CATS fault trees are used, or multiple CATS fault trees are combined. Modifications to CATS fault trees are mainly done to come to level of detail that is appropriate for ASCOS. The ASCOS risk model uses 29 accident and accident avoidance scenarios. Note that EASA's European Aviation Safety plan (EASp) identifies categories of operational (safety) issues of commercial air transport operations. The EASp operational issues of primary importance are runway excursions, mid-air collisions, controlled flight into terrain (CFIT), loss of control in flight (LOC-I), and ground collisions. Table 1 provides the initiating events for the ASCOS ESDs, and their relation with the EASp main operational issues.

Table 2: Initiating events of ASCOS accident model

		EASp category				
ESD	**Initiating event**	**Runway excursion**	**Mid air collision**	**CFIT**	**LOC-I**	**Ground collision**
1	Aircraft system failure during take-off	√				
2	ATC related event during take-off	√				
3	Aircraft directional control by flight crew inappropriate during take-off	√				
4	Aircraft directional control related system failure during take-off	√				
5	Incorrect configuration during take-off	√			√	
6	Aircraft takes off with contaminated wing				√	
8	Aircraft encounters wind shear after rotation				√	
9	Single engine failure during take-off	√				
10	Pitch control problem during take-off	√				
11	Fire, smoke, fumes onboard aircraft				√	
12	Flight crew member spatially disorientated				√	
13	Flight control system failure				√	
14	Flight crew incapacitation				√	
15	Ice accretion on aircraft in flight				√	
16	Airspeed, altitude or attitude display failure				√	
17	Aircraft encounters thunderstorm, turbulence, or wake vortex				√	
18	Single engine failure in flight				√	
19	Unstable approach	√			√	
21	Aircraft weight and balance outside limits during approach				√	
23	Aircraft encounters wind shear during approach or landing	√				
25	Aircraft handling by flight crew inappropriate during flare	√				
26	Aircraft handling by flight crew inappropriate during landing roll	√				
27	Aircraft directional control related systems failure during landing roll	√				

31	Aircraft are positioned on collision course in flight		√			
32	Runway incursion					√
33	Cracks in aircraft pressure cabin				√	
35	TAWS alert			√		
36	Conflict on taxiway or apron					√
38	Loss of control due to poor airmanship				√	

The representation and the evaluation of the emerging/future risks using CATS ESDs can be done if each base event of the fault tree is linked to precursors and if a dedicated capture process is defined for these precursors. 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 become hazardous is known to be significant.
- Events known yet, but for which risk to become hazardous may have been underestimated, neglected or even unidentified up till now, unless revealed by an actual occurrence of the hazard.

The application of the precursors capture process allows calculating the precursor occurrence rates and then the emerging/future risks by using CATS ESDs. For that it is necessary to ensure that the CATS ESDs are sufficiently complete. It is important to note that precursors should be related to base events of the risk model fault trees. If a precursor cannot be associated with an element of the model, the applicable part of the model should be reviewed and modified or extended to allow a connection between the precursor and the model. This means that all initiating events in the future situation are envisaged, all pivotal events are recognized, no safety barrier is forgotten and no base event in fault trees is overlooked. This can be done in two steps:

- Step 1: Using safety assessments and product description and operational documentation for identification of all safety barriers implemented in the design and ensuring that all these safety barriers are considered in CATS ESDs.

- Step 2: Reviewing the CATS ESDs with experienced people having different points of view (e.g. design, maintenance operation, pilots, flight operation, ground operation, airport operation, ATM operation) to assure completeness of safety barriers considered in CATS ESDs.

The essential elements that an organization should take into account to establish and maintain a Safety Culture are well described in literature. These elements provide a useful guidance to make a Safety Management System successful and effective in improving the safety record of an organization and in contributing, as an aggregated result, to the improvement of the safety performance of the entire aviation system. Plus they pave the way for the identification of Safety Culture indicators to be monitored at the level of individual organizations. However a number of reasons suggest avoiding the modelling of safety culture and safety management elements in accidents scenarios to be directly attached to the Event Sequence Diagrams and Fault Trees of the ASCOS risk model. The most important reasons are shortly summarized below.

- **The safety culture related failures are mainly negative conditions favouring long term and latent failures. While the Fault Trees are better suited for representing system failures and errors at the sharp end**. A positive Safety Culture may take time to be established in an organization and does not produce its effects immediately. On the other hand a failure to establish a Safety Culture also on specific aspects of the operations can remain silent for a long period and disclose its negative effect even after a long time from the initial program for its implementation. And it is worth noting that this is not limited to the occurrence of human errors. For example a piece of equipment may have been discovered to fail in very specific circumstances which occur rarely. However this defect may have gone unnoticed for a long time due to the weak Just Culture of the organization which discouraged the controller or pilot to report the inconvenience in which they were involved, even in case of minor incidents. In this way the information about the technical inconvenience may not reach the management of the organization, thus leading to a lack of any concrete preventive measure and to a potential for a serious threat to safety once the same or very similar circumstances will be reproduced. Therefore trying to set a frequency for a condition like this, with a potential for influencing the frequency of other fault tree events, appears quite arbitrary, due to the potential combination of too many elements in ways which are difficult to predict and very peculiar to the specific context of occurrence.

- **The same safety culture failure or safety management might simultaneously contribute to several FT basic events.** Another problem in linking potential safety culture failures and safety management failures to a fault tree based accident scenario lies in the difficulty to relate them to a specific failure event. As a matter of fact if an organization has a severe limitation in its Safety Culture, this may potentially have a simultaneous impact on a large set of fault tree events, acting as a sort of common cause for several failures. For example an inadequate Reporting Culture may cause more than one safety issue to become unnoticed or misunderstood, including both technical failures and human errors. However modelling the same Safety Culture factor as a unit influencing the frequency of all the events in the fault tree does not appear appropriate, since the same factor is unlike to have the same effect on all the elements of the fault tree. The different effects upon different fault tree elements will again depend on very peculiar circumstances and combinations of events which cannot be easily captured in a fault tree.

- **Safety Culture measurements appear more appropriate for the monitoring of trends within the same organization or for comparison between different organizations, rather than for the identification of absolute frequencies.** The intrinsic fuzziness of the concept make it difficult to measure the Safety Culture in a stable, standardized and ultimately reliable way. The same can be said for safety management. Assessments and measures may certainly result precious to monitor the trend of Safety Culture factors and safety management factors over time inside the same organization, as well as it may prove useful to compare with the same method the performance of two or more organizations in a limited time frame. Nonetheless the distortion and biases that can characterize the collection of data, as well as the difficulties in evaluating the actual role of Safety Culture and safety management in improving safety, suggest avoiding use of these measurements as absolute data from which it is appropriate to derive absolute frequencies of failures. Therefore the inclusion of Safety Culture elements and safety management elements into the generic accident scenarios appears of limited added value also for the difficulties that it would imply in terms of feeding the models with new data as soon as they arrive. While new data on specific incidents and safety occurrences categorized in a standard format are relatively easy to feed into the models, it would be questionable to use the result of Safety Culture and safety management investigations to update the same models.

Although representation of safety management and safety culture in accident scenarios is not practically possible, it is to some extent possible to quantify the effect of a certain level of safety management and safety culture on the existing elements of the accident model. This is done by deriving a modification factor that can be applied to a model element that is affected by the safety management and safety culture of a particular organization. The modification factor can be determined based on the level of maturity of a safety management system of an organization and on the level of safety culture. The methodology can be extended by specifically measuring the maturity level of the different pillars of safety management and the level of certain elements of safety culture. A different modification factor can then be applied to model elements that are affected by specific pillars of safety management and specific elements of safety culture. This method will rely heavily on expert opinion.

The modification factor alters the probability of occurrence of a certain element. The modification factor needs to be applied to the base elements of a fault tree; if the base events are altered, the complete model quantification will be adjusted as well. It is therefore necessary to determine per base event:

- Which type of organization (operator, MRO, ANSP etc.) affects the likelihood of this event?
- Which pillars of safety management affect the likelihood of this event?
- Which elements of safety culture affect the likelihood of this event?

The ASCOS accident model supports safety management in several ways. By describing a system or service in terms of where it resides in the model and in terms of its relationship to the safety related service one is able to share a common understanding of the service or system under consideration. The accident model can be used to improve the continuous oversight function by identifying a more complete and correct set of monitoring requirements by inspection of the complete model. Inspection of a complete accident model of the aviation system also has the potential to improve the identification of the boundary of influence of a proposed change and thereby improving the management of change. Inspection of a complete model of the total system behaviour has the potential to provide a clear understanding of the safety significance of a service, supporting service or system which one is then able to use in the determination of an appropriate level of oversight.

The ASCOS accident model supports the proposed certification approach (WP 1.3) in several ways. Describing the system or service in terms of where it resides in the model supports the definition of the change (step 1 of the certification approach). The prime use of the model is to calculate the safety effect of a proposed change, supporting the safety assessment (step 4 of the certification approach). Using the model also helps to identify a more complete and correct set of monitoring requirements in support of continuous oversight (stage 9 of the certification approach [12]).

3.4 Conclusion and recommendations

A key step in an improved certification process is a total aviation system risk model, supported by an improved hazard identification process, including a ‘predictive’ approach, aimed at discovering future hazards that could result as a consequence of future changes inside or outside the global aviation system and then initiating mitigating actions before the hazard is introduced. A predictive approach is supported by describing how emerging and future risks can be represented in a risk model. This ASCOS risk model is based on the Causal Model for Air Transport Safety (CATS). For the purpose of the ASCOS risk model some qualitative changes have been made to the CATS ESDs to incorporate the lessons-learned of the last couple of years in which CATS has been used and studied. The representation and the evaluation of the emerging/future risks using CATS ESDs can be done if each base event of the fault tree is linked to precursors and if a dedicated capture process is defined for these precursors. The efforts of the Future Aviation Safety Team (FAST) in identification and publication of Areas of Change (AoC) and associated hazards across aerospace is used as a suitable precursor capture process. The application of the precursors capture process allows calculating the precursors’ occurrence rates and then the emerging/future risks by using the ASCOS risk model. For that it is necessary to ensure that the ASCOS risk model is sufficiently complete. This means that all initiating events are envisaged, all pivotal events are recognized, no safety barrier is forgotten and no base event in fault trees is overlooked.

Quantifying the impact of safety management and safety culture on the level of safety of the total aviation system using an accident model is difficult. In fact, direct representation of safety culture and safety management in the risk model is not possible. It is recommended that for quantification of the influence of safety management or safety culture a modification factors is used that is applied to the base events of the risk model. The modification factor can be determined based on the level of maturity of a safety management system of an organization and on the level of safety culture. Quantification of the modification factors relies on expert opinion. It is recommended that a web based tool is used to support the elicitation and integrated on subject matter expertise regarding the magnitude of the modification factors. Using a web-based tool has the advantage that for the same level of effort more experts can be elicited that with traditional methods.

The ASCOS risk model supports safety management in several ways. By describing a system or service in terms of where it resides in the model and in terms of its relationship to the safety related service one is able to share a common understanding of the service or system under consideration. The risk model can be used to improve the continuous oversight function by identifying a more complete and correct set of monitoring requirements by inspection of the complete model. Inspection of a complete risk model of the aviation system also has the potential to improve the identification of the boundary of influence of a proposed change and thereby improving the management of change. Inspection of a complete model of the total system behaviour has the potential to provide a clear understanding of the safety significance of a service, supporting service or system which one is then able to use in the determination of an appropriate level of oversight.

4 *Tool for Risk Assessment*

4.1 Introduction and objectives

The objective of the WP3.3 study is the development of a software tool for risk assessment. The tool should embody the ASCOS risk models and representation of accident scenarios, which are based on CATS. The tool should allow the user to access, explore and modify the ASCOS risk models and accident scenarios. It should allow the user to utilize the safety risk method developed to support the new proposed certification approach.

The tool for risk assessment is a web-based software tool that can be used by a safety practitioner as support in the risk assessment process. It uses the Event Sequence Diagram (ESD) and Fault Tree logic to represent the total aviation system risk model that was developed in the WP3.2 study. The user can use the tool to explore the risk model developed in ASCOS and to assess the impact of modifications in the Total Aviation System in order to support the certification process. The tool is currently being validated within ASCOS WP5 Validation.

4.2 Terminology

The **model master** is the ‘baseline’ version of the risk model developed in ASCOS WP3.2. The user can use the tool to explore the Event Sequence Diagrams (ESD) and Fault Trees of the model master. The model master is also the reference version of the risk model that is used to perform analyses using the tool. Within the tool the model master is considered the current state of the total aviation system.

When performing an **analysis,** the tool is used to estimate the impact of changes to the model master. An analysis is performed for a specific case, e.g. the introduction of new technologies, operations or a system. To export the analysis, an output report can be generated that contains all modifications the user made to the model master. The report is presented in excel and in pdf.

By adding **modifications** the structure and values of the model master can be changed. A modification can be used to delete or change values of existing elements of the model master, as well as add new ESDs, ESD elements, Fault Trees and Fault Tree elements. The modification factors can be used to represent and quantify the effect of safety culture and safety management in the model, e.g. based on the level of maturity of a safety management system of an organization and on the level of safety culture (see Section 3.3).

The **modified model** combines the model master and modifications within an analysis. It is the resulting risk model after the modifications within an analysis are applied to the model master.

Associations are used to categorize and filter ESD and Fault Tree elements by precursor, risk-type, area of change (AoC), EASP category, stakeholder and safety-barrier. The user can create associations for all elements in the risk model. Associations can be used to i.e. monitor the impact of changes to user-defined safety-barriers, or to see all elements related to t a specific stakeholder.

4.3 Results Summary

The tool for risk assessment is a web-based tool. It requires a computer connected to the internet, with a web browser such as Internet Explorer, Safari or Mozilla Firefox. The software tool has been developed – and is maintained – by the TU Delft, based on a set of required functionalities established by NLR [6]. Initial testing was performed by APSYS, JRC and NLR, resulting in software updates. It should be noted that the tool is still being validated. User feedback and comments may still be processed until the end of ASCOS WP5 Validation. The current version of the tool, which is hosted on the NLR server, can be accessed through the URL:

http://www.ascos-project.eu/risk-tool

To get access and use the tool, an account and login data can be requested from the ASCOS coordinator.

The functionalities of the software tool necessary to meet the software requirements are defined in a software functional design. The functionality of the software tool is represented in a flow chart (See Figure 1). This flow chart depicts the different screens the user is presented with while using the software. Software requirements have been developed to meet the goals and required functionalities defined by the description of work, as well as user requirements. The detailed list of these functionalities, which are partly based on interactions with EASA in the context of an agreement to support the EASp (2014 – 2017), can be found in reference [6].

The tool is based on a database that can be administered centrally. It dynamically generates the graphical user interface and performs all calculations necessary to implement the ASCOS risk model. Any changes made by the administrator to the model master can immediately be accessed by the users, which make it an easy and convenient way to disseminate different, new or updated versions of the risk model.

An example realistic quantification of the ESDs and FTs is available in the current version of the risk model implemented in the tool. However, prior to any use of the tool, the user still needs to verify that the quantitative and qualitative model corresponds to the scenario that is going to be modeled and represented.

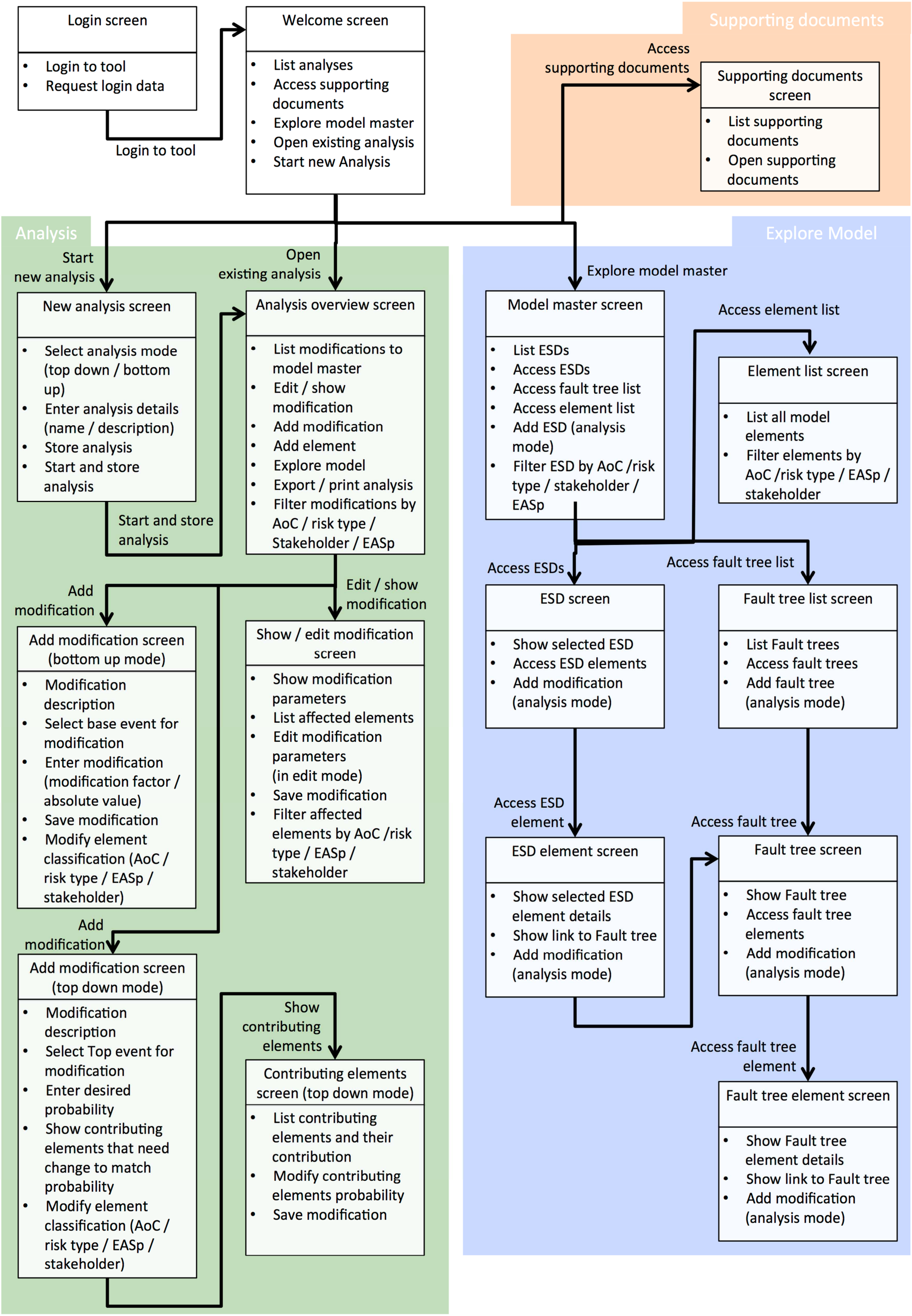
Login screen
Login to tool
Request login data
Login to tool
Welcome screen
List analyses
Access supporting documents
Explore model master
Open existing analysis
Start new Analysis
Supporting documents
Access supporting documents
Supporting documents screen
List supporting documents
Open supporting documents
Analysis
Start new analysis
Open existing analysis
New analysis screen
Select analysis mode (top down / bottom up)
Enter analysis details (name / description)
Store analysis
Start and store analysis
Start and store analysis
Analysis overview screen
List modifications to model master
Edit / show modification
Add modification
Add element
Explore model
Export / print analysis
Filter modifications by AoC / risk type / Stakeholder / EASp
Add modification
Edit / show modification
Add modification screen (bottom up mode)
Modification description
Select base event for modification
Enter modification (modification factor / absolute value)
Save modification
Modify element classification (AoC / risk type / EASp / stakeholder)
Show / edit modification screen
Show modification parameters
List affected elements
Edit modification parameters (in edit mode)
Save modification
Filter affected elements by AoC /risk type / EASp / stakeholder
Add modification
Add modification screen (top down mode)
Modification description
Select Top event for modification
Enter desired probability
Show contributing elements that need change to match probability
Modify element classification (AoC / risk type / EASp / stakeholder)
Show contributing elements
Contributing elements screen (top down mode)
List contributing elements and their contribution
Modify contributing elements probability
Save modification
Explore Model
Explore model master
Model master screen
List ESDs
Access ESDs
Access fault tree list
Access element list
Add ESD (analysis mode)
Filter ESD by AoC /risk type / stakeholder / EASp
Access element list
Element list screen
List all model elements
Filter elements by AoC /risk type / EASp / stakeholder
Access ESDs
Access fault tree list
ESD screen
Show selected ESD
Access ESD elements
Add modification (analysis mode)
Fault tree list screen
List Fault trees
Access fault trees
Add fault tree (analysis mode)
Access ESD element
Access fault tree
ESD element screen
Show selected ESD element details
Show link to Fault tree
Add modification (analysis mode)
Fault tree screen
Show Fault tree
Access fault tree elements
Add modification (analysis mode)
Access fault tree element
Fault tree element screen
Show Fault tree element details
Show link to Fault tree
Add modification (analysis mode)

Figure 2: Functional flow diagram of the tool for risk assessment

4.3.1 Main functionalities

a) Create safety risk picture for the current and future aviation system

The tool for risk assessment implements the risk model and accident scenarios developed within the ASCOS initiative. The tool provides a model-master that represents a risk model for the current total aviation system. A quantification of this risk model provides the current risk picture [11]. Within an analysis, the user can make modifications to the model-master and create new elements, fault trees and event sequence diagrams (see the other main functionalities described below), to develop a safety picture of the future. Therefore, the tool for risk assessment also enables the user to make an analysis to develop a safety picture of the future.

b) Support safety analysis for the certification process

The tool can perform analysis in two ways:

- First, the tool enables the user to quantify how much a certain novelty or existing product impacts the probability of the end states of the accident scenarios. The user can incorporate changes and make modifications to the risk model by adding, updating or removing base-events. The effects of these modifications propagate through the risk model, according to the methodology developed in the WP3.2 study, all the way to the end states of the accident scenarios in the related ESD.
- Secondly, the tool enables the user to impose a probability to the end states of the accident scenarios (safety objective) and to identify which elements should improve their failure rate in order to achieve this safety objective.

In this way the tool supports the process of creation of safety objectives and safety requirements. The user can as well create new elements in the ESD or FT in order to achieve certain safety objective; therefore, the tool can collaborate with the design process (see Section 6.3.3). This top-down type of analysis also enables the user to assess necessary changes resulting from desired (usually higher) safety performance levels.

c) Support analysis of future and emerging risk

The tool enables users to create and modify ESDs and FTs. The user can create future scenarios representing novelties in order to analyse the impact of such novelties in the Total Aviation System. The tool quantifies the modification of the end states of the accident scenarios probabilities and it identifies the emerging and future risks associated to a certain novelty. The results can be filtered by current/emerging or future risk.

d) Create Precursors and Safety barriers

In case precursors of base-events in the Fault Trees have been identified by aviation safety experts, the tool enables the user to link these precursors to base-events, and get an overview of all elements affected by a precursor, which can be used as an input to the certification process (See Section 6.3.5). The user can as well create safety barriers and quantify how much certain precursors impact certain safety barriers and if such impact is modified by the introduction of a novelty.

e) Represent safety culture and Safety Management

The tool enables the safety practitioner to create modification factors (as new elements) in order to represent and quantify to some extent the effect of safety culture and safety management on the elements in the risk model (see Section 0). It is assumed that the modification factor can be determined, by aviation safety experts, based on level of maturity of a safety management system of an organization and on level of safety culture. This method will rely heavily on expert opinion and therefore results should be handled carefully.

f) Classify and filter results by EASp; AoC and stakeholder

The tool enables the user to establish association of each element with the operational issues of the European Aviation Safety plan (EASp), AoC or stakeholder. The quantitative results can be filtered by these categories. Aall ESDs of the ASCOS risk model are associated to operational issues of the European Aviation Safety plan (EASp). These associations are implemented in the tool and the tool allows filtering of ESDs by EASp categories.

4.3.2 Development of possible picture of the future

EASp Action EME1.2 [13] seeks to develop a possible picture of the future by establishing a foresight cell. Such cell could be used at strategic level to evaluate how risks develop with time and identify the kind of expertise needed to be prepared to face the changes. An agreement has been reached by ASCOS with EASA to support the EASp with an initial test case using the FAST areas of change to develop a picture of the future [19]. Safety improvements efforts can be prioritized on the basis of foresight incorporating emerging and future risk [7]. The initial methodology consists of nine steps, which are summarized in Table 1 below. The main outputs are:

1. Prioritisation of EASp issues (and associated accident scenarios) for specified time frames
2. Prioritisation of the aviation domains that would require most effort within the specified time frames.

The tool for risk assessment supports the proposed methodology as described in Table 1.

Methodology steps	Functionalities provided by the current version of the tool
1. Determine, for each of the Areas of Change, the target year of actual implementation (time frame)	The estimation of realistic time of frame for AoC was performed by the FAST, with support of NLR. Results are available at http://www.nlr-atsi.nl/fast/aoc/. Four time frames are considered (ongoing, near term, mid term, and far term). The tool enables the user to create new ESD and Fault Tree or to delete existing ones, it is possible then, to associate a specific scenario to a certain time frame. During the process of development, the possibility of adding a functionality that enabled the user activate or deactivate certain elements of the model master depending on a potential associated time frame was considered. The idea was finally considered to be not feasible and not recommendable. However, it will in principe be possible in further developments to create such functionality.

Methodology steps	Functionalities provided by the current version of the tool
2. Correlate Areas of Change with applicable accident scenarios and associated EASp operational issues	The tool enable the user associate all ESDs of the ASCOS risk model to operational issues of the European Aviation Safety plan (EASp) and AoC. These associations are implemented in the tool and the tool allows filtering of ESDs by EASp categories and AoC.
3. Correlate hazards, associated with Areas of Change, with accident scenarios & EASp operational issues	The tool enables the user to relate each element to an specific AoC and EASp. The user can create scenarios associated to an AoC and quantify the impact of this AoC on an EASp category.
4. Assess for each hazard, associated with FAST Areas of Change, likelihood/severity of consequences	The user can develop the model and increase the level of detail of the fault trees and ESD in order to represent the hazards. The elements representing the hazards can be associated to an AoC. The tool can filter the results (quantitative results) per AoC.
5. Estimate increase or decrease of all accident scenario frequencies, relative to the baseline risk picture	The tool can provide the quantitative results in an excel sheet that compares the probability of the event before and after the introduction of a modification in the baseline scenario.
6. Determine future risk pictures for all accident scenario frequencies per flight	The tool enables the user to create future risk and to filter the quantitate results per EASp. The unit of the probability (per flight, per flight/hour…) depends on the units of the input.
7. Determine future risk pictures for the EASp issues (operational, systemic and/or emerging)	The tool enables the user to classify the elements per EASp domain, it is possible to develop the tool to enable the user to associate the elements to EASp issue; at this moment the tool can associate the elements to the concept: current, emerging or future.
8. Prioritize EASp issues related to future risk pictures (using highest estimated frequencies)	The tool itself cannot prioritize the EASp issues, however it is possible for a safety practitioner to model the future risk and use the output of the tool (increase/decrease of the end states of the accident scenarios probabilities) to prioritize EASp issues
9. Prioritize the aviation domains by identifying all the Areas of Change associated with the prioritized	The tool itself cannot prioritize the aviation domains. However it is possible for a safety practitioner to model the future risk and use the output of the tool (increase/decrease of the end states of the accident scenarios probabilities) to prioritize the AoC (the tool can filter per AoC and per stakeholder).

Table 3 Proposed Initial Methodology for using the ASCOS risk assessment tool for EASp EME 1.2

As a conclusion the tool can model accident scenarios and include the novelties at the level of detail defined by the user. The elements and the end states of the accident scenarios can be filtered by EASp and/or AoC. The tool cannot prioritize the EASp issues or aviation domain by itself (this is also not recommendable), but it can provide relevant quantitative information so that the safety practitioner can set up this prioritization.

4.4 Conclusion and recommendations

A tool for risk assessment was developed. The tool embodies the ASCOS risk model and representation of accident scenarios, which are based on CATS. The tool allows the user to access, explore and modify the ASCOS risk model and accident scenarios. It allows the user to utilize the safety risk method developed to support the new proposed certification approach. The tool for risk assessment is a web-based software tool that can be used by a safety practitioner as support in the risk assessment process. The tool is currently being validated within ASCOS WP5 Validation. User feedback and comments may still be processed for further improvements.

The software tool has now reached a stable prototype level. It supports the following functionalities:

a) Create safety risk picture for the current and future aviation system
b) Support safety analysis for the certification process
c) Support analysis of future and emerging risk
d) Create precursors and safety barriers
e) Represent safety culture and safety management
f) Classify and filter results by EASp; AoC and stakeholder

The tool for risk assessment supports an initial proposed methodology developed in the context of an agreement between ASCOS and the EASp Action EME1.2 [13], which seeks to develop a possible picture of the future by establishing a foresight cell. This would help to prioritize safety improvements efforts on the basis of foresight incorporating emerging and future risk. However, it should be noted that EASA and/or other CAA's have not yet tested or evaluated the current version of the tool. Follow-up activities in the ASCOS WP5 should dedicate some efforts towards evaluating the usability of the tool in the context of the EASp Action EME1.2.

For future work, it is recommended to seek opportunities to widen the scope of the tool for risk assessment. This could be achieved by opening up access to the tool for risk assessment to more users, and collect their feedback on which functionalities of the tool are useful to them and from which additional functionalities they could benefit. However, it should be noted that the ASCOS tool for risk assessment is recommended to be used only by aviation safety experts with sufficient and relevant aviation safety expertise and knowledge.

5 *Tool for Overall Safety Impact*

5.1 Introduction and objectives

The WP3.4 main objective is to detail how to perform an overall safety impact assessment of the total aviation system linked to the introduction of new **Safety Enhancement Systems and/or operations**.

The study builds on the assumption that the propagation and amplification of uncertainties throughout the air transport system has an impact on the safety performance of the system. The approach is therefore to study the **network delays and overloads** (indicators of amplification and propagation of uncertainties) linked to different Safety Enhancement Systems, and to estimate **their influence on the occurrence of safety issues at congested airports**.

Safety is a complex multi-dimensional subject. In non-domain specific definitions (e.g. ISO standards) 'safety' is considered as freedom from unacceptable risk, where risk is a combination of the probability of occurrence of harm and the severity of the harm. According to this definition, safety is subjective, depending on what the safety practitioner considers as "acceptable".

"*Safety also has a probabilistic aspect, and this is one of the reasons why it is a difficult subject to measure, since absence of harm does not necessarily indicate the absence of risk"* [9] In the ASCOS Safety Performance Indicator Framework [9], the safety performance concept for the aviation domain is described as "*the accident probability that is achieved in relation to the accident probability that is considered acceptable*". Therefore, aviation safety performance indicators should provide an indication of the probability of an accident.

The definition of an overall "safety level" has been also addressed in Air Traffic Management by. In the SESAR Safety Reference Material [10] to interpret "*the **x10 SESAR safety performance target***", the preferred metric for the safety level is the probability of accidents per encounter. Furthermore, the paper refers to specifying the safety level per type of airport (e.g. large, medium and small) and airspace (differing characteristics of En-route and TMA airspace). In conclusion, the overall "safety level" is understood as a probability of occurrence of certain specific safety events (accidents) across the different local-specific areas of the network.

The **overall safety level** is defined in the context of the WP3.4 study as an estimation of the safety performance of the air transport network and the probability that safety issues occur. This probability is influenced by several factors, and amongst them, by the network state in terms of presence of congestion (demand exceeding capacity and leading to overloads occurrence) and of network behaviour in terms of robustness (ability to hold back delay propagation) and resilience (ability to recover from states of generalised congestion with long delays spreading across several areas of the network). It is considered that degraded situations with high congestion and large delays with long recovery times have an impact on Air Traffic Management aspects, such as controller workload, that at their turn are factors used to assess the probability of occurrence of safety events in the pathway of incidents.

In the proposed approach, depicted in Figure 3, the combined use of a simulation tool of the European air transport system with a causal risk model is studied.

In particular, the simulation tool proposed is ATM-NEMMO, which is able to simulate the implementation of new systems/operations in the European Air Traffic Management (ATM) system, and to capture the associated impact on network performance (delays, overloads, etc.). The causal risk model for safety risk analysis corresponds to the CATS model, improved as part of ASCOS WP3 work, which is able to assess safety risk (in terms of accident probabilities) from the occurrence of hazards and failures of safety barriers.

In order to perform an overall (network-level) assessment of the impact of a specific new system or operation, this system/operation is first translated into a variation in the input parameters to the ATM-NEMMO model. The model output in the form of efficiency and predictability **performance indicators** is the input to a specific safety module, based on the CATS risk model, which is able to translate the ATM-NEMMO outputs to safety performance impact in two possible ways:

- Using network-wide average efficiency and predictability **performance indicators** as input to the safety module, obtaining overall safety impact results at the network level;
- Using local performance results as input to the safety module to identify areas of the network that are highly at risk.

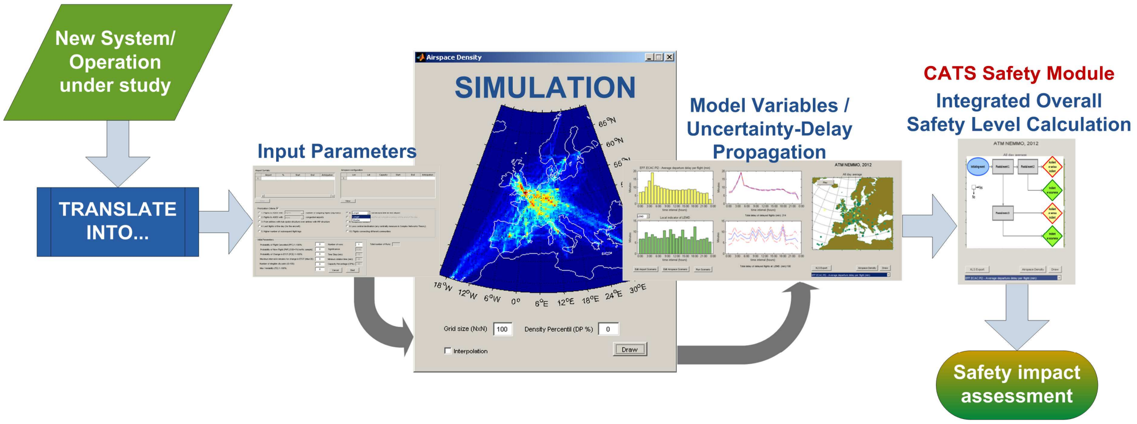
New System/ Operation under study
TRANSLATE INTO...
Input Parameters
Airspace Density
SIMULATION
66°N
60°N
56°N
18°W 12°W 6°W 0° 6°E 12°E 18°E 24°E 30°E
Grid size (NxN) 100
Density Percentil (DP %) 0
Interpolation
Draw
Model Variables / Uncertainty-Delay Propagation
ATM NEMMO, 2012
CATS Safety Module
Integrated Overall Safety Level Calculation
Safety impact assessment

Figure 3 Overall Safety Impact Approach using ATM-NEMMO/ CATS tool

5.2 Terminology

A **"Safety Enhancement System"** is a new system, product or operational concept (including for example new procedures and operating methods), that is expected to have a positive impact on the Safety of the Total Aviation System. This definition also applies to systems, products, or operational concepts that have not been primarily designed for the purpose of enhancing safety but – due to their nature and way of changing operations – are expected to have a direct or indirect safety benefit on the Total Aviation System.

An "**input parameter**" is a customisable value representing an aspect of the performance of an Air Traffic Management system/ operation in ATM-NEMMO model. It is used to simulate predictability/efficiency enhancements linked to the implementation of a Safety Enhancement System.

A “**Performance Indicator**” is a value obtained as output of the simulation using ATM-NEMMO. It provides information of the air transport system performance in terms of capacity (e.g. hourly throughput overloads), efficiency (e.g. percentage of flight departing on time) and predictability (e.g. average delay of delayed flights).

A “**disturbance**” is an event which produces variations from the planned operation of the Air Transport processes or elements. External disturbances are produced by an element which is not part of the Air Transport network.

5.3 Results Summary

The approach is to model a macroscopic scenario for network-wide safety analysis, enabling to assess the safety impact of introducing new safety enhancement systems and/or operations in the total aviation system. This has been done by analysing both safety critical points and safety benefits that can arise out of foreseen changes in the total aviation system, as example four safety enhancements have been proposed and analyzed. The starting point is the ATM NEMMO tool, which is a Network Macro Modelling tool to analyze macroscopic behavior of multi-component systems with complex interactions. WP3.4 has analyzed a combination of NEMMO and CATS to support the overall safety assessment. In addition, a User’s guide has been developed with guidance on how to use the NEMMO-CATS combination tool to support the safety assessments [4].

The theoretical study is focussed on Safety Enhancement Systems as the new systems/operations for which to obtain an overall safety assessment. The list of Safety Enhancement Systems that have been analyzed is included in the table below. The systems have been selected trying to cover as much as possible all flight phases and to consider both ground and airborne systems.

	Safety Enhancement System	Flight Phase
1	A-SMGCS (Advanced-Surface Movement Guidance and Control System)	Taxi out/Take Off
2	Brake to Vacate	Landing/ Taxi in
3	ASPA-IM-S&M (Airborne Spacing – Interval Management - Sequencing & Merging) Application	TMA
4	ATSAW-ITP (Airborne Traffic Situation Awareness - In-trail procedure)	En Route

Table 4 List of Safety Enhancement Systems

For each Safety Enhancement System considered, the input parameters to implement in the ATM-NEMMO model have been identified. Two approaches are considered:

- **Success approach**, in which it is assessed how effective the new concepts and technologies would be when they are working as intended. This is concerned with the positive contribution to aviation safety that the safety enhancement systems make in the absence of failure;
- **Failure approach**, in which the risks from the new concepts and technologies are assessed, i.e. as a result of the failure of the new concepts and technologies. This is concerned with the negative contribution to the risk of an accident that the ATM changes might have in the event of failure(s). This approach covers e.g. the loss of the system functionality and erroneous functioning and, in both

cases; the detected or undetected failure case can be considered. In the present study the failure approach considered is **detected loss**.

In order to later translate the performance results displayed by ATM-NEMMO as response to the relevant input parameters, into a safety impact, a safety module based on the CATS causal model diagrams is used. The core of the CATS causal risk model is formed by events that may lead to accidents/incidents, and that can be described as hazards. A particular hazard can be caused by multiple root causes, and the failure of safety barriers after a hazard takes place also has root causes. To represent this, the CATS model uses Event Sequence Diagrams (ESD) in combination with Fault Trees (FT). Fault Trees are used to represent the root causes of both the initiating event and the pivotal events of an ESD. Each fault tree contains events that are stated as faults and are combined by logic gates. The quantification of accident scenarios is done by assigning absolute probabilities to the initiating events of each ESD and conditional probabilities to the pivotal events, referred to the 'yes' branches of the events. The probability of the base events is determined by using historical air safety data, when available, by calculation using other quantified events (e.g. precursors) or by expert opinion.

In the WP3.4 study, the theoretical development of a CATS safety module for ATM-NEMMO tool builds on the idea that the implementation of certain new systems/operations has an impact on the probability of occurrence of certain base events considered in the ASCOS risk model (or CATS model).

The CATS safety module integrates the ESDs and FTs developed and quantified in ASCOS WP3.2 and links directly the outcomes of ATM-NEMMO simulations (Performance Indicators) to the probability of occurrence of specific base events that are considered to be sensitive to changes in the level of delay and/or overloads. This rationale is depicted in Figure 4. For each scenario of implementation of a Safety Enhancement System (either success or failure approach), the output of the ATM-NEMMO tool in terms of Performance Indicators is calculated. The resulting value of each Performance Indicator (PI) is compared with the value of the same PI in a baseline scenario (without the Safety Enhancement System implemented), from which the difference (either positive or negative change) is calculated. This change is linked to an increase or decrease of the probability of occurrence of certain base events in CATS module.

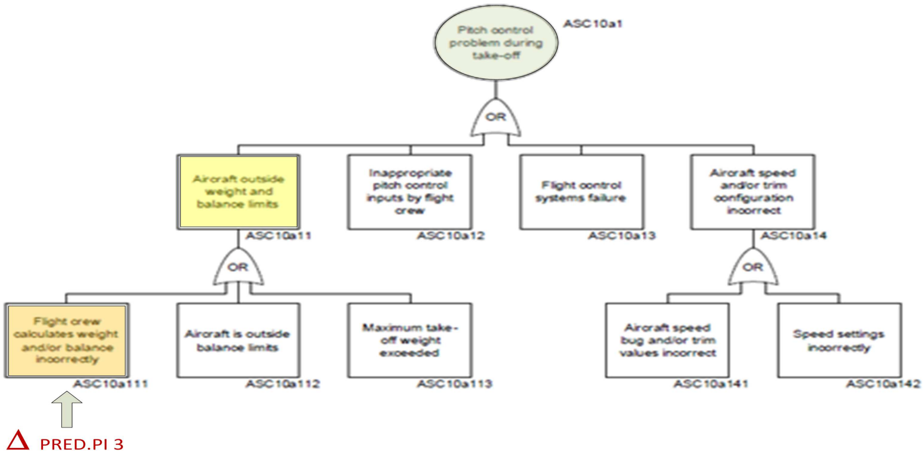
Pitch control problem during take-off
ASC10a1
OR
Aircraft outside weight and balance limits
ASC10a11
Inappropriate pitch control inputs by flight crew
ASC10a12
Flight control systems failure
ASC10a13
Aircraft speed and/or trim configuration incorrect
ASC10a14
OR
Flight crew calculates weight and/or balance incorrectly
ASC10a111
Aircraft is outside balance limits
ASC10a112
Maximum take-off weight exceeded
ASC10a113
OR
Aircraft speed bug and/or trim values incorrect
ASC10a141
Speed settings incorrectly
ASC10a142
Δ PRED.PI 3

Figure 4 Example of Impact of Variation in Reactionary Delay (PRED.PI 3)

In the example above, the increment of PI PRED.PI 3 has an impact on the probability of occurrence of the base event “Flight crew calculates weight and/or balance incorrectly”, and the resulting probability change is transmitted upstream up to the probability of the initiating event “Pitch control problem during take-off”. Through the corresponding ESD, this probability change in the base event is finally reflected in a change of the probabilities of the related end states (runway excursion, aircraft stops on runway and collision with ground).

An analysis of the influence of each ATM-NEMMO Performance Indicator on the CATS base-events has been performed, providing a rationale for each influence and an indication of positive or negative impact on the probability of the base-event considered. Quantification of these influences is left to expert judgement, where safety experts can customise the values in the tool according to the needs of their environment and type of assessment.

An expected generic impact on safety of each Safety Enhancement System has also been considered. The aim is to provide indications to the safety experts using the ATM-NEMMO/CATS model to customise the CATS diagrams:

- On one side, the network performance results for the new system in operation are translated into changes in probabilities of occurrence of CATS base-events;
- On the other side, the generic safety impact might be also translated into changes in CATS diagrams, in terms of failure rates and improvement/ addition of safety barriers.

The customised CATS diagrams in the CATS module, in combination with ATM-NEMMO performance results, form the tool to perform a **complete overall safety assessment of each Safety Enhancement System**.

Regarding the safety enhancements considered, the **baseline scenarios** are created through certain network characteristics and traffic customization. Additionally to the representation of nominal conditions, baseline scenarios also cover changes in the traffic volume and the application of external disturbances causing capacity shortfalls at airports and high density airspace areas. A disturbance is an event which produces variations from the planned operation of the Air Transport processes or elements. External disturbances are produced by an element which is not part of the Air Transport network. This facilitates the analysis of the system behaviour and the potential safety benefits of Safety Enhancement Systems also under critical conditions of operation.

Specific scenarios are defined according to the Safety Enhancement Systems studied. In order to obtain the safety risk picture associated to the success approach and the failure approach, the simulation results of the scenario must be compared to the corresponding baseline scenario. An example is shown in next table.

Scenario	Δ PI	Associated safety risk variation
Success scenario SEnS 1 + External disturbance B	↶ +z%	+x% in ESD-5
Baseline scenario + External disturbance B		

Table 5 Comparative Variation of Safety Risk Associated to Safety Enhancement

Besides, the particular scenarios considered can represent an inhomogeneous application of the Safety Enhancement Systems throughout the network, for those systems aiming at improved operations at airports, with highly safety robust airports and other airports with increased uncertainty in operations. For the failure scenarios consisting on detected loss of a Safety Enhancement System, also inhomogeneous applications are possible, with detected loss only at certain airports where the system is implemented and during different periods of time.

The results, in terms of overall safety level, can then be obtained at:

- Network level, using the variations of the global ATM-NEMMO performance indicators as homogenous input to the Fault Trees in the CATS module;
- Airport level, using the variations of the related local Performance Indicators at the specific airport;
- Cluster level, where Performance Indicators can be defined at a semi-global level, integrating only measures from a pre-defined set of airports, that can be, for example, those where an inhomogeneous implementation of a given Safety Enhancement System.

The results present the safety risk picture in terms of probability of occurrence of safety accident or incident for each of the following seven end-states: Runway excursion; Collision with ground, In flight break-up; Collision in mid-air; Collision on runway; Collision with ground; Collision on taxiway or apron [2, 4].

For each of them, he calculated change with regard to the baseline situation is shown for each of the ESDs in which the end-state is present. A proposed graphical representation of this overall safety level associated to a given Specific Scenario is shown in the next figure.

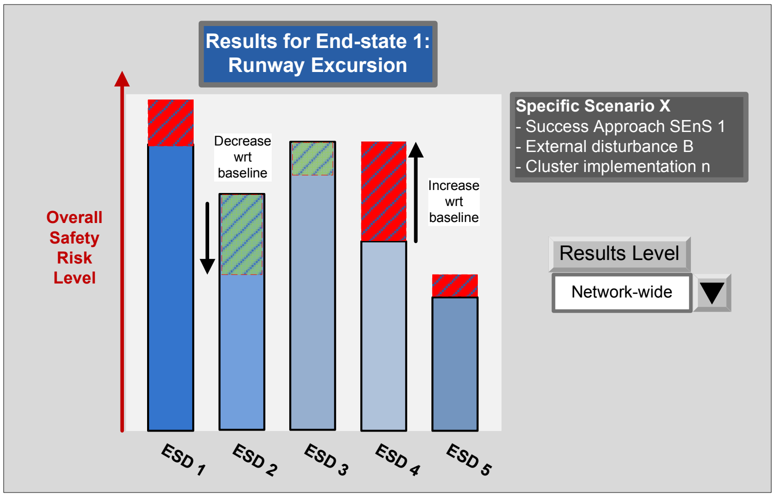

Figure 5 Overall Safety Level for Specific Scenario and End-State

As example, technical steps for production of overall safety level **at a given airport (Airport A)** for a given end-state linked to scenario SEnS #1 being implemented (success approach) only at a given cluster of airports are:

- Determine baseline (without SEnS #1) - ATM NEMMO PIs and corresponding base event probabilities, and baseline accident probability **at airport level for Airport A**;
- Implement Safety Enhancement System #1 (success approach) in ATM-NEMMO only at a given cluster of airports;
- Determine ATM-NEMMO PIs with SEnS #1 implemented **at airport level for Airport A**;
- From percentage changes in PIs, derive changes in probability of occurrence of certain base events in the CATS diagrams feeding the accident probability of the relevant end-state using the CATS-Safety Module integrated in ATM-NEMMO (CATS version);
- Calculate with CATS the new accident probability of the relevant end-state. This safety level is referred to the accident probability of the relevant end-state **for Airport A**, since DPIs used as input to the CATS diagrams were representative of performance variation only at Airport A;
- Display results (as shown in **Error! Reference source not found.**) using the CATS-Safety Module integrated in ATM-NEMMO (CATS version).

5.4 Conclusion and recommendations

The consideration of flight delays and other performance measures of the ATM system for the estimation of the total aviation system safety risks is a domain of study that is gaining attention. Long term and innovative research approaches are seeking to deepen into the ATM influences on safety risk, and in particular to explore how to better understand the ATM network behaviour and its impact on the safety level. The SESAR network on “Mastering complex system safely” is putting effort in this line of investigation. Modelling and simulation techniques are proposed to be used for trying to refine the estimation of safety risks by incorporating ATM network performance related factors, such as efficiency, predictability or uncertainty propagation.

The relationship between flight delays and safety in airline maintenance has been previously considered by safety practitioners. This relation being complex, related works demonstrate the effectiveness and feasibility of relating delays with civil aviation safety risk propagation and superposition.

WP3.4 has explored the integration of ASCOS/CATS causal risk models into an innovative modelling and simulation tool with the capacity to capture network performance and propagation of ATM related uncertainties. Sharing this discussion with the ATM and safety community will bring useful feedback on the way forward. And of course, implementing the proposed approach and testing representative cases will reveal strengths and weaknesses of the method, and will provide more insight into the intricacies of managing the complex air transport network and ensuring that safety risks are minimised.

6 *Total Aviation System Safety Standards*

6.1 Introduction and objectives

The ASCOS project aims at developing certification process adaptations with supporting safety tools to ease certification and safety enhancement in operation of the TAS. Within this global objective, WP3.5 contributes to this objective by proposing a process to improve the total aviation system safety standards using lessons learned from experience. Consideration of future risks associated to the impact of future changes in total aviation system organization is part of the study. The process will be 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.
    - 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:
    - The coordinated implementation within TAS stakeholders of a harmonized framework for safety standards,
    - The implementation of a continuous in operation feedback for safety standard improvement, and
    - The identification of safety issues and decide on mitigation means

Applying a Total 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. ASCOS D3.5 defines principles for a safety management organization at inter-stakeholder level and at stakeholder level for the total aviation system that should give birth to the standards needed to create the necessary working harmonization. The application of the safety standard improvement process described in this document needs the implementation of a set of actions. In this sense, the WP3.5 study aims at defining a common standard framework for product development applicable to each stakeholder and support the proposed certification approach developed in D1.3 [12].

6.2 Terminology

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): Total Aviation System (TAS): The TAS includes stakeholders active in all the domains in aviation including e.g. aircraft manufacturers, 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.

6.3 Results Summary

6.3.1 ASCOS overall process for safety standards improvement

The process starts with the identification of the standards to apply for system development and system assessment in operation. It ends up with a feedback loop to improve these standards using a continuous improvement process from lessons learned from operation. The proposed generic process is illustrated in the following figure

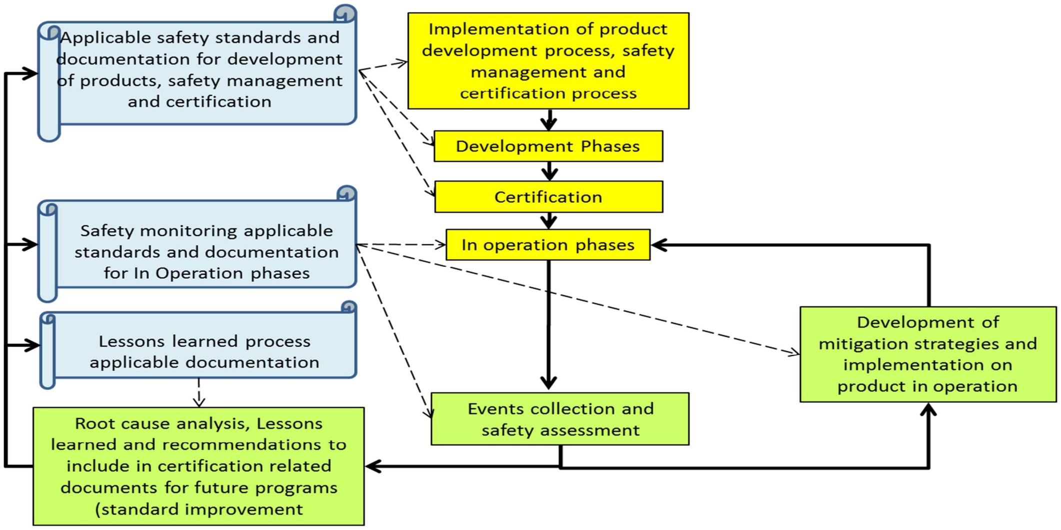
Applicable safety standards and documentation for development of products, safety management and certification
Implementation of product development process, safety management and certification process
Development Phases
Certification
Safety monitoring applicable standards and documentation for In Operation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

Figure 6 Safety Standard Improvement Generic Process

6.3.2 ASCOS Standard framework model for product development and Safety Assurance Process in operation

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 on development process.

The generic standard framework recommended is illustrated in the following figure.

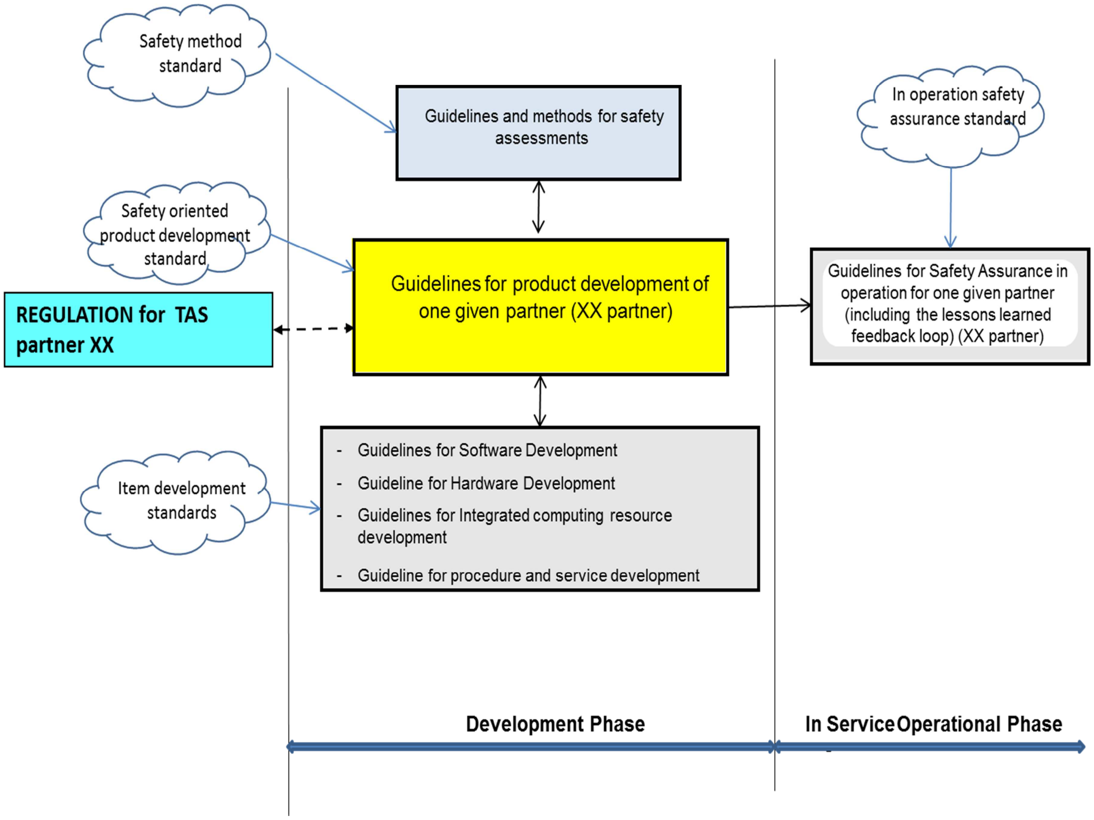
Safety method standard
Guidelines and methods for safety assessments
In operation safety assurance standard
Safety oriented product development standard
Guidelines for product development of one given partner (XX partner)
Guidelines for Safety Assurance in operation for one given partner (including the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

Figure 7 Generic Standard Framework recommended

6.3.3 ASCOS model for Safety Assurance Process in operation

The ASCOS Product Safety Assurance in Operation, merges the two main models for Assurance Processes from the ICAO SMM [18] and ARP 5150 [17], and uses the results from WP3.2 to support the identification of monitoring parameters, the detection of incidents and the risk assessment. The ASCOS process Product Safety Assurance in Operations 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.

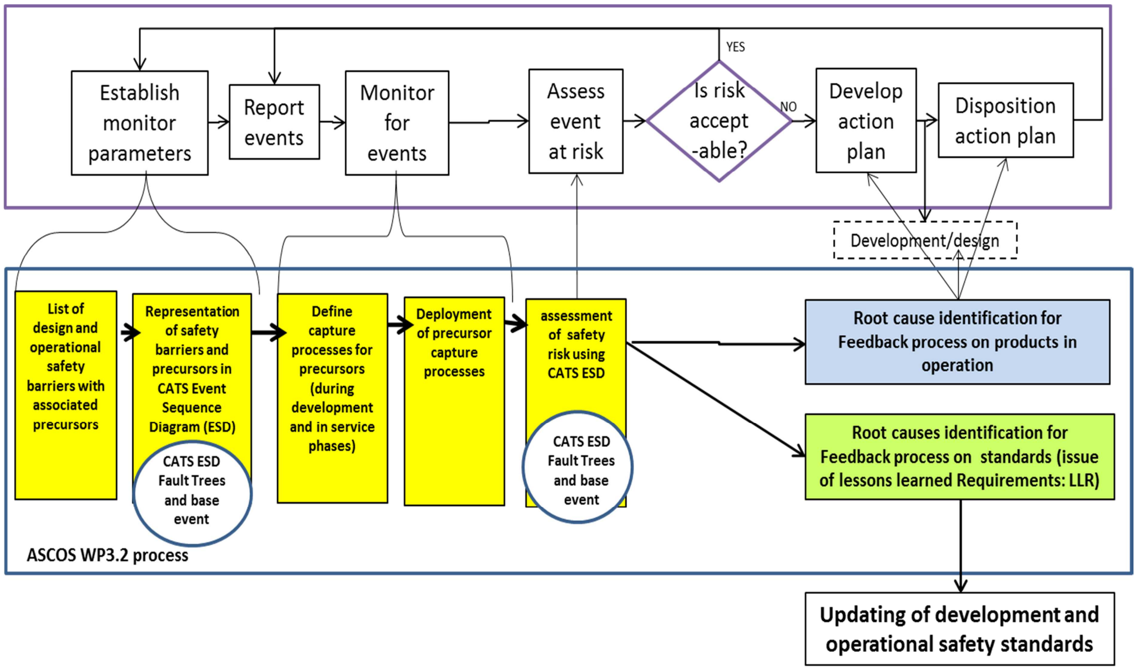
Establish monitor parameters
Report events
Monitor for events
Assess event at risk
Is risk accept -able?
YES
NO
Develop action plan
Disposition action plan
Development/design
List of design and operational safety barriers with associated precursors
Representation of safety barriers and precursors in 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 process
Updating of development and operational safety standards

Figure 8: ASCOS detailed safety assurance process in operation

6.3.4 ASCOS Process model for product development

During a product development process, the safety assessment process plays a key role generating safety requirements. 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. All these processes (including the safety assessment process) are called ”Integral processes”.

As per ASCOS WP3.1 [1], the recommended industrial practices for safety oriented development are organized around a coordinated planning and a sound and clear Work break down structure and the implementation of 8 safety oriented integral processes (see Figure 9).

Each integral process should be structured in the same way:

- A plan describing 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 [14] for aircraft and system development. These models are generic enough to be applied to the development process of each stakeholders of the total aviation system.

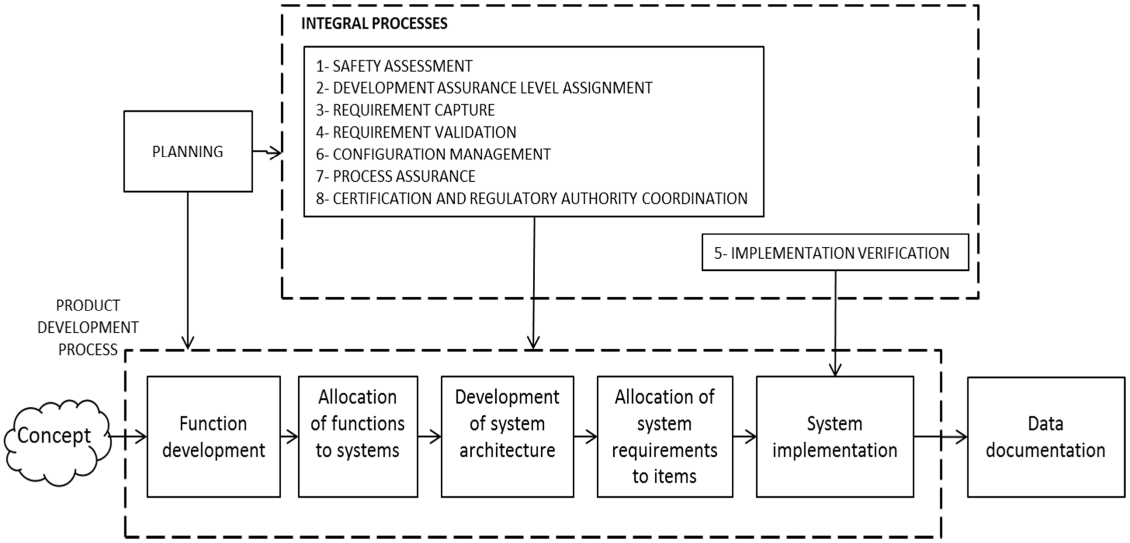
INTEGRAL PROCESSES
1- SAFETY ASSESSMENT
2- DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT
3- REQUIREMENT CAPTURE
4- REQUIREMENT VALIDATION
6- CONFIGURATION MANAGEMENT
7- PROCESS ASSURANCE
8- CERTIFICATION AND REGULATORY AUTHORITY COORDINATION
5- IMPLEMENTATION VERIFICATION
PLANNING
PRODUCT DEVELOPMENT PROCESS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

Figure 9- Development process model including integral processes (derived from ED79A/ARP 4754A[14])

In the above organization the steps of the ICAO SRM model [18] 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 mandatory to assure an efficient safety oriented development and to perform efficient safety assessment activities. ASCOS is to consider these models as a framework applicable at the level of each stakeholder of the total aviation system.

6.3.5 Precursors identification and Safety standards improvements from event in development and in operation

During the development and in service phase a product is facing situation due to failure, development errors, maintenances error, etc. These situations can be anticipated in safety assessments and mitigation means can be implemented in the design, these mitigating means are the safety barriers.

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. The malfunctions of safety barriers are precursors of situations that may lead to Hazardous or Catastrophic events. It is then necessary during the development phase to identify safety barriers and associated precursors (malfunctions of safety barriers), and during the product operation phases to monitor the precursors and to identify the root causes of barrier failures.

The identification of the safety barriers will be made first considering each stakeholders of the TAS independently, secondly by considering the different stakeholders of the TAS in an integrated way. These safety barriers and the barrier malfunctions (precursors) will be easily identified and visualized when constructing the safety risk models [2].

In the ASCOS project, the risks will be modelled through Events Sequence Diagrams (ESD) and Fault Trees developed using "Causal Model for Air Transport Safety" (CATS) tool for the five (5) operational issues identified in the European Aviation Safety plan (EASp). In these models safety barriers as well as precursors that can result in the failure of safety barriers are incorporated.

6.3.6 Feed back loop for safety standards improvement

The capture and root cause analysis of in operation events are the starting point of a feedback loop for safety standard improvement:

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 continues 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 is related to process development activity to generate a Lesson Learned Requirement (LLR) for improvement of development process standards.
4- The LLR are incorporated in development process standards including process and method documents, but also in questionnaire or checklists to use for requirement validation, requirement verification and review activities.

The steps 1 and 2 can be identified as a current safety follow up activities performed by TAS stakeholders on a product in operation. The steps 3 and 4 are specific for standards improvement. This is illustrated in the following figure:

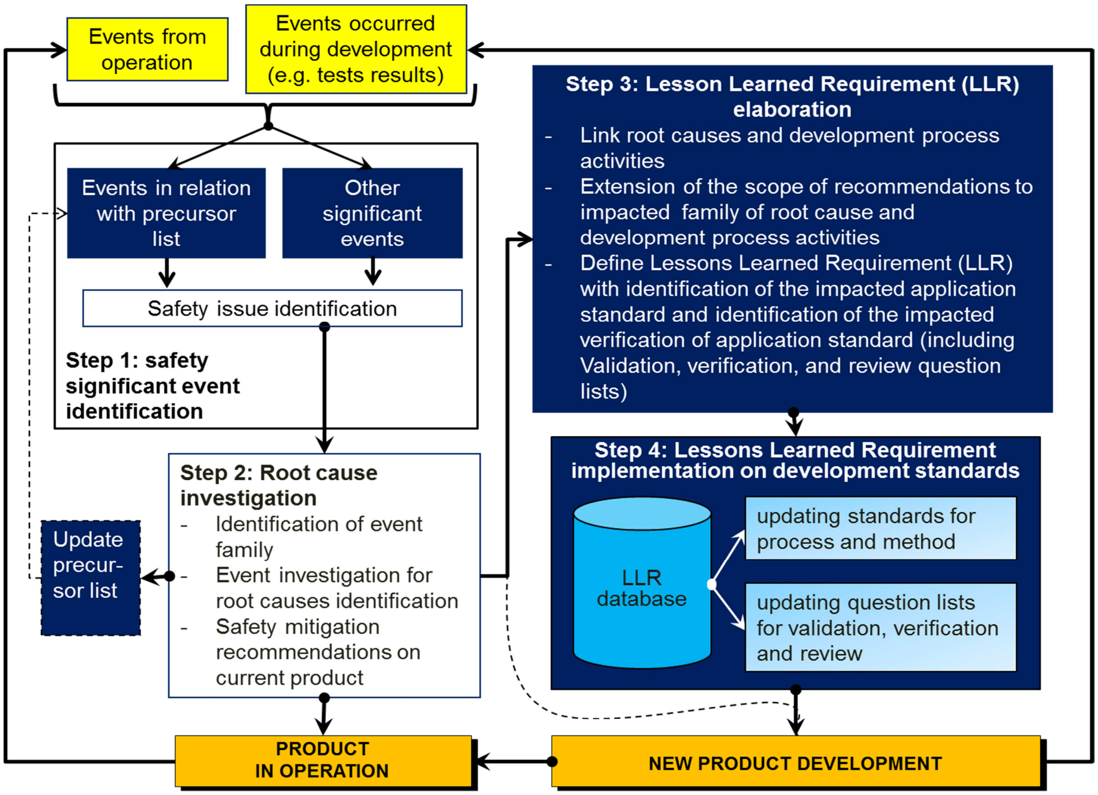
Events from operation
Events occurred during development (e.g. tests results)
Events in relation with precursor list
Other significant events
Safety issue identification
Step 1: safety significant event identification
Step 2: Root cause investigation
- Identification of event family
- Event investigation 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 10- Lesson Learned Requirement Process to improve standards

6.3.7 Principle for an in operation automatic identification of precursors

Definition of methods to detect and code automatically aircraft system malfunctions with a taxonomy that is “safety barrier oriented” and to record them in the maintenance computer are described in chapter 5.5 of ASCOS D3.5 [5]. Within the task the following steps were performed:

- Description of existing recording process of system malfunction in the maintenance computer of the aircraft,
- Definition of generic taxonomy that is:
  - safety barriers failure oriented – enabling identification and coding of safety barrier failure.
  - coherent with safety barriers identified in ASCOS/CATS model
  - compatible with existing safety taxonomies (CICTT/ADREP 2000 taxonomy),
- Identification of methods for automatic coding of aircraft system malfunctions and other errors and failures (e.g. related to flight crew, air traffic controller or ground service errors) with a taxonomy that is “safety barrier oriented” and record it in aircraft maintenance computer or other appropriate system. The process would be based on:
  - establishing of new, alternative sources of flight data
  - methods aiming at detection of precursors identified in within the WP2.3.
- Extension of the results of all steps above to each main player of the Total Aviation System (Airlines, ATM, Airports, Airworthiness and Crew licensing, with taking into consideration its specification).

6.3.8 ASCOS recommended common scheme for organization of safety standards applicable during product development and product 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. Each stakeholder develops coherent documents:

- 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).

Besides these documents, 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. At the level of each stakeholder the safety plan should describe the safety management implemented by the considered stakeholder.

It is 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. This ESG 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 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).

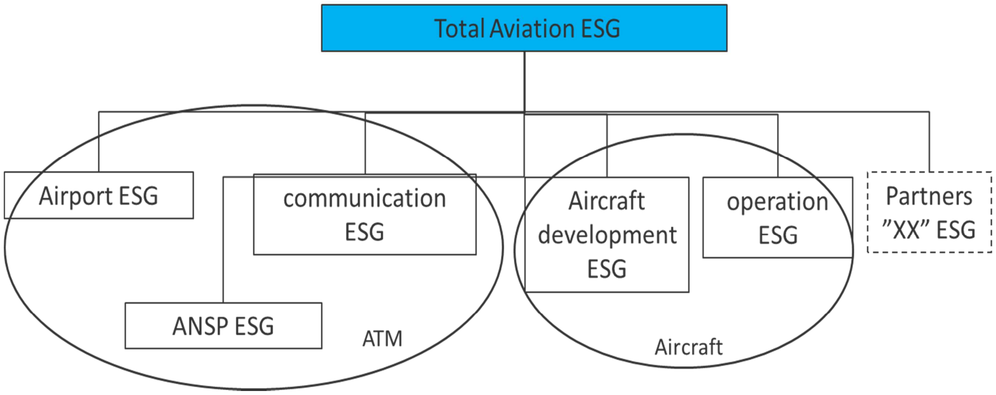

Figure 11- Safety management organization at TAS inter-stakeholder level and at stakeholder level

6.4 Conclusion and recommendations

A seamless certification process at Total Aviation System implies coordination and coherencies between the different stakeholders of the TAS. This coordination and coherency should be reflected the Safety standards used by each stakeholder of the TAS and in the TAS Safety organization.

Safety standards harmonization:

The ASCOS WP3.5 study promotes the application of a "common safety standard framework", by each of the TAS stakeholders, that will help to avoid certification bottle neck, to avoid identifying certification safety issues late in the certification process, 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.

Safety standards continuous improvement:

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 of the products. This improvement activity will assure the permanent adaptation of the standards to the safety and certification needs while maintaining a seamless certification process.

The ASCOS WP3.5 study promotes to implement a feedback process for safety standard improvement based on identification of in operation safety issue (with consideration of precursor events), identification of development and design root causes that have led to the safety issue and generation of Lessons Learned Requirements (LLR). These Lessons Learned Requirements are used for safety standard improvement and they will be systematically applied during the development of future products through the normal requirement Validation/Verification process.

TAS safety management organization:

ASCOS WP3.5 recommends the implementation of a TAS safety management organization. This TAS safety management organization will be based on an Engineering and Safety Group (ESG) at total aviation system inter-stakeholder level (TESG), see actions for this group on the Table below, 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 will be the interface with ICAO/EASA for application of the SMS and State Safety Plan as required by ICAO and EASA.

Action REF	Action description	ASCOS D3.5 Chapter ref for explanation
1 Safety standards organization	Safety standards organization	3 - 4
1.1 Safety standard framework	Implement in accordance with model illustrated in figure 15 a common safety standard framework applicable at each TAS stakeholder level and covering both product development and in operation safety assurance	4.4
1.2 Safety standards development	Develop/identify and implement at the level of each stakeholder of TAS, using the common safety standard framework, coherent safety standards for:	4.2 - 4.3 - 4.4
1.2.1	Product development	4.3 - 4.4
1.2.2	Software Item development	4.3 - 4.4
1.2.3	Hardware item development	4.3 - 4.4
1.2.4	Procedure and service development	4.2 – 4.4
1.2.5	Safety applicable methods	4.3 – 4.4
2. Precursor identification and coding/ continuous Safety standards improvement loop		5
2.1 Safety precursor identification	At TAS (inter-stakeholder level) implement a process for safety precursor identification based on CATS Event Sequence Diagrams (ESD)	5.2
2.2 Safety Precursor identification	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)	5.2
2.3. Safety standard continuous improvement	Implement a continuous improvement loop based on lessons learned from in operation events	5.3
2.4 future risk consideration	implement a process for future risks identification and mitigation	5.4
2.5 Precursor automatic coding	At TAS level as well as each stakeholder level implement as far as possible a process for an automating coding of the precursor events when they occurs	5.5
3. Safety management at TAS (inter-stakeholder) level and at stakeholder level	Implement at TAS (inter-stakeholder level) a safety management group to: - Enforce the activities and processes recommended in action item 1.1 to 2.5 in this table - Assure and Coordinated 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	6

Table 6 List of task to perform at TESG

7 *Overall conclusions and recommendations*

WP3.1 has identified several areas of improvement that would be necessary to address in order to develop a total safety methodology that could address the emerging and future risk, these required improvements are:

- More anticipation resulting from FAST EME1.1 inputs to any existing methods, permitting to mitigate risks (future and emerging risks) much earlier combined with promoting more safety assessment in early program phases
- Improved and more generalized detection of precursors confirming and characterizing emerging risks
- Management dispositions permitting a seamless application of methods through interfaces within the increasingly complex aviation system with particular emphasis to directly interfaced aviation systems such ground and airborne systems
- Proposing introduction of more management dispositions into standards which widen the scope and strength of the recommendations and will contribute to reduce gaps and shortcomings in safety assessments.

In order to respond to these issues, WP3 sets up a safety assessment methodology and safety standards improvements for the total aviation system. The methods and tools proposal are expected to support a seamless process between aviation domains, especially between the aircraft and ATM domain.

This safety assessment methodology takes benefits from the process described in WP3.2 that enable the safety practitioner to foresee the emerging and future risks and to connect them with precursors (specific tools are developed to represent the risks scenarios in WP3.3) It is possible to enlarge the scope of the WP3.2 by including a model ATM-NEMMO&CATS (WP3.4) that considers the impact of the safety enhancement in the aviation network. The safety assessment methodology proposes:

- Safety standards harmonization: Application of a “common safety standard framework” by each of the TAS stakeholder that will help to avoid certification bottle neck, to avoid identifying certification safety issues late in the certification process, 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.
- Safety standards continuous improvement: Implementation a feedback process for safety standard improvement based on identification of in operation safety issue (with consideration of precursor events), identification of development and design root causes that have led to the safety issue and generation of Lessons Learned Requirements (LLR). These Lessons Learned Requirements are used for safety standard improvement and they will be systematically applied during the development of future products through the normal requirement Validation/Verification process.
- TAS safety management organization: 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.

References

#	Identification, Title
[1]	ASCOS D3.1 Aviation Safety Assessment Methodology
[2]	ASCOS D3.2 Risk Models and Accidents Scenarios
[3]	ASCOS D3.3 Tool for risk assessment
[4]	ASCOS D3.4 Tool for Overall Safety Impact
[5]	ASCOS D3.5 Total Aviation system Safety Standards
[6]	Required functionalities of the risk assessment tool
[7]	ASCOS Minutes of Meeting, 04-09-2013
[8]	ASCOS D1.1 Analysis of existing regulations and certification processes
[9]	ASCCOS D2.1 Framework Safety Performance Indicators
[10]	SESAR JU P16.06.01, SESAR Safety Reference Material, Edition 2.1, 30/01/2012
[11]	ASCOS D2.2 Total Aviation System Baseline Risk Picture
[12]	ASCOS D1.3 Outline Proposed Certification Approach
[13]	EME1.2 Preliminary Proposal, EASA
[14]	ARP 4754/ED 79A Guidelines for Development of Civil Aircraft and Systems
[15]	ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
[16]	AIR 6218 Constructing Development Assurance Plan for Integrated Systems
[17]	ARP 5150 Safety Assessment of Transport Airplanes in Commercial Service
[18]	ICAO Safety Management Manual Doc 9859, 2nd edition
[19]	NLR Safety Methods Database, Version 1.0, 4 March 2013, Maintained by NLR
[20]	FAA/EUROCONTROL, ATM Safety Techniques and Toolbox, Safety Action Plan 15, Issue 2, http://www.EUROCONTROL.int/eec/gallery/content/public/documents/EEC_safety_documents/Safety_Techniques_and_Toolbox_2.0.pdf October 3, 2007.
[21]	GAIN; Guide to Methods & Tools for Airline Flight Safety Analysis, Second Edition, June 2003