Risk models and accident scenarios in the total aviation system

A.L.C. Roelen, J.G. Verstraeten, L.J.P. Speijker (NLR), S. Bravo Muñoz, J.P. Heckmann (APSYS), L. Save (Deep Blue), T. Longhurst (CAA UK)

A key step in an improved certification process is a risk model for the total aviation system. The objective of this study is to provide an integrated approach to risk modelling in which the total aviation system, and human factors and cultural aspects are considered in connection with technical and procedural aspects and with emphasis on representation of emerging and future risks.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	S.B. Munoz (APSYS)

Grant Agreement No.	314299
Document Identification	-
Status	Approved
Version	1.0
Date of Issue	06-01-2014
Classification	Public

This page is intentionally left blank

Abstract

Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance call for the adaptation of existing certification processes. The European Commission (EC) Project 'Aviation Safety and Certification of new Operations and Systems' (ASCOS) contributes to removal of certification obstacles and supports implementation of technologies. A key step in an improved certification process is a risk model for the total aviation system. The objective of this study is to provide an integrated approach to risk modelling in which the total aviation system, and human factors and cultural aspects are considered in connection with technical and procedural aspects and with emphasis on representation of emerging and future risks. Specific objectives are:

- To represent safety of the current total aviation system in accident scenarios;
- To represent emerging and future risks in accident scenarios;
- To represent safety culture and safety management in accident scenarios;
- To explain how to quantify the accident scenarios.

This paper describes how emerging and future risks can be represented in a risk model. This risk model is based on previous accident model development work, primarily the work performed to create the Causal Model for Air Transport Safety (CATS), which represents the total aviation system. The representation and the evaluation of the emerging/future risks using CATS can be done if model elements are 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 proposed as a suitable precursor capture process. The application of this process allows calculating precursors' occurrence rates and then the emerging/future risks by using the ASCOS risk model. The ASCOS risk model can be quantified by assessing the probability of occurrence of each of the different pathways in the scenarios. 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. The only practical solution to this problem is to derive a modification factor by expert opinion that can be applied to a risk model element that is affected by the safety management and safety culture of a particular organization. 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.

The risk model supports safety management in several ways. A common understanding of the service or system under consideration is enhanced when 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. 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 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.

This page is intentionally left blank

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank

1 Introduction

1.1 Background and scope

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

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

Introducing certification process adaptations cannot be done without giving due account to safety considerations. Any certification process requires evidence on safety assurance as key element. In this respect, it is relevant to note that the need for safety improvement is also recognized in the ACARE Beyond Vision 2020 (Towards 2050) (European Commission, 2010a), which states that 'society is increasingly reluctant to accept failures in the Air Transport System, which exerts more pressure on safety considerations'. The Flight Path 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. Just culture will be adopted as essential element of the safety process' (European Commission, 2011). Clearly, 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.

Although a total aviation system approach is becoming more widely supported in aviation, there is still a lot to be done before this will actually be embedded in certification processes and safety management. ASCOS aims at contributing to such total aviation system approach by conducting research on the following topics: development of a framework of Safety Performance Indicators, establishment of a baseline risk picture and safety performance targets, definition of a process for continuous safety monitoring, development of risk models and accident scenarios representing the future aviation system, and subsequent incorporation of the – total aviation system – safety methods and tools in safety standards.

1.2 Needs

Certification of new operations, systems and products requires an assessment of the safety risks involved. It is proposed to conduct such assessments with support of risk models and accident scenarios representing the total aviation system.

A total aviation system approach for the certification of new operations, systems and products requires a good view on potential emergent and future risks not present in today's aviation system. A proactive approach will have to be taken to ensure that potential future hazards and risks can be mitigated and safety will be maintained or even increased as compared to the current safety level. It will be necessary to develop a safety picture of the future, taking into account likely changes, trends as well as the introduction of new products, systems, technologies and operations for which safety regulations may need to be updated.

The risk models and accident scenarios that are being used in the certification process should include procedures to incorporate emerging and future risks. This will enable better anticipation and responding to precursors instead of merely reacting on accidents.

1.3 Objectives

The objective of this study 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. Specific research objectives are:

- To represent safety of the current total aviation system in accident scenarios;
- To represent emerging and future risks in accident scenarios;
- To represent safety culture and safety management in accident scenarios;
- To explain how to quantify the accident scenarios.

1.4 Research approach

This study proposes to apply risk modelling as one of the methods for supporting certification of operations, systems and products. The current state of the art in aviation system wide risk modelling and tools is provided by the EUROCONTROL Integrated Risk Picture (IRP) (Eurocontrol, 2006), SESAR Accident/Incident Model (SESAR, 2012), FAA's Integrated Safety Assessment Model (ISAM) (Borener et al., 2012), and the Dutch Causal Model for Air Transport System (CATS) (Ale et al., 2009), 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. Each ATM change is modelled through adjustments representing its expected impacts on appropriate elements of the risk model. These effects, together with the effects of changes in traffic levels, can then be summed to estimate the total risks and contributory / causal breakdown for 2013, 2017 and 2020. This approach allows investigation of the improvements that are necessary to satisfy the ECAC wide safety targets. 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.

To represent future and emerging risks, this study builds on the work that is performed by the Future Aviation Safety Team (FAST), which developed an approach to discovering aviation futures which uses the concept of 'Areas of Change'. These possible futures might interact with the concept under analysis, producing unanticipated hazards or rendering existing safety barriers less effective (FAST 2012, FAST 2013, and Masson et al., 2012). The next step is to define precursors, i.e. identifiable events that may be used as indicators for hazards. These precursors should then be related to elements of the risk model.

2 Risk modelling and accident scenario approach

The approach is to base the risk modelling on the practice of Probabilistic Risk Assessment (PRA) that originates from the nuclear power industry and is also applied in other industries such as oil and gas and the chemical process industry. Probabilistic risk methods were introduced in the nuclear industry because of a desire to meet risk targets and to quantify and to evaluate the effects of design improvements of nuclear power plants (Keller and Modarres, 2005). The methods for probabilistic risk analysis that were used originated from the aerospace industry (fault trees) and decision theory (event trees). The first full-scale application of these methods to a commercial power plant was undertaken in the Reactor Safety Study WASH-1400 published by the American Nuclear Regulatory Commission NRC in 1975 (NRC, 1975). Event trees and fault trees were used to represent possible accident scenarios following six different initiating events. Although an independent evaluation (Lewis et al., 1979) concluded that the WASH-1400 study had shortcomings it also said that the study provided the most complete single picture of accident probabilities associated with nuclear reactors. The use of fault trees and event trees coupled with an adequate database was considered to be the best available tool to quantify these probabilities. After the Three Mile Island accident[1] , the use of PRA in the nuclear industry expanded and by 1995 the use of PRAs had been well established in the nuclear industry. Importantly, PRA results, tools and techniques are fundamental in all regulatory matters in the nuclear industry. Even though the use of a fault trees originated from the aerospace industry, and fault trees are explicitly mentioned in advisory material on FAR.25.1309 (FAA, 1988) and EASA CS 25.1309 (EASA, 2013), the application of PRA is aviation is primarily restricted to assessment of technical systems in aircraft.

In this study, PRA will be applied to the total aviation system, i.e. the application of fault trees and event trees coupled with an adequate database for a safety assessment of the total aviation system. The fault trees and event trees are derived from the Causal Model for Air Transport Safety (CATS) that has been developed earlier by an international consortium led by Delft University of Technology and funded by the Dutch government (Ale et al, 2009). A fundamental characteristic of CATS is that it describes accident scenarios and accident avoidance scenarios.

An accident scenario is a chronological description of a series of events leading up to an accident. A common way to visualize such a scenario is by the Swiss cheese model of Reason (1990). In the total aviation system there are, or must be, multiple safety barriers in place such that a single failure does not result in an accident. These safety barriers are not flawless, because they involve both fallible humans and systems, and flows are represented in the Swiss cheese model by the holes in the cheese. As history has shown there are trajectories of accident opportunity through multiple layers, or slices of cheese, leading to accidents. Every accident is a unique occurrence. Each accident involves different causes, different components, different locations, environmental circumstances, organisations and people. Representing every single detail of every possible accident in a single risk picture is practically impossible. To limit the number of accident scenarios in a risk

[1] The accident at the Three Mile Island nuclear power plant near Middletown, Pennsylvania, on March 28, 1979, was the most serious in U.S. commercial nuclear power plant operating history, even though it led to no deaths or injuries to plant workers or members of the nearby community. The accident resulted in a partial meltdown of the reactor core but only very small off-site releases of radioactivity.

model that represents the total aviation system, each scenario must represent a 'typical' accident that is obtained by generalisation and discretisation of individual occurrences. A review of aircraft accidents indeed shows that often event sequences are very similar, even for cases where human error plays an important role in the accident sequence. An example of such a recurring accident type is an aircraft stall and loss of control following an attempt to take off while the aircraft's wing is contaminated with snow or ice. Crash due to stall and loss of control following an attempt to take off with a contaminated wing in icing conditions can be considered an accident archetype. Another example of an accident archetype is a runway overrun following landing long and fast on a wet runway, possibly in combination with cross- or tailwind. A review of a large set of aircraft accidents identified 33 of such accident archetypes (Roelen and Wever, 2005).

For the purpose of ASCOS, the accident scenarios are represented using event sequence diagrams (ESD) and fault trees. An ESD consists of an initiating event, pivotal events and end states. A representation of a generic ESD is given in Figure 1. ESDs provide a description of series of events leading to accidents. An initiating event represents the start of the main accident scenario. Subsequent pivotal events determine how the occurrence evolves into different possible end states. A single ESD therefore represent accident scenario(s) as well as accident avoidance scenarios. In case of the generic ESD of Figure 1 there are two accident scenarios and two accident avoidance scenarios. Fault trees are used to represent the root causes of both the initiating event and the pivotal events of an ESD. Mathematically, fault trees and event sequence diagrams are relatively simple as they both use Boolean logic and combining fault trees with ESDs is very straightforward. The great advantage of ESDs and fault trees is that a very simple set of rules and symbols provides the mechanism for analysing very complex systems. Both the ESDs and the fault trees are quantified in the sense that probabilities of occurrence are assigned to the various events.

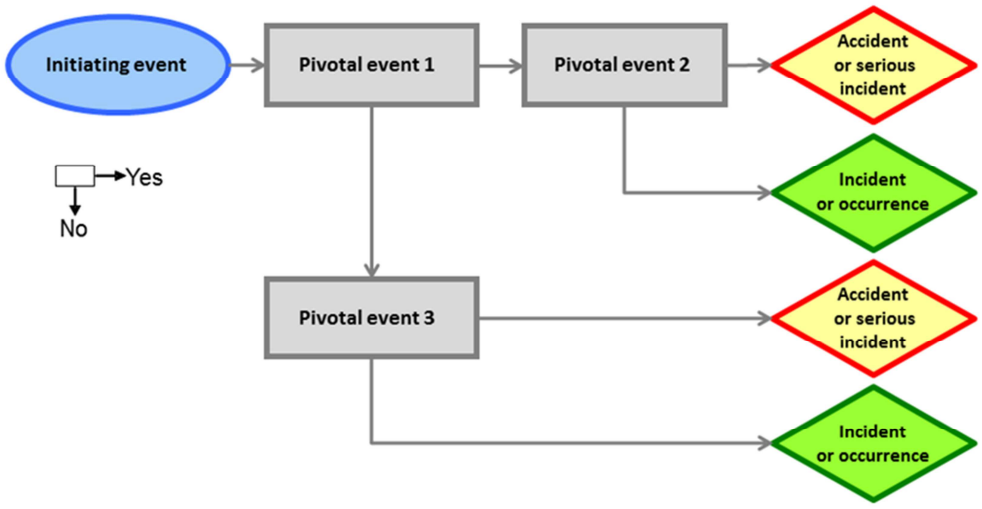

Figure 1: Generic representation of an Event Sequence Diagram

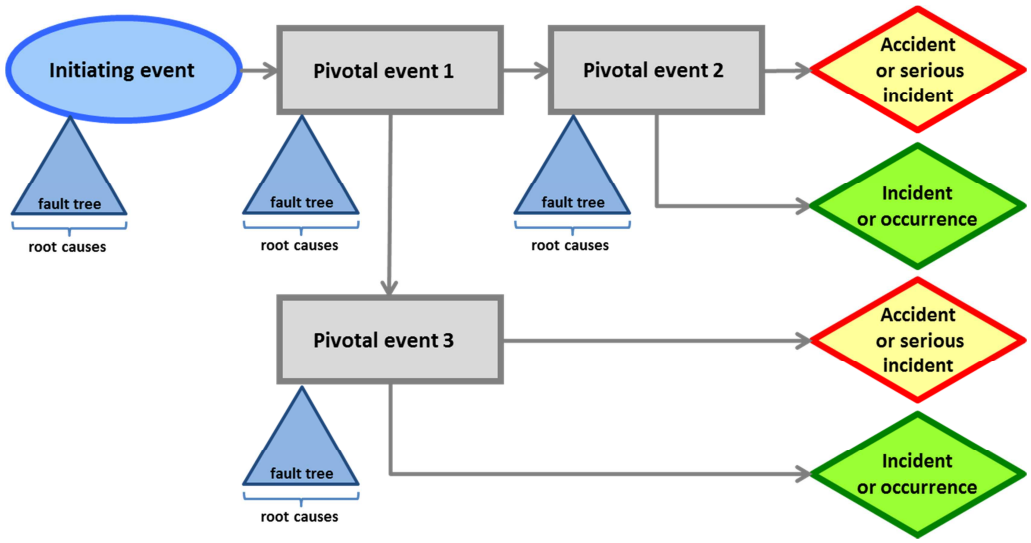

Figure 2: Fault trees connected to the ESD.

3 Risk model for the total aviation system

3.1 Development of the ASCOS accident model

The ASCOS accident model consists of ESDs and fault trees developed to represent the total aviation system. The ASCOS accident model is based on previous accident model development work, primarily the work performed to create CATS (Ale et al., 2009). The ESDs and fault trees of CATS are used as a starting point to create the ASCOS accident model. For the purpose of the ASCOS accident 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. These changes include different naming of events, different definitions, addition or deletion of events, and combining of ESDs. To assure compatibility, the CATS numbering of ESDs is maintained. Gaps in numbering are either because a specific ESD was dropped during the development of CATS, or because two or more CATS ESDs are combined to form a single ASCOS ESD. The ASCOS accident model includes a fault tree for each initiating event, and for most pivotal events. According to NASA's Fault Tree Handbook (NASA, 2002), "the development of a quantitative model is based on the need to get the best possible estimate for the top event probability, considering the data and other information that are available. Fault trees are developed to a level of detail where the best failure probability data are available". Since detailed failure information on non-critical events is often lacking in aviation, the fault trees cannot be too detailed.

3.2 Quantification of the ASCOS accident model

The ASCOS risk model is quantified by assigning probabilities of occurrence to each of the different pathways in the scenarios. A quantified model gives a risk picture of the system that is described by the model, based on historic or expert opinion-derived data. It can be used to analyse the risk of individual events: for each event in the model the probability is known and the severity can be derived from the conditional probability of an accident given the particular event occurring. The model can also be used to assess the impact on safety of changes to the system. Proposed changes can have an influence on the probability of occurrence of events described by the model. By quantifying this influence, the model can be used to determine the quantitative influence of the change on accident risk. The model can also be expanded by adding new events that are specific to the particular change.

3.3 ASCOS accident model and aviation safety in Europe

EASA's European Aviation Safety plan (EASp) identifies main risk areas of commercial air transport operations (EASA, 2012). The main operational issues are identified through the reporting and analysis of safety occurrences; events where the available safety margin towards accidents or serious incidents has been reduced. The EASp lists the following operational issues as being of primary importance: runway excursions, mid-air collisions, controlled flight into terrain (CFIT), loss of control in flight (LOC-I), and ground collisions.

Table 1 provides the ASCOS ESD initiating events and their relation with the EASp main operational issues.

Table 1: 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				√	

One of the aims of ASCOS is to progress beyond the state-of-the-art by developing and validating a continuous monitoring process in which safety occurrences will be used as safety performance indicators. These safety occurrences are a measure of safety performance because they are precursors to the five categories of end states as defined in the EASp. The ASCOS accident model can be used to translate the safety performance indicators into a measure of safety in terms of the likelihood of accidents or serious incidents taking place. Therefore, Table 1 matches the ESDs of the ASCOS accident model with the five end state categories of the EASp. A match indicates that the ESD represents scenarios involving that particular end state. Some ESDs represent safety occurrences that can evolve into more than one end state depending on which safety barriers are breached.

4 Representation of emerging and future risks

Before starting to discuss how emerging and future risk can be represented in the risk model, it is necessary to describe how we define emerging and future risks.

- A "current/known risk" is defined by the combination of severity and the current/known likelihood of harm (damage to people or equipment) accepted in the certification process.
- An "emerging risk" is defined as a current/known risk that is increasing or a new risk that becomes apparent in new or unfamiliar conditions (derived from IRGC, 2010).
- 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).

Risk is a condition that is inflicted by a hazard. To detect if a hazard is present, precursors are required. A precursor is defined as an "identifiable event that may be used as an indicator for known or potential hazards". Representation of emerging and future risks in a risk model therefore starts with the identification of precursors associated with emerging and future hazards. The second step is to link the precursors with elements of the model. 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.

Identification of precursors

A commonly used method for identifying and describing emerging and future risks involves creating a series of possible futures describing how the system of interest (the aviation system in our case) might develop. For each possible future, the hazards that may cause risk are identified (IRGC, 2010).

This way of working is also applied by the Future Aviation Safety Team (FAST), a group of multi-disciplinary, international safety experts whose primary focus is identification and publication of emerging and future risks across aviation and space sectors (FAST, 2012). FAST representatives were drawn from major air carriers, pilot communities, regulation and certification authorities, airframe and avionics manufacturers and research laboratories from Europe, the United States and Canada. The FAST philosophy promotes a holistic, system-wide view of safety in possible future aerospace environments. As FAST began its work in 1998, the team arrived at an early consensus position that to identify emerging and future risks possibly affecting the aviation system, one must first understand the context in which aviation operations occur. These contextual factors consist of both changes within the aviation system and changes external to the industry. To this end, FAST has identified and maintains a repository of Areas of Change (AoC). An AoC is defined as any phenomenon that will affect the safety of the aviation system either from within or from domains external to aviation, i.e. it is a possible description of (part of) the future. The time horizon for the AoCs varies between 5 and 25 years into the future. As far as we know, this list of AoCs is the only dedicated, comprehensive compilation of transformational phenomena affecting the global aviation system. The FAST AoC list is reviewed on a regular basis (approximately every two years) by the FAST Team. In addition, the FAST Team continuously monitors the aviation system and the external environment for new AoCs that may arise.

For each AoC, the FAST team has identified hazards that may result from the change. Of primary interest are hazards generated by interaction among AoCs. A fundamental premise of the FAST approach is that the interactions and overlaps or gaps among the system to be assessed and the AoCs are the most likely catalysts for revealing and understanding future hazards.

A recent catalogue of approximately 100 Areas of Change (FAST, 2013) is a deliverable to the Aviation Systems Analysis Team (ASAT) within the NASA Aviation Safety Program. Among a wide spectrum of issues this catalogue in particular addresses:

- Characteristics of NextGen/SESAR
- Air/ground automation
- Shifts in aviation personnel demographics
- Pilot training and simulator fidelity
- Flight deck and aircraft systems
- Unmanned Aerial Systems integration
- Proactive safety systems & SMS
- Commercial passenger/tourist spaceflight developments
- De-orbiting satellite debris.

Potential hazards associated with each AoC are also listed, resulting in a total set of approximately 450 near-, mid-, and far-term hazards. The next step in the process is to define precursors, i.e. identifiable events that may be used as indicators for hazards. For instance, one AoC is 'Increasing numbers of Light Sport Aircraft' with the associated hazard 'Inadvertent flight into unapproved airspace' (FAST, 2013). A precursor for this hazard is the number of airspace infringements.

Linking precursors with model elements

Precursors should be related to base events of the risk model fault trees. In case a precursor cannot be related to a base event, the applicable fault tree and ESD should be reviewed and expanded with elements that can incorporate the precursor.

Ensuring completeness of the risk model

The representation of emerging and future risks in the risk model can be done if a dedicated precursor capture process is defined and if each precursor can be related to a base event in the model. For that it is necessary that the risk model is sufficiently complete. This means that all initiating events are envisioned, all pivotal events are recognised, no safety barrier is forgotten and no fault tree base events are overlooked. This can be done in two steps:

1. Using safety assessments, product descriptions and operational documentation to identify all safety barriers that are implemented in the design and verifying that these safety barriers are represented in the risk model.
2. Review of the risk model by experienced people from different domains, e.g. aircraft design, flight operation, air traffic control, ATM procedure design, airport design.

Example application: Loss of control due to fire

As an example we consider the accident type 'loss of control in flight' and particularly a scenario where the loss of control is induced by an on-board fire. Cases of accidents that followed this scenario are ValuJet flight 592 of 11 May 1996 (NTSB, 1997) and Swissair Flight 111 of 2 September 1998 (TSB, 2003).

In the ASCOS risk model, this scenario is represented as ESD ASC-11. Figure 3 shows the full ESD for this scenario, while Figure 4, Figure 5 and Figure 6 show the associated fault trees.

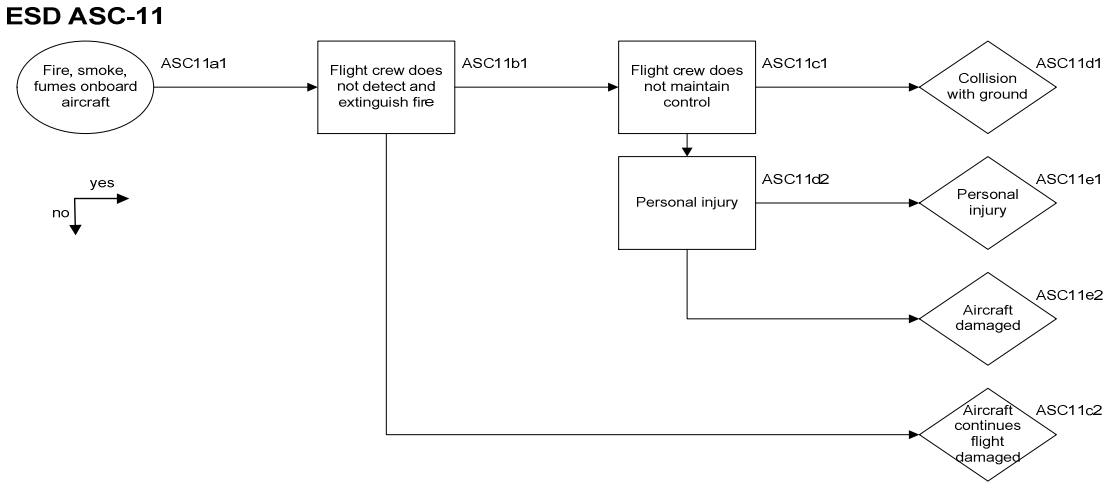

Figure 3: Event Sequence Diagram for ESD ASC-11

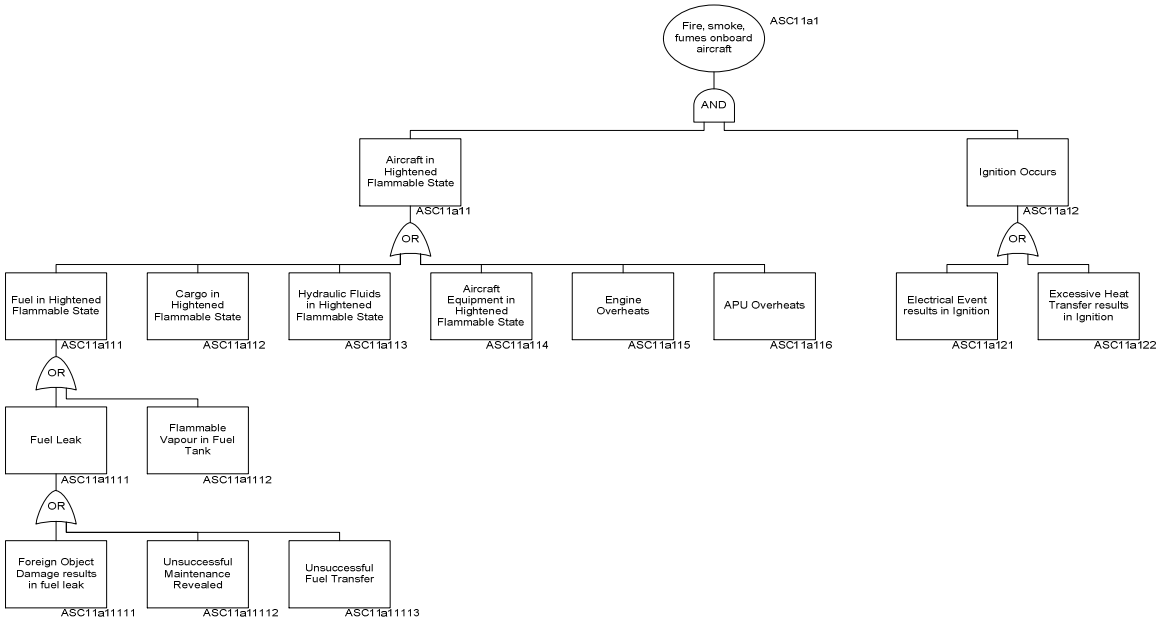

Figure 4: Fault tree for the initiating event of ESD ASC-11

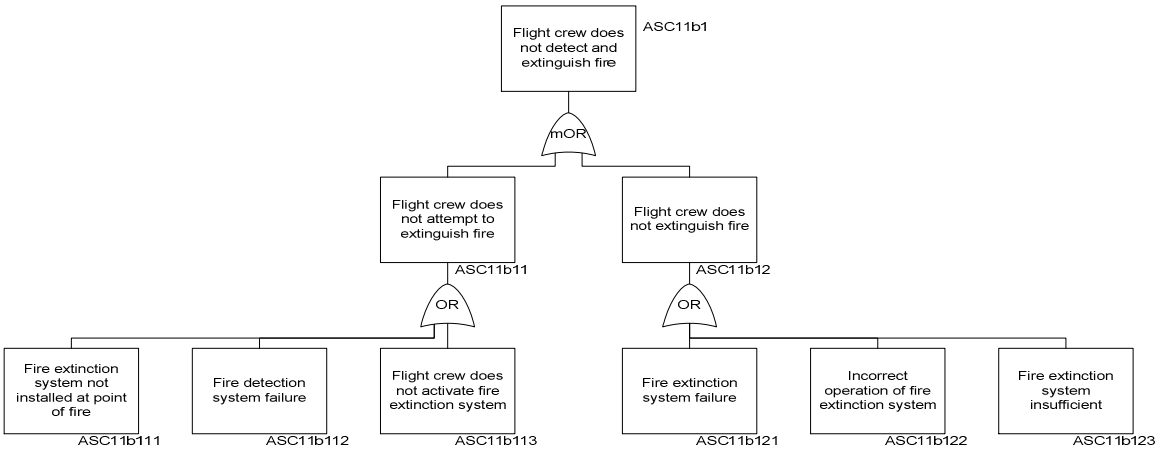

Figure 5: Fault tree for first pivotal event of ESD ASC-11

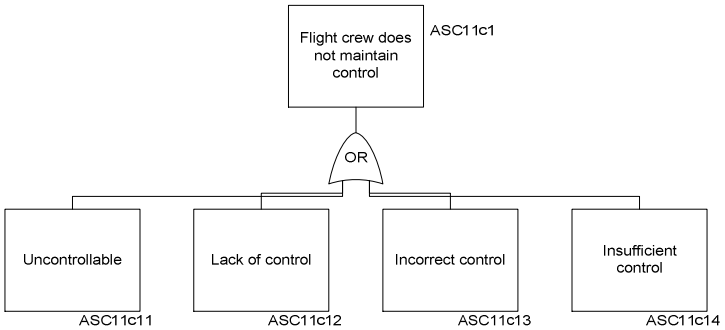

Figure 6: Fault tree for the second pivotal event of ESD ASC-11

There are several areas of change as identified by FAST that could potentially alter future probabilities of the fault tree events. One of the most obvious is FAST area of change 19 '*Emergence of high-energy propulsion, power and control systems*' and the associated hazard '*unexpected thermal runway/overheating and combustion*', which influences the fault tree for the initiating event (Figure 4). This hazard can be linked directly with fault tree base events ASC-11a121 'Electrical event results in ignition' and ASC11a122 'Excessive heat transfer results in ignition'. All else remaining equal, the realisation of this hazard will lead to increased probabilities of these fault tree base events and consequently an increase in the probability of end state ASC-11d1 'collision with ground', which represents an unrecovered loss of control accident. The current estimated probability of this end event, based on European accident data over the years 1995 through 2011, is $4.59 \cdot 10^{-10}$ per flight (ASCOS D2.2, 2013). To monitor whether this hazard is indeed materialising, precursors need to be identified that tie the hazard to these fault tree base events. Obvious precursors for this hazard therefore are 'Electrical events' and 'excessive heat transfer events'. Monitoring these precursors allows predictive adaptation of the accident probability estimates.

However, the future will see many changes, not only the possible emergence of high-energy propulsion, power and control systems. It is the ability to systematically assess multiple potential changes (i.e. multiple possible futures) that make these risk models so powerful. Some areas of change as identified by FAST are related to pilot skills and therefore potentially influence fault trees ASC-11b1 (Figure 5) and ASC-11c1 (Figure 6). An example is AoC 189 '*Shifting demographics from military to civilian trained pilots*' which has as one of its hazards '*Lack of aircraft system knowledge and diagnostic skills by air crew*'[2]. This hazard can be linked directly with fault tree base events ASC11b113 'Flight crew does not activate fire extinction system' and ASC11b122 'Incorrect operation of fire extinction system'. A precursor for this hazard is the percentage of commercial pilots with a military background. While AoC 19 alone might not be sufficient to significantly change the accident probability, a future that combines AoC 19 and AoC 189 might be a different story altogether.

[2] This hazard was also identified by NTSB Vice Chairman Christopher Hart during a presentation to Vaughn College of Aeronautics, New York, NY, on October 25, 2013 (Hart, 2013).

5 Representation of safety culture and safety management

A safety culture is the attitude of an organisation and its members that helps the organisation to maximise its own safety. A strong safety culture ensures that the organisation defines and continues to implement safety measures also in the absence of accidents and is an enabler to insure that the organisation's safety management system works in practice.

According to Reason (1997) a safety culture encompasses the following components:

- A *reporting* culture, which encourages employees to divulge information about all safety hazards that they encounter.
- A *just* culture, which holds employees accountable for deliberate violations of the rules but encourages and rewards them for providing essential safety-related information.
- A *flexible* culture, which adapts effectively to changing demands and allows quicker, smoother reactions to off-nominal events.
- A *learning* culture, which is willing to change based on safety indicators and hazards uncovered through assessments, audits, and incident analysis.

All these activities can be said to make up an *informed* culture (Eurocontrol, 2008), one in which those who manage and operate the system have current knowledge about the human, technical, organizational and environmental factors that determined the safety of the system as a whole.

Several instruments are available to assess the level of safety culture within an organisation, most are applied in the form of web- or paper-based surveys to various organisational levels within the organisation, see for instance, Gordon et al. (2004), ATSB (2004), Thaden and Gibbons (2009), Balk and Montijn (2010), IAA (2011).

An SMS is a system to assure the safe operation of aircraft through effective management of safety risk (ICAO 2012). The four components of an SMS are:

1. *Safety policy and objectives*: outlines the principles, processes and methods of the organization's SMS to achieve the desired safety outcomes.
2. *Safety risk management*: ensuring that the safety risks encountered in aviation activities are controlled in order to achieve their safety performance targets.
3. *Safety assurance*: processes and activities undertaken by the service provider to determine whether the SMS is operating according to expectations and requirements
4. *Safety promotion*: encouraging a positive safety culture and creating an environment that is conducive to achievement of the service provider's safety objectives.

The effectiveness of safety management can be measured by a methodology based on the ATM safety maturity survey framework (see Eurocontrol, 2009)[3].

[3] The effectiveness of safety management as measured by a methodology based on the ATM safety maturity survey framework is one of three safety performance indicators for ANSPs as required by the European Commission (2010b).

Representation of safety culture and safety management in the risk model is ideally done by linking the components of safety culture and safety management with the base event of the fault trees. However, there are a number of reasons why this is not practical:

- Safety culture and safety management are more related to latent failures, while elements of the risk model are more related with active failures.
- The same safety culture or safety management component might simultaneously contribute to several fault tree elements. Although the difficulty of representing such common causes is well known and solutions have been identified (Vesely et al., 1981) it is still a complication that cannot be ignored. A particular difficulty is the fact that the influence of safety culture is not likely to be the same for different affected elements of the fault tree.
- Measurements of safety culture and safety management appear more appropriate for monitoring trends within the same organisation or comparison between different organisations rather than for the identification of absolute frequencies.

Lin (2011) presents a theoretical solution to linking components of safety management with elements of the fault trees, but the description of safety management that is used there does not fit well with the components of SMS as defined by ICAO.

A stopgap measure for this problem is to derive 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. A similar approach is applied in Eurocontrol's Integrated Risk Picture (IRP) to represent organisational and cultural factors (Eurocontrol ,2006) and in the FAA's Integrated Safety Assessment Model (ISAM) Borener et al., 2012). ISAM uses a web based tool 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.

6 Use of the risk model to support safety management

Even though it was concluded in the previous chapter that representing safety management in a risk model is not feasible, there can be a link between safety management and the risk model in the sense that the risk model can support and enhance safety management in various ways.

Use of the risk model to determine the 'visibility of safety'

The risk model may be used to seek an improvement in the management of safety risk by using the risk model to provide certainty as to what is being managed i.e. is it safety of a service or is it the quality of a supporting service (e.g. contracted service) or system. By describing a service or system in terms of where it resides in the risk model and in terms of its relationship to the safety related service one is able to share a common understanding of the safety significance of the service or system under consideration. This introduces the notion of a 'view on safety' whereby only a provider of a system or service that has direct safety significance is considered to have a view on safety. This approach can be used across the whole of aviation as a way of describing the 'safety significance' of each cross domain relationship. For the purpose of safety assurance:

- Systems or services that have visibility of safety require, prior to implementation, assurance that the systems or services are safe for a given application in a given environment, whilst
- Systems or services that do not have visibility of safety require, prior to implementation, assurance that the systems or services behave only as specified in a given environment.

This aligns with the definitions, currently under development within EASA Rule Making Tasks (RMT) 0469, of a 'safety assurance case' and a 'safety support assurance case' as given below;

- A safety assurance case is: "a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment".
- A safety support assurance case is: "a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that the system behaves only as specified in a given environment".

Use of the risk model to improve the Continuous Oversight function

The second proposal of this section is to improve the Continuous Oversight function that is a part of Safety Management. For effective Continuous Oversight the Safety Assurance case is required to identify a complete and correct set of monitoring requirements. Inspection of a complete model of the total aviation system behaviour has the potential to identify a significantly more complete and correct set of monitoring requirements. A complete model of the total aviation system behaviour will also facilitate the better interpretation of observed events/results, incidents and accidents.

Use of the risk model to improve Management of Change

The risk model may be used to improve the Management of Change (a function of the Safety Management System. Inspection of a complete model of the total aviation system behaviour has the potential to improve the identification of the boundary of influence a proposed change to the system will have i.e. the extent to which the proposed change will impact on other systems and services.

Use of Continuous Oversight to improve confidence in the risk model

The risk model may be used to improve the confidence in the Risk Model by comparing the predicted performance and any assumptions expressed in the model with the actual performance of the system as determined through Continuous Oversight. It is envisaged that this will be an iterative process with corrective action as appropriate e.g. an update to the model, a reconsideration of any assumptions made or perhaps a change in the monitoring strategy.

Use of the risk model to determine the appropriate level of oversight

The risk model may be used to better inform the level of oversight. 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. Consider, for example, the role of regulation and the regulator. For example, is it required to have regulations to reinforce contracts to assure the behaviour of those upon which you may be dependant (as determined by inspection of the model) that are beyond one's own immediate influence (e.g. a supplier of a supporting service, such as ground handling and de-icing, contracted through a third party).

7 Conclusions and recommendations

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 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. In this paper, 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 previous accident model development work, primarily the work performed to create the Causal Model for Air Transport Safety (CATS). CATS has been developed for the Dutch Ministry of Transport and represents the total aviation system. The ESDs and fault trees of CATS are used as a starting point to create this risk model. 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 proposed 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.

The ASCOS risk model can be quantified by assessing the probability of occurrence of each of the different pathways in the scenarios. A quantified model gives a risk picture of the system that is described by the model, based on historic or expert opinion-derived data. It can be used to analyse the risk of individual events: for each event in the model the probability is known and the severity can be derived from the conditional probability of an accident given the said event occurring. The model can also be used to assess the impact on safety of changes to the system. Proposed changes can have an influence on the probability of occurrence of events described by the model. If this influence can be quantified, the model can be used to determine the quantitative influence of the change on accident risk. The model can also be expanded by adding new events that are specific to the particular change.

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. The only practical solution to this problem is to derive 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. 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.

Acknowledgement

This technical publication has been realized partly with funding from the European Commission, ASCOS Grant Agreement No. 314299. The support of the ASCOS consortium partners (see http://www.ascos-project.eu) and dr. Michael Kyriakopoulos, EC scientific officer for project ASCOS, is greatly appreciated.

8 References

1. ACARE. (2001). European Aeronautics Vision for 2020: Meeting society's needs and winning global leadership, Report of the Group of Personalities, Advisory Council for Aviation Research and Innovation in Europe.
2. Ale, B., Bellamy, L.J., Cooke, R., Duyvis, M., Kurowicka, D., Lin, P.H., Morales, O., Roelen, A., Spouge, J. (2009). Causal Model for Air Transport Safety: Final report. Directorate General of Civil Aviation and Maritime Affairs, Ministry of Transport, Public Works and Water Management, The Hague, Netherlands.
3. ASCOS D1.3 (2013). Outline proposed certification approach. [Online] available from http://www.ascos-project.eu.
4. ASCOS D2.2 (2013). Total aviation system baseline risk picture. [Online] available from https://ascos.projects.nlr.nl/, access restricted.
5. ATSB. (2004) ATSB Aviation Safety Survey- Safety Climate Factors, Aviation Research Paper B2003/01222, Australian Transport Safety Bureau, Canberra, Australia.
6. Balk, A.D., Montijn, C. (2010). Development of an aviation-wide safety culture assessment tool, paper presented at PSAM 10, Seattle, USA.
7. Borener, S., Trajkov, S., Balakrishna, P. (2012). Design and development of an Integrated Safety Assessment Model for NextGen, American Society for Engineering Management.
8. EASA. (2012). European Aviation Safety plan (EASp) (2012 – 2015), TE.GEN.00400-002, European Aviation Safety Agency, Cologne, Germany.
9. EASA. (2013) Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS-25, Amendment 13, Annex to ED Decision 2013/010/R, European Aviation Safety Agency, Cologne, Germany.
10. Eurocontrol (2006). Main report for the 2005/2012 Integrated Risk Picture for Air Traffic Management in Europe, EEC Note No. 05/06, Eurocontrol Experimental Centre, Brétigny-sur-Orge, France.
11. Eurocontrol (2008). Safety culture in air traffic management, a white paper, Eurocontrol/FAA Action Plan 15 Safety, European Organisation for the Safety of Air Navigation (Eurocontrol), Brussels, Belgium.
12. Eurocontrol (2009). ATM Safety Framework Maturity Survey, European Organisation for the Safety of Air Navigation (Eurocontrol), Brussels, Belgium.
13. European Commission. (2010a). Aeronautics and Air Transport: Beyond Vision 2020 (towards 2050), A Background Document from ACARE, European Commission, Directorate-General for Research, Directorate Transport, Brussels, Belgium.
14. European Commission. (2010b). Commission Regulation (EU) no 691/2010 of 29 July 2010 laying down a performance scheme for air navigation services and network functions and amending Regulation (EC) No 2096/2005 laying down common requirements for the provision of air navigation services. Official Journal of the European Union, 3.8.2010, pages L 201/1- L 201/22.
15. European Commission. (2011). Flightpath 2050: Europe's Vision for Aviation, Report of the High Level Group on Aviation Research, European Commission, Directorate-General for Research and Innovation, Directorate General for Mobility and Transport.

16. FAA. (1988). Advisory Circular AC 25.1309-1A, System Design and Analysis, 21 June 1988, Federal Aviation Administration, Washington D.C., USA.
17. FAA. (2002). The report on the FAA Associate Administrator for Regulation and Certification's Study on the Commercial Airplane Certification Process, Federal Aviation Administration, Washington D.C., USA.
18. FAST. (2012). The FAST approach to discovering aviation futures and associated hazards, Methodology Handbook, Future Aviation Safety Team.
19. FAST. (2013). Areas of Change Catalogue: Ongoing and future phenomena and hazards affecting aviation, compiled by the Future Aviation Safety Team, February 19, 2013.
20. Gordon, R., Kirwan, B., Perrin, E. (2004). Measuring safety culture in a research and development centre: A comparison of two methods within the Air Traffic management Domain, paper presented at the 23rd International NeTWork-Workshop "Safety Culture and Behavioural Change at the Workplace", Blankensee, Germany.
21. Hart, C. A. (2013). Presentation to Vaughn College of Aeronautics, New York, NY, on October 25, 2013. [Online] available from http://www.ntsb.gov/news/speeches.html [accessed 17 December 2013].
22. IAA (2011). Safety Culture and Safety Management Systems in Ireland, Safety Regulation Division, Irish Aviation Authority, Dublin, Ireland.
23. ICAO (2012). Safety Management Manual, Doc 9859, third edition, International Civil Aviation Organization, Montreal, Canada.
24. IRGC. (2010). The emergence of risks: contributing factors. International Risk Governance Council, Geneva, Switzerland.
25. Keller, W., Modarres. M. (2005). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry, a tribute to the late Professor Norman Carl Rasmussen, Reliability Engineering and System Safety, 89, p. 271-285.
26. Lewis, H.W., Budnitz, R.J., Kouts, H.J., Lowenstein, W.B., Rowe, W.D., Von Hippel, F., Zachariasen, F. (1979). Risk assessment review group report to the U.S. Nuclear Regulatory Commission, NUREG/CR-0400, U.S. Nuclear Regulatory Commission, Washington D.C., USA.
27. Lin, P.H. (2011). Safety management and risk modelling in aviation, Ph.D. Thesis, Delft University of Technology, Delft, the Netherlands.
28. Masson, M., Morier, Y. and FAST. (2012). Methodology to Assess Future Risks - Action EME 1.1 of the European Aviation Safety Plan (EASp), presented to the European Aviation Commercial Aviation Safety Team 4-12, 11-12-2012, EASA, Cologne, Germany.
29. Mearns, K., Whitaker, S., Flin, R. (2003). Safety climate, safety management practice and safety performance in offshore environments, Safety Science, 41, p. 641-680.
30. NASA. (2002). Fault Tree Handbook with Aerospace Applications, National Aeronautics and Space Administration, Office of Safety and Mission Assurance, Washington, D.C. USA.
31. NTSB. (1997). In-flight fire and impact with terrain, ValuJet airlines flight 592, DC-9-32, N904VJ, Everglades, near Miami, Florida, May 11, 1996. Aircraft Accident Report AAR-97/06, National Transportation Safety Board, Washington, D.C., USA.

32. NTSB. (2000). In-flight Breakup Over The Atlantic Ocean, Trans World Airlines Flight 800, Boeing 747-131, N93119, Near East Moriches, New York, July 17, 1996. Aircraft Accident Report AAR-00/03, National Transportation Safety Board, Washington, D.C., USA.
33. NRC. (1975). Reactor Safety Study, WASH-1400, NUREG –751014, United States Nuclear Regulatory Commission, Washington D.C., USA.
34. Reason, J. (1990). Human Error, Cambridge University Press, New York.
35. Reason, J. (1997). Managing the Risk of Organizational Accidents. Ashgate Publishing Limited, Aldershot, UK.
36. Roelen, A.L.C., Wever, R. (2005). Accident scenarios for an integrated aviation safety model, NLR-CR-2005-560, NLR Amsterdam.
37. SESAR. (2012). SESAR Reference Material, Edition 00.02.01, Project ID 16.06.01.
38. Sexton, J. B., Helmreich, R. L., Neilands, T. B., Rowan, K., Vella, K., Boyden, J., Roberts, P. R. and Thomas, E. J. (2006). The Safety Attitudes Questionnaire: psychometric properties, benchmarking data, and emerging research. BMC Health Services Research, 6, p. 44.
39. Thaden, T. L. von, Gibbons, A.M. (2009). The Safety Culture Indicator Scale Measurement System (SCISMS), Office of Aviation Research and Development, Federal Aviation Administration, Washington D.C.
40. TSB. (2003). Aviation Investigation Report, In-Flight Fire Leading to Collision with Water, Swissair Transport Limited, McDonnell Douglas MD-11 HB-IWF, Peggy's Cove, Nova Scotia 5 nm SW, 2 September 1998. Report Number A98H0003, Transportation Safety Board of Canada.
41. Traufetter, G. (2013). Fugzeug ohne Flügel, Der Spiegel, Issue 30/2013, p 26-29.
42. Vesely, W.E., Goldberg, F.F., Roberts, N.H., Haasl, D.F. (1981). Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington D.C., USA.