FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme / specialisation: MSc. Risk Management	Spring semester, *2023* Confidential
Author: Aneesh Somanpillai Vijayakumariamma	
Supervisor at UiS: Professor Lasse Berg Andersen	
Thesis title: On the treatment of risk/safety aspects within safety assessment of aviation	
Credits (ECTS): 30	
Keywords: Aviation Safety, Risk, SMS, ALARP, Acceptable Level of Safety, Regulation	Pages: 46 Stavanger, *June 2023*

ABSTRACT

Safety of aircraft is a hot topic due to the safety-critical nature of its operation and its significant negative impact it could pose to a larger society. In order to understand aviation safety in detail, it is important to understand how safety is considered at fundamental level historically and how it is incorporated in problem solving and decision-making process of recent times. In aviation, safety and risk are most often used interchangeably. Safety is used to represent overall condition of safety of the system of systems or the safe operation aspect of aircraft or aircraft as an integrated flightworthy system which needs to demonstrate safety in a regulatory point of view. Risk is the term used to represent or address extreme events having high impact potential which could possibly derail overall safety of aircraft or also Risk is a prospective concept whose careful implementation could help organizations to demonstrate and achieve safety in a longer period of time.

This thesis was approached with a generic literature survey which includes a summarized view on the risk implementation in aviation. The thesis considers Safety Management System as a framework with which safety is incorporated in aircraft. The thesis investigates various aspects of importance in aviation safety management area.

The overall question to be addressed is on how aspects of safety/risk is incorporated into aviation safety. The study revealed that the risk constructs are significant in aviation safety when it is applied through a standardized framework which is framed with the principle of safety at its core.

ACKNOWLEDGMENTS

This Master thesis was written in the spring of 2023 at the University of Stavanger, Department of Safety, Economics & Planning, under the supervision of Professor Lasse Berg Andersen. The work corresponds to 30 ECTS at University of Stavanger.

The purpose of this master thesis was to write on the generic treatment of risk/safety aspects within safety assessment of aviation.

The 30 ECTS workload for this master thesis was evenly distributed throughout the semester, following a project plan. The majority of the work was done in collaboration with literature survey from different sources.

I would like to express my sincere gratitude to Professor Lasse Berg Andersen, Department of Safety, Economics and Planning, University of Stavanger for providing me with the necessary guidance support throughout.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Aviation safety is a very dynamic concept. Since new safety hazards and risks are continuously emerging in aviation due to evolving nature of technological systems, there must be enough provisions to mitigate them appropriately. Safety systems historically to date have focused largely on individual safety performance and local control over similar category of aircraft, with minimal regard for the wider context of the total aviation system. This has led to growing recognition of the complexity of the aviation system and the different organizations that all play a part in aviation safety. There are numerous examples of accidents and incidents showing that most of the time the interfaces between organizations have contributed to negative outcomes rather than the individual components themselves.

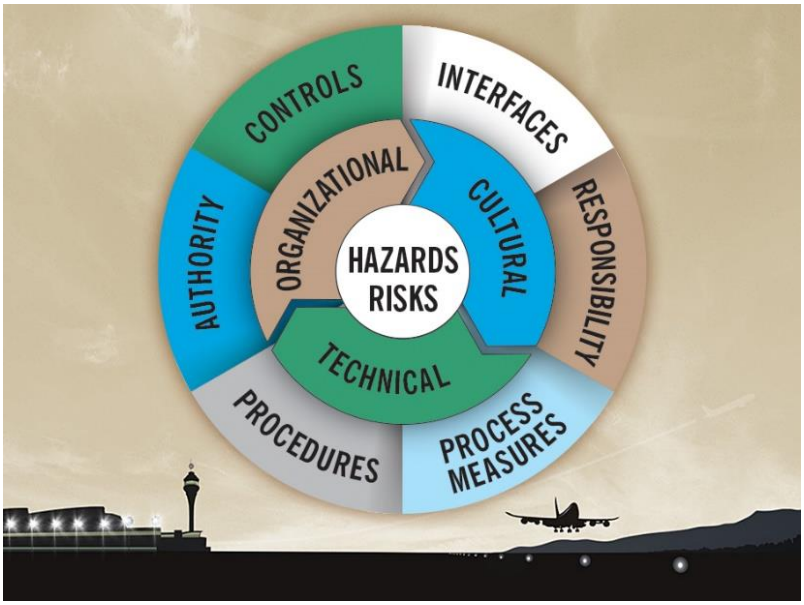

Figure 1 Aviation Safety- Broad factors influencing Hazards & Risks

(Ref: Aviation Safety & Regulations - M2C Aerospace, Inc.)

In a nutshell, in civil aviation, safety is typically influenced by the factors represented in Figure 1. Level of hazards and risks resulted in as the result of safety analyses are the factor which determines the overall level of safety towards achieving safety targets. The major factors influencing level of hazard and risk are the safety offered by technical aspects of the aircraft or aircraft systems, Organizational factors in achieving the safety, and cultural factors of perceiving safety. Organizational factors are determined by the organization's authority in achieving safety

and organization’s ability to apply controls to ensure a satisfactory level of safety. Technical factors are determined by the available procedures to achieve safety and capability in measuring the process’s ability in attaining safety target. Cultural factors are influenced by the type of interfaces connected with the system and responsibility of each interface towards ensuring safety of overall system.

Safety targets are one of the important performance constructs in the formulation of safety by regulatory agencies towards safety compliance purposes. A safety performance target composed of one or more safety performance indicators [14], together with desired outcomes expressed in terms of those indicators. Acceptable Level of Safety Performance (ALoSP) is "the minimum level of safety performance of civil aviation in a State, as defined in its state safety program, or of a service provider, as defined in its safety management system, expressed in terms of safety performance targets and safety performance indicators". Safety targets to be met to be eligible for certification of aircraft as a system are usually defined by regulatory agencies through their safety requirement document declaration. In civil aviation, the industry or airline handles the responsibility or accountability of the respective system safety of their system that they are dealing with. They make individual safety assessment plans to meet requirements put forth by regulatory agencies. Regulating airworthiness authorities are responsible for development of broad definition of safety requirements to satisfy at the end. Then it is only a matter of checking the adequacy of the individual system level safety assessments which are made by industries to justify compliance with overall aircraft safety requirements. In civil aviation, International Civil Aviation Organization (ICAO) is responsible for ensuring commonality among international agencies towards common requirement of aviation safety. ICAO Doc 9859 - Safety Management Manual [11] defines goals or objectives towards aviation safety. The safety performance targets are determined during its planning phase.

In aviation context, safety is a state in which the risk to harm to persons or damage to assets or loss due to unexpected event is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management. Safety is an emerging characteristic. Whereas safety management is the comprehensive process of addressing those safety-risks that emerge during integration or management of operations of technical systems with financial, security and human factor element additions to it. What is intended to achieve with a

safety management system is to put the proven safety management process together in a sound framework so that the processes work as a system to enhance the safety, efficiency, and effectiveness of the operation. The desire is to anticipate the hazards systematically and proactively, and thereby take the surprises out by making appropriate and effective risk management decisions. A clearly defined framework of safety objectives, polices, procedures and accountabilities are required for the proper implementation of SMS [20].

This thesis further investigates on the risk management importance or how risk assessment techniques are leveraged in its journey towards realizing the overall safety of the aviation system or in achieving compliance requirements imposed by regulating agencies. In aviation, safety implementation in reality supersedes many folds than just merely achieving safety clearance level. But for compliance safety is required to be demonstrated. Only for that purpose safety is limited to a framework level of implementation to bring a systematic approach to safety journey.

1.1 RESEARCH OBJECTIVES

1. Investigate on how risk management constructs are incorporated in aviation safety?
2. What are the available frameworks used for safety or risk assessment of aircraft?
3. Discuss the issues of relevance pertinent to aviation safety when aircraft is considered as a system.

1.2 SCOPE OF THESIS

The scope of thesis is a general perspective on how risk or safety management is being incorporated in aviation safety area and its issues, without delving too much into sophisticated risk or safety treatments. The thesis can be utilized to get an overall perspective rather than as a reference combined source of information for various risk assessment techniques applicable in aviation arena. This thesis points out only major risk assessment techniques generally applied across aviation safety management area. The terms Safety and Risk are used interchangeably as per its contextual significance in this thesis.

2 LITERATURE STUDY

During the earlier days of aviation, piston and propeller driven aircrafts were the majority and accidents at those times were caused due to individual equipment failures. Later turbo-jet airplanes become the mainstay. During this transition, there has been a substantial improvement in the incidents due to equipment failures mainly due to the emergence of fail-safe systems together with the implementation of lessons learned from the past. The more sophisticated the systems became, the more robust the design resulted with the implementation of more advanced control systems. But many accidents in those modern times were due to the mismanagement of the control systems by flight crew.

Figure 2 illustrates typical interaction elements for a complex-socio technical system. In a complex system, it is not only individual elementwise excellence is expected, but also the overall safety through the consideration of all the associated elements and their interactions between them [7].

Figure 2 Example for elements of a complex-socio technical system

The objective of performing literature study is to understand existing issues faced by aviation especially with respect to ensuring safety to aircraft or systems.

2.1 CHALLENGES IN ENSURING SAFETY OF AVIATION SYSTEMS

The challenge associated with complex emerging systems is the lack of widespread or upfront cause-consequence understanding of the principles and techniques of modern systems. In that context, towards addressing safety of complex emerging aviation systems, risk-based

considerations [3] have significant opportunities to provide an extra informed risk picture to regulators on top of existing standardized approaches towards certifying aircraft systems.

Existing standards in general works with an approach of safety assessment of aircraft systems through implementation of specific methods or means adopted to comply with requirements which would lead to overall safety of aircraft. In civil aviation, the industry or airline handles the responsibility or accountability of the respective system safety of their system that they are dealing with. They make individual safety assessment plans to meet requirements put forth by regulatory agencies. Regulating airworthiness authorities are responsible for development of broad definition of safety requirements to satisfy at the end. Then it is only a matter of checking the adequacy of the individual system level safety assessments which are made by industries to justify compliance with overall aircraft safety requirements.

In a modern aircraft with its complex interconnected systems, the safety of aircraft can only be achieved through the assessment of individual system level and combined system level [7], thorough assessment of potential failures together with a quantification of the extent or degree of hazard resulting from such failures. The quantification of failure probability estimates will be an ideal prospect to certifying agencies. Based on prior understanding of the existing safety level of aircraft in general, the authorities declare the new requirements to meet, as a formal safety objective to be met in order to enable the aircraft to be declared as a safe one. One example of such an objective to meet is that "New designs of new civil transport aircraft should be able to achieve a fatal accidental rate of better than one in 10 million operational hours from all systems causes combined or individually". To demonstrate such a safety objective the airline or industry investigates individual systems in its features to have a single or combined probability of exceedance potential through a risk assessment technique of choice. In general, the safety overrun of aircraft can be caused due to negative externalities in the form of potential material limitations (fatigue, creep, fracture), immature design philosophy (ice formation, lightning strikes, foreign object damage), unattainable manufacturing considerations, poor maintainability considerations in design, or uncertain human errors made by crew of airline or maintenance personnel are the potential drivers causing safety issues in aircraft away from its certified state. Figure 3 depicts some of the factors affecting aviation safety. Hence the system owners must consider of these factors early in the design stage to achieve a reasonable margin in target level of safety. Hence the

safety problem changes from risk assessment to risk management considerations [3]. To determine whether a safety assessment is necessary and to what depth that it should be, the designer normally conducts “Preliminary Hazard Analysis” in which all possible hazards emanating from system, or its functionality will be understood. After preliminary hazard assessment, the designer would get an idea on which critical features that needs more intense evaluation of safety assessment. All such early discoveries of all possible negative externalities through risk assessment that could derail the safety target must go back to the design space as design safety constraints to satisfy during design, manufacturing, and operation of the aircraft. This later leads to detailed instructions in the form of checklists to be followed while operating or taking care of aircraft through in its entire lifecycle stages.

Safety assessment of aviation systems begins prior to its design stage itself to incorporate lessons learned from the overall safety assessment as an advantage in the form of mitigating compliance risks. So, the context of investigation of safety assessment standards or techniques in literature is directed towards both techniques of safety assessment of systems as well as safety assessment of the aircraft. In existing scenario, the aircraft critically depends upon the individual system safety towards overall safety. Safety of aircraft is not an individual responsibility but a collective effort of civil aviation, international agencies, industries, academia, etc.

The modern civil aviation started to shape in 1940’s to 1950’s time frame. In those days, the aviation systems were simple in design and operating principles. They had very minimal electronic devices and most of the systems were very reliable mechanical devices. Their operation was not of a crucial concern in respect of safety. There was a higher level of system level interaction independence considerations in those systems in their construction and operation. Hence the failure of one component or system had less impact on the safe operation of others. The airworthiness requirements of the world at that time were aligned based on circumstances. Separate requirement sets were stated for each system and engineering detail were relied on to obtain sufficient system reliability. For those systems which had the potential to create a hazardous event in the case of a failure (single event failure) were addressed through duplication of the primary systems in the form of extra redundant or parallel system arrangement. Compliance at that times were demonstrated through engineering analysis. Failure mode and effects analysis (FMEA) were utilized to supplement the engineering analysis to assess the impact of single event failures. There were less

considerations given at those times to quantify the combined failure events. Also, compliance requirement considerations by authorities towards likely frequency of occurrences of failures were negligible.

In current civil aviation scenario, there exists a significant amount of complex electronic devices which are cross-coupled through fly-by-wire technology. The fly-by-wire technology replaced old mechanically driven concepts. This critical innovation caused a sudden leap in the emergence of new age complex systems. In such a scenario, the analyst is thus faced to perform safety analysis of each system, but also of its independent actions or combined actions. Thus, the earlier way of addressing safety through duplication of only primary systems were in principle has become an uncertain way of dealing with safety. Complex systems were so innovative and had the potential to favorably influence the concept of economy flying. Complex systems posed a challenge to define appropriate requirements to certification authorities. This concern gradually led to the adoption of the principle of acceptable level of safety, in the form of probability of fatal accident due to dependent or single event failures. As part of the broad objective form of requirements statement to the industries with the help of acceptable level of safety requirements, the regulatory authority stayed away from intervening the design freedom of engineers to fully utilize their technical capability to innovate the system to a sophisticated level that is desired. Today, both American and European agencies adopt a broad objective-based safety requirements definition.

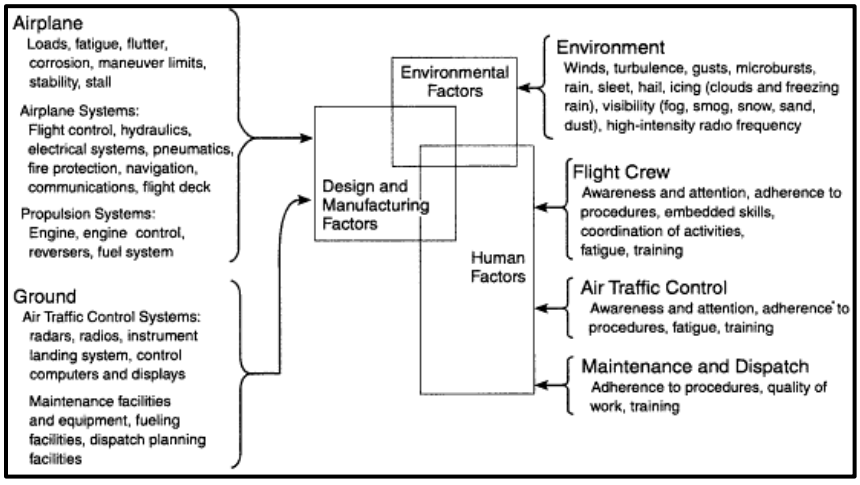

Figure 3 Aviation technical safety contributing factors

(Ref: https://www.nap.edu/openbook/0309061857/xhtml/images/img00012.gif)

Figure 3 provides an overall information on the technical dimension of safety or risk contributing factors to overall safety of aviation. The safety contributing elements of Design and manufacturing factors includes air-based elements and ground-based elements. Environmental factors-based safety contributing elements are based on the operating environment-based issues. Human factors are another factor which has largest uncertainty-based contribution to safety of aviation systems. Human factors can influence an organization's safety in both positive and negative ways. Consideration of human factors [13] is an integral part of safety management and is necessary to understand, identify and mitigate risks and optimize organizational safety [23].

2.2 TRADITIONAL APPROACHES TO SAFETY

In the traditional approach to safety, when an accident event occurred, the typical questions investigated were:

- How and why did the circumstances led to the accident?
- Could similar accident happen again?
- How could the similar accident be avoided in future?

In the past, it was often the practice of investigators to examine the chain of events or circumstances that led to some random failure event or someone doing something inappropriate, thereby triggering the accident. Such inappropriate error mostly be due to judgment error, or an inattention error (error that may have been related to a heavy workload or preoccupation with another activity, or a deviation from standard operating procedures (SOPs)). The investigation usually tends to put blame on operators for the unfortunate incident instead of focusing on the root cause of the incident. Most of the time there would be wrong managerial practices that would lead to a safety incident rather than the procedures followed by operators. The safety management efforts are mostly concentrated on eliminating human error through a management strategy.

Poor pilot training, not windshear, was at fault in the recent Lion Air crash in Indonesia, raising concerns about human error and the role it plays in air crashes. Another example is the issue of runway incursions. In the past, runway incursions may have been attributed to human error. The pilot failed to adhere to the clearance and entered the runway without clearance, or the Air Traffic Controller (ATC) made an error when he or she issued the clearance.

The errors or violations that trigger accidents often occur randomly. With no historical data to support on the specific incident, usual safety management efforts to reduce or eliminate random events are usually ineffective. Human being human are expected to produce mistakes due to various reasons. Even the best workforce is not far away from a bad day to cause an error. Hence, in general it is unrealistic to try to eliminate human error. Rather, the best approach is that we need to predict how error can occur, and how to manage the circumstances to reduce the probability of those errors, and to manage the results when they do occur. In general, the focus moves from human error to human factors [26].

Analysis of historical accident data [8] often reveals that accidents doesn't happen out of thin air. There would be sufficient indicators before a major accident. Most often there exists safety situations that are the consequence of decisions made by management. They recognized the systemic risks, but other priorities required a trade-off action from their side. At other times, the hazards and risks are not properly recognized by the decision-makers. Indeed, front-line management personnel often work in a context that is already set by organizational and management factors beyond their reach of influence or direct control.

Due to these above discussed reasons, to be successful in ensuring safety, safety management systems required to be implemented.

2.3 CHANGES OBSERVED

Knowledge from the past twenty years indicates that accidents are related to breaches of the defenses that are established to manage the hazards and associated risks inherent in a specific operation or in the aviation industry as a whole. The Accident Causation Model developed by Professor James Reason is a graphic depiction of this accident causation understanding. This model recognizes that most accidents are due to organizational issues.

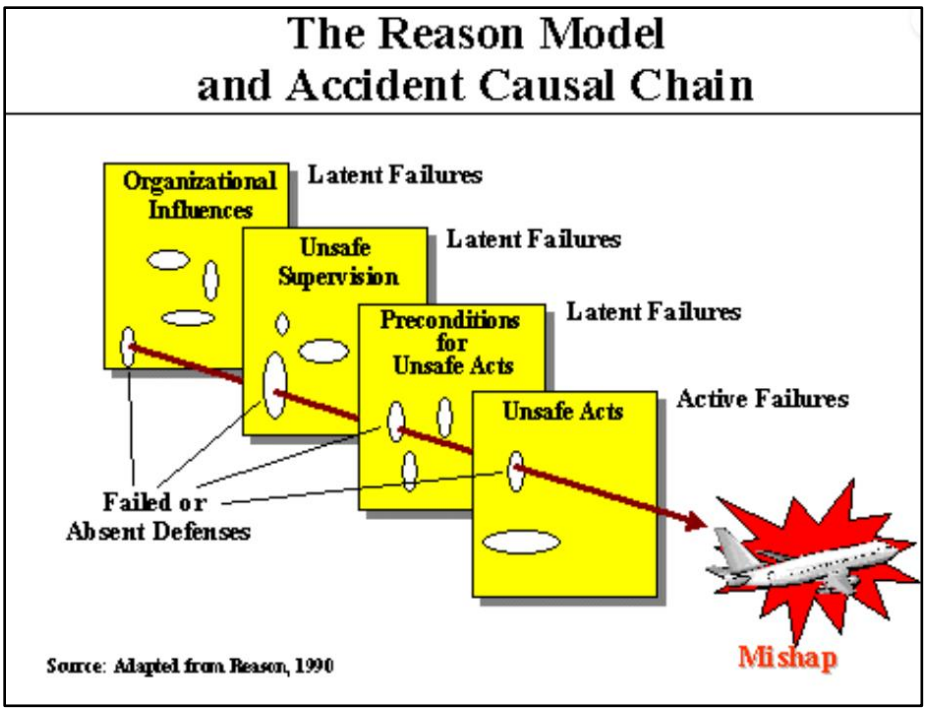

Figure 4 Reason's Model for Safety Management [12]

The above image depicts the importance that the Decision Makers in a company with an SMS must be aware that there are hazards and associated safety risks present in the system, so they can develop and implement relevant policies and make appropriate decisions to manage (mitigate or control), the known hazards and associated risks. Line Managers then implement the policies and decisions and develop and implement procedures within the same objective.

Often not all of the hazards and associated risk have been identified or correctly understood. These constitute the latent conditions that often are the system safety deficiencies that permit the hazards to exist quite often. System safety deficiencies are the circumstance that permits hazards of a similar nature to exist. Various defenses are built into the system to protect against inappropriate performance, poor decisions, or other threats to the safety of the system. The above model also recognizes the fact that the decisions that created as defenses can also create certain latent conditions that could lead to an accident. The latent conditions exist because of issues such as poor design, gaps in supervision, undetected defects or maintenance failures, unworkable procedures, poor training, conflicting goals, and objectives, etc. They then combine with, or cause, active failures, such as errors or violations of procedures that produce an accident. These latent conditions may have their origin in management decisions that were made with good intentions and were

based on the best available information but have unintended consequences. When the failures in the defenses left by the latent conditions line up with the active failures, the defenses are breached, and an accident or incident can occur. In this way, we can see how the four terms we used to understand risk management (i.e., system safety deficiencies, hazards, risk, and mitigation), map out on James Reason's Swiss-cheese model of accident causation. We can clearly see that we need a system to manage hazards and risks to reduce the likelihood of an accident from occurring.

The real world of aviation is not as simple as the two-dimensional depictions of Figure 4 model. Rather, it is a complex interaction between systems, each with their own latent conditions and potential for active failures. A typical aviation operation with sub-systems involving aircraft operations, aircraft, maintenance, dispatch, air traffic control, airports, Fixed Base Operators (FBOs), etc. suddenly doesn't appear as simple as we may believe.

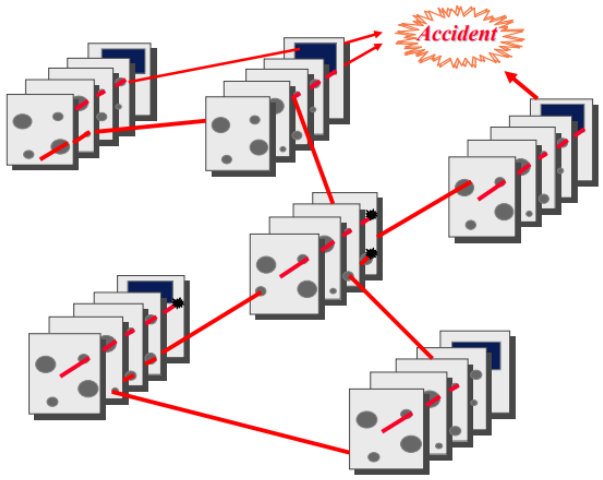

Figure 5 Complex system of systems interaction model in aviation

There are always some precursors to accidents. Figure 6 illustrates the pyramid structure on the idea of the accident ratio historically seen from various industries. This is generated as a rough estimate looking at the vast historical data and knowledge from accident investigations from several industries. A fatal accident is at the tip of the iceberg. Below the tip lie precursors that may include a few accidents involving serious injury, a number of accidents involving property damage, numerous related incidents with no injury or damage and a host of latent conditions. All too often these precursors are only recognized after an accident. These precursors, or latent conditions, can be identified through an objective, in-depth hazard identification and risk management process.

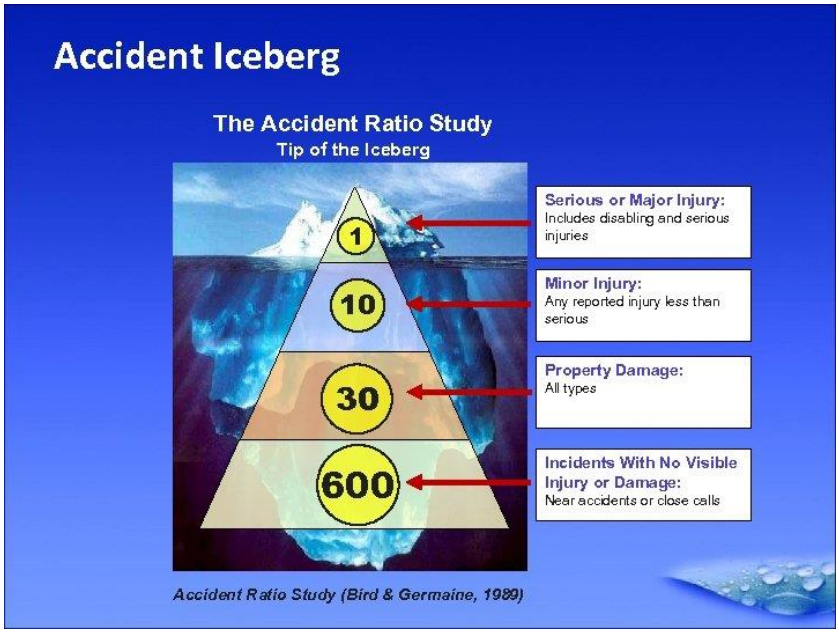

Figure 6 An statistic towards accident emergence

In summary, Accidents and incidents occur within a defined set of circumstances and conditions. These include the aircraft and other equipment, the weather, the airport, and flight services, as well as the regulatory, industry and corporate operating nature. They also include the permutations and combinations of human behavior. At any given time, some of these factors may align in such a way as to create conditions that are ripe for an accident. Understanding the context in which accidents occur is fundamental to safety management. Some of the principal factors shaping the context for accidents and incidents include equipment design, supporting infrastructure, human and cultural factors, corporate safety culture and cost factors.

2.4 BETTER UNDERSTANDING OF SAFETY

The aviation community has historically experienced a very low accident rate as compared to other safety-critical industries. That safety record has largely been the result of successes in a series of technological advances and operational and regulatory activities. To sustain safety at this exceptional level as aviation activity increases, safety management practices are shifting from a reactive mode to a more proactive mode. In doing this a number of factors have been found to be effective. They include:

- Commitments from senior management level to the management of safety,

- Application of scientifically backed risk management methods,
- Corporate safety culture that fosters safe practices, encourages safety communications, and actively manages safety with the same attention to results as financial management,
- Implementation of standard operating procedures (SOPs), including the use of checklists and briefings,
- A just culture or non-punitive environment to foster effective incident and hazard reporting activity,
- Implementation of systems to collect, analyze and share safety-related data arising from normal operations,
- Competence in investigation of accidents and serious incidents identifying systemic safety deficiencies, rather than just targets for blatant blame,
- Safety training integration, including human factors, for operational personnel,
- Sharing of safety lessons learned and best practices through the active exchange of safety information among companies and regulatory authorities, and
- A systematic safety oversight and performance monitoring aimed at assessing safety performance and reducing or eliminating emerging problem areas.

The standalone implementation of these element cannot meet today's expectations for risk management. Rather, an integrated application of these elements will reduce the occurrence of unsafe acts and improve the management of latent conditions within a safety critical operation. However, it must be understood that while effective safety management will significantly reduce the risk of an accident, there can never be a guarantee that all accidents will be prevented through its implementation. Attaining a risk and hazard-less environment is highly impossible especially when humans use highly complex technological systems to provide aviation services.

2.5 TYPICAL AVIATION SYSTEM-LEVEL FAILURE TYPES

- Single event or single active failure
- Combination of independent failures
- Common-mode failures
- Passive and undetected failures
- Cascade failures

- Environment-induced failures

Single event failures are catastrophic consequence producing failures. For example, engine failure or jamming of controls by foreign objects, the asymmetry of control surfaces actuation caused by fracture of linkage mechanisms, runaway of hydraulic or electrical actuators, misbehavior of propeller pitch characteristics, etc. On 4th October 1962, a malfunction of the electric elevator trim tab unit resulted in aircraft uncontrollability and subsequent structural failure of the wing of Lockheed Lodestar 18 aircraft.

Even though redundancy is built into the system, there still exists probability of multiple failures. Such failures need careful assessments. There could be combinations of active failures such as multiple failures of engine, or electrical generators, or hydraulic systems. The failures need not necessarily be limited to the same system. Standalone failure in one system could cause a failure in another system in an independent way. For example, in the event of a single engine failure in a twin engine aircraft, the asymmetry in engine power causes directional instability to aircraft or an unwanted yawing moment to aircraft causing it to change the heading. To avoid the yaw due to loss of one engine power, the aircraft must produce an equal and opposite yawing moment through flight controls, especially with rudder control. A failure in hydraulic system components causes lack of availability of hydraulic fluids in the rudder actuators which leads to inoperability of rudder unit. Such combinations of independent failure events could produce a fatality. The assessment of such combinations independent failure events requires a strong knowledge of aircraft systems and its operations.

Common mode failures are caused by a single root cause failure event triggering failure of similar functioning systems. For example, electrical systems in fly-by-wire flight-control based aircrafts are affected by electromagnetic or electrostatic interference causing failure or jamming of devices. To avoid such eventuality electrical systems are usually driven by a ram air turbine to cover the losses produced by multiple engine failures.

Passive and undetected failures occur with little or no warning or indication. Such undetected failures may or may not lead to an immediate accident event, but the failure can occur gradually over time if it remains undetected during periodic inspection or maintenance activities. For example, in a multi-channel redundant system, the failure of one channel of electrical or hydraulic supply should not cause any harm provided that the flight crew is informed of such an anomaly

with a cockpit warning or indication. Modern aircrafts are equipped with flight control computers to disconnect automatic controls in the event of a malfunction or to give sufficient warning indications to pilot when dangerous conditions emerge. Routine pre-flight checks have the potential to identify some of the dormant failure modes within the system. The consideration of such failure plays an important part in the safety assessments. Cascade failures are caused by a non-harming single failure triggering multiple connected failure events. Lightning strikes are one example for failure induced by environment.

Some of the negative externalities that affect the safety of aviation systems mentioned by "World airline accident summary" are as below,

- Design errors
- Errors in manufacturing or maintenance
- Pilot mismanagement of established procedures
- Inadequate incorporation of environmental conditions in design
- Wrongful intentional actions from people involved

2.6 HISTORICAL MEASURES OF SAFETY

Now if we look at what are the historical measures that were adopted to measure the safety of aviation systems.

1. Allocation of shares of accident and focusing on major ones:

   Bo Lundberg of Sweden recommended the idea that the best way to seek to control the overall accident rate would be to allocate shares to the main classes of accident and then try to control each contributing one. This is one technique often used in the practices of Airworthiness authorities. Here total accident rate is seen as sum of the accident arising from a variety of causes.

   As can be seen in the below table, only 12% of fatal accidents were caused due to system issues. About half of the catastrophic accident caused are attributed due to operational aspects. Pilot error and poor system design are the major reason for operational issues. Pilot induced errors can be very well accommodated through better design philosophies.

Accident type	Fatal	Total	Fatal/Total
System specific			
Airframe structural failure	1	21	5
Fire (Cabin, Toilet, etc)	2	7	29
Landing gear failure	1	20	5
Landing gear mechanism failure	0	13	0
Engine fire/failure	5	58	9
System failure	7	14	50
Operational specific			
Bird strikes	3	19	15
Weather	6	18	33
Striking high ground	14	14	100
Undershoot	23	45	51
Overshoot/Over run	4	28	14
Heavy landing	2	23	9
Miscellaneous	8	42	19
Total	**76**	**338**	**23**

Table 1 Types of accident- Passenger jet aircraft

2. Fatal accident rates:

FAR is one of the common historical indicators of lack of safety of system. Fatal accident data is reliable measure since it was brought to attention of a larger audience due to its severity as compared to a just a record of historical accidents. There is a positive sense of trustability of the information content in them. But as per the definition of a fatal accident "one in which one or more people are killed in 1 million flight hours" leaves no room for varying interpretation possibility of what constitutes such an accident. If the fatal accident rate fell from 2 per 1 million flying hours in 1960s dropped to 0.5 per 1 million flying hours in 1990s, it sends a wrong sense of safety feel to common people. But this change could be due to a safety performance improvement in technology from piston-engine propeller aircrafts of 1960 to modern turbo powered jet aircrafts. So usually, time dimension or technological advancements are completely neglected in FAR. Also, as compared to 1960s

aircrafts flying hours, modern aircrafts can fly more hours. So, the FAR reduction of 0.5 from 2 could also be due to a large flying hour which could lead to a false safety perception. Also, there is a mixture effect in fatal accident rates due to diversity of aircrafts available in modern times as compared to limited historical aircrafts. Another issue is that in 1960s only technical excellence of the system was a major contributor of safety and the operational characteristics or handling characteristics of the aircraft was not so significant, but in modern times handling characteristics of aircraft is vital due to the complexity of operations the aircrafts are being subjected to. Usually when an aircraft gets damaged (complete loss of structural integrity, Substantial damage, Minor damage) the next possible sequence is that it results in a fatality. FAR doesn't incorporate information on the condition of aircraft at the time of accident or afterwards an accident. In other words, the situation which led to accident, or the post-accident severity is not at all evident from the FAR measures.

Another challenge of using FAR in design stage is that FAR measure looks back into history and makes inferences for present, but a better and more suitable approach would be to look at future to make inferences for present. For example, when the current system becomes a reality in future what would be the consequences or limitations and how to mitigate such a scenario or in other words what accident rates would be practicable to use now for a futuristic level of safety performance. This doesn't mean that historical developments on the system under consideration is not useful. Any technical system gets to its refined level due to improvements done upon them with the understandings of the past experiences of working with them. That learning curve is of course unavoidable. But one must be able to remove historical noise mentioned above while utilizing such a knowledge for future applications. Hence FAR is not a good measure to use.

3. Failure Rates and probabilities:

   Failure rates and probability measures are commonly used to describe a technical failure. For example, to describe Fatigue or wear-out failures. They exhibit a time dimension effect in their failure event behavior.

Rates are the long-term average frequency measure. Such a measure is adopted where the cause of accident is such that there is no reason to believe that its likelihood of occurrence varies from flight to flight. In such a scenario the rates and probability are the same. An accident rate of 1 per 10^7 hours correspond to an accident probability of 10^7 per hour. There exists a scenario where though the overall failure rate is low, the probability of failure due to the age of the system is very high.

MTBF (Mean Time Between Failures) is used as a good approximation to failure rate or probability under normal loading conditions of aircraft. It is not a good indicator of failure rate under added load conditions.

2.7 INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)

International Civil Aviation Organization (ICAO) is the nodal agency responsible for ensuring civil aviation safety by acting as a global agency combining several states and country-based aviation organizations thereby issuing commonly acceptable recommendations between each participatory states in a systematic fashion. The ICAO exercises its regulatory functions continuously. ICAO establishes standards or amend the existing standards in response to developments in the civil aviation market, advanced technology, and growth in aviation transport worldwide. ICAO defines recommended practices towards its contracting states in ensuring safety. Recommended Practices are any specification for physical characteristics, configuration, material performance, personnel or procedure, the uniform application of which is recognized as desirable in the interest of safety, regularity, or efficiency of international air navigation and to which Contracting States will endeavor to conform in accordance with the Convention. The recommended practices are also known as “Soft Law”.

The ICAO is an inter-governmental organization formulated to provide safe and orderly international air transport by establishing certain principles and arrangements. It is envisioned with norm-setting powers by an international treaty, i.e., the Chicago Convention (1944). Nineteen Annexes, which contain the Standards and Recommended Practices (SARPs) [12] regarding the safety and security of civil aviation, have been developed by the ICAO to establish a high degree of technical uniformity to develop civil aviation in a safe, efficient, and orderly manner [11]. ICAO flight safety management deals with safety and security dimensions towards flight safety. The

concepts of safety and security refers to different types of dangers. The concept of safety is defined in the ICAO Safety Management Manual as; “the state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management” [10]. The main focus of aviation safety regulations is on “preventing accidental harm”. Annex 17 regulates aviation security by safeguarding international aviation against acts of unlawful interference. Therefore, the security measures regulated in Annex 17 focus on “preventing intentional harm” carried out by an individual/individuals.

3 AVIATION SAFETY

3.1 SAFETY MANAGEMENT SYSTEM IN AVIATION

Existing safety governance systems prior to incorporation of SMS were static in the sense of not able to incorporate all sorts of airborne devices of any size and capacity. SMS is an effort to standardize the efforts of assuring overall safety improvements. Aviation systems are unique technical systems which poses joint air and ground-based threat scenario in a socio-technical environment where less margin of error is tolerable. Hence, rather than standalone risk assessments there is a need to incorporated risk-based governance. There are several instances where entire aircraft program is put on hold or scrapped due to unexpected and unanticipated safety incidents which put public sentiments against it. Being a high consequence probable socio-technical system, the regulators face significant challenges to meet the safety standards due to its emerging nature of risks and regulatory challenges due to not able to generalize or authoritatively state a full technical boundary to enable them to generalize the approval process as a standardized approach. Airworthiness certification is the existing approach regulators adopt to certify the aircraft systems and aircraft.

The challenge associated with emerging systems were the lack of widespread or upfront cause-consequence understanding of the principles and techniques of modern systems. In that context, towards addressing safety of complex emerging aviation systems, risk-based considerations have significant opportunities to provide an extra informed risk picture to regulators on top of existing standardized approaches towards certifying aircraft systems.

Existing standards in general works with an approach of safety assessment of aircraft systems through implementation of specific methods or means adopted to comply with requirements which would lead to overall safety of aircraft.

Safety assessment of aviation systems begins prior to its design stage itself to incorporate lessons learned from the overall safety assessment as an advantage in the form of mitigating compliance risks. So the context of investigation of safety assessment standards or techniques in literature is directed towards both techniques of safety assessment of systems as well as safety assessment of the aircraft. In existing scenario, the aircraft critically depends upon the individual system safety

towards overall safety. Safety of aircraft is not an individual responsibility but a collective effort of civil aviation, international agencies, industries, academia, etc.

The modern civil aviation started to shape in 1940's to 1950's time frame. In those days, the aviation systems were simple in design and operating principles. They had very minimal electronic devices and most of the systems were very reliable mechanical devices. Their operation was not of a crucial concern in respect of safety. There was a higher level of system level interaction independence considerations in those systems in their construction and operation. Hence the failure of one component or system had less impact on the safe operation of others. The airworthiness requirements of the world at that time were aligned based on circumstances. Separate requirement sets were stated for each system and engineering detail were relied on to obtain sufficient system reliability. For those systems which had the potential to create a hazardous event in the case of a failure (single event failure) were addressed through duplication of the primary systems in the form of extra redundant or parallel system arrangement. Compliance at that times were demonstrated through engineering analysis. Failure mode and effects analysis (FMEA) were utilized to supplement the engineering analysis to assess the impact of single event failures. There were less considerations given at those times to quantify the combined failure events. Also, compliance requirement considerations by authorities towards likely frequency of occurrences of failures were negligible.

In current civil aviation scenario, there exists a significant amount of complex electronic devices which are cross-coupled through fly-by-wire technology. The fly-by-wire technology replaced old mechanically driven concepts. This critical innovation caused a sudden leap in the emergence of new age complex systems. In such a scenario, the analyst is thus faced to perform safety analysis of each system, but also of its independent actions or combined actions. Thus, the earlier way of addressing safety through duplication of only primary systems were in principle has become an uncertain way of dealing with safety. Complex systems were so innovative and had the potential to favorably influence the concept of economy flying. Complex systems posed a challenge to define appropriate requirements to certification authorities. This concern gradually led to the adoption of the principle of acceptable level of safety, in the form of probability of fatal accident due to dependent or single event failures. As part of the broad objective form of requirements statement to the industries with the help of acceptable level of safety requirements, the regulatory

authority stayed away from intervening the design freedom of engineers to fully utilize their technical capability to innovate the system to a sophisticated level that is desired. Today, both American and European agencies adopt a broad objective-based safety requirements definition.

In a modern aircraft with its complex interconnected systems, the safety of aircraft can only be achieved through the assessment of individual system level and combined system level, thorough assessment of potential failures together with a quantification of the extent or degree of hazard resulting from such failures. The quantification of failure probability estimates will be an ideal prospect to certifying agencies. Based on prior understanding of the existing safety level of aircraft in general, the authorities declare the new requirements to meet, as a formal safety objective to be met in order to enable the aircraft to be declared as a safe one. One example of such an objective to meet is that "New designs of new civil transport aircraft should be able to achieve a fatal accidental rate of better than one in 10 million operational hours from all systems causes combined or individually". To demonstrate such a safety objective the airline or industry investigates individual systems in its features to have a single or combined probability of exceedance potential through a risk assessment technique of choice. In general, the safety overrun of aircraft can be caused due to negative externalities in the form of potential material limitations (fatigue, creep, fracture), immature design philosophy (ice formation, lightning strikes, foreign object damage), unattainable manufacturing considerations, poor maintainability considerations in design, or uncertain human errors made by crew of airline or maintenance personnel are the potential drivers causing safety issues in aircraft away from its certified state. Hence the system owners must consider of these factors early in the design stage to achieve a reasonable margin in target level of safety. Hence the safety problem changes from risk assessment to risk management considerations. To determine whether a safety assessment is necessary and to what depth that it should be, the designer normally conducts "Preliminary Hazard Analysis" in which all possible hazards emanating from system, or its functionality will be understood. After preliminary hazard assessment, the designer would get an idea on which critical features that needs more intense evaluation of safety assessment. All such early discoveries of all possible negative externalities through risk assessment that could derail the safety target must go back to the design space as design safety constraints to satisfy during design, manufacturing, and operation of the aircraft. This later leads to detailed instructions in the form of checklists to be followed while operating or taking care of aircraft through in its entire lifecycle stages.

The implementation of safety management requires some consideration to be given to the pre-requisites that should be in place, the development of a good system description, including both internal and external interfaces, and the size and complexity of the organization in order to ensure effective results. When establishing or maintaining any system, States and service providers should ensure they have considered three basic elements – people, process, and technology, and, most importantly, how they will work together to enable the organization to meet its safety objectives.

A safety management system consists of a safety management strategy which includes the safety objective, safety policy, procedures, and accountabilities. According to strategy, all hazards, and associated risks inherent in the operation are identified and assessed continuously and a Safety Risk Profile is developed. Then a mitigation or control plan is developed, to either eliminate the hazards or reduce the associated risk to a level as low as reasonably practicable (ALARP) level [1]. This Strategy is then implemented through programs, procedures, and training as appropriate. These are the Safety Management Activities. Safety assurance activities including the feedback from tracking the appropriateness and effectiveness of safety management activities, through the identification of additional hazards and the results of audits, safety reviews and SMS evaluations, all provide the information that is analyzed and used to adjust the Safety Risk Profile, Safety Management Strategy and Safety-risk Management.

In safety-risk management, safety is all about understanding and identifying Hazard and Risk management is all about implementation of frameworks and approaches towards treatment of risks once hazards are identified. In an effort to manage the safety of an operation and reduce the likelihood risk of an accident, concerned authority must effectively manage the risks associated with any hazard that cannot be eliminated. It is important to have a clear understanding of several terms and how they are used interchangeably in safety management contexts.

ICAO has described a safety management system as being composed of four components with 12 elements. They are as shown in Figure 7:

1. Safety Policy and Objectives
    1.1 Management commitment and responsibility
    1.2 Safety accountabilities
    1.3 Appointment of key safety personnel
    1.4 Coordination of emergency response planning
    1.5 SMS documentation
2. Safety Risk Management
    2.1 Hazard identification
    2.2 Safety risk assessment and mitigation
3. Safety Assurance
    3.1 Safety performance monitoring and measurement
    3.2 The management of change
    3.3 Continuous improvement of the SMS
4. Safety Promotion
    4.1 Training and education
    4.2 Safety communication

Figure 7 Twelve elements of ICAO safety management system [10]

3.2 SAFETY-RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEM

Safety-risk management is one of the important elements of Safety Management System defined by ICAO. In safety-risk management, safety is all about understanding and identifying Hazard and Risk management is all about implementation of frameworks and approaches towards treatment of risks once hazards are identified. In an effort to manage the safety of an operation and reduce the likelihood risk of an accident, concerned authority must effectively manage the risks associated with any hazard that cannot be eliminated. It is important to have a clear understanding of several terms and how they are used interchangeably in safety management contexts.

3.2.1 Key Terms

- Hazard - The condition or circumstance that can lead to physical injury or damage.
- Risk - The consequence of a hazard measured in terms of likelihood and severity.
- Mitigation -The measures taken to eliminate a hazard, or to reduce the likelihood or severity of a risk.
- System Safety Deficiency - The circumstance that permits hazards of a like nature to exist.

3.2.2 An example case

Safety context – Existence of an obstacle at the end of a runway

Hazard – Aircraft could hit the obstacle. Or the condition or circumstance that can lead to physical damage or loss to aircraft.

- Risk 1 – Aircraft hitting directly with the obstacle
- Risk 2 – Runway excursion due to initiation of avoidance action from colliding obstacle
- Risk 3 – More fuel consumption and loss of time due to go around action

By drawing on accident and incident data and other available information (such as operational experience), an assessment of the likelihood and severity of each of the three risks associated with the hazard of the obstacle on the end of a runway, can be made. In the example above, the consequence of hitting the obstacle while in flight is likely to be more severe than the aircraft running-off the end of the runway while attempting to avoid hitting the obstacle. But both risks will normally cause more damage than the option of go around sacrificing associated fuel loss and time loss to passengers.

Step 1: Classification of Severity and Likelihood

For the example above, it is evident that there are a broad range of potential risks associated with the hazard, due to the presence of obstacle and the end of the runway. Each of the identified risks poses different potential severity and a likelihood chance of occurring. In order to appropriately focus on available resources to deal with the hazard and the associated risks it is necessary to first classify them systematically according to their severity. There are many risk classification systems available in literatures ranging from simple to complex system classification. In any event, it is important to use available data and information to appropriately classify the risks.

Severity	
Category A	Potential for loss of life or destruction of the aircraft
Category B	Potential for serious injury or major damage to the aircraft
Category C	Potential for minor injury or minor damage to the aircraft
Category D	Trivial (e.g. inconvenience)

Likelihood	
High	Often
Medium	Occasionally
Low	Seldom
Rare	Unlikely
Very rare	Highly Unlikely

Figure 8 Severity and Likelihood table definition

Step 2: Identification of Hazards

While identifying the hazard, it is important to not to get confused it with the associated risks. As we discussed earlier, the presence of obstacle on the end of the runway was the hazard which could result in a physical damage or loss.

The three identified risks associated with that hazard are,

- The first risk to safety was that an aircraft could possibly hit the obstacle while taking off or landing of flight operation.
- The second identified risk was that the pilot may know the obstacle was there and in order to ensure the aircraft does not hit the obstacle, he or she may carry out a steeper than normal approach and arrive at the end of the runway, continue with the landing, and run off the end of the runway.
- A third risk that was identified was that the pilot in the second scenario may recognize that he or she is hot and high and execute a go around and attempt another landing.

It is important to delve deep into all possible scenarios to ensure that all the underlying hazards are identified. Once the hazards and all associated risk are identified, potential courses of action to manage them should be attempted. One possible course of action may be to eliminate the hazard (the obstacle at the end of the runway) entirely by removing it. If that cannot be done, a second course of action may be to avoid the hazard by not using that runway. The hazard still remains, but the likelihood of it being struck by aircraft during take-off or landing is reduced. A third possible course of action is to develop and implement mitigation plans to reduce the three identified risks to an acceptable level as possible. The third course of action requires the operator or airline to pre-determine the criteria regarding the acceptable level of risk and to assess the benefits of the operation versus the risks involved.

Step 3: Risk Management

The quantitative risk management process is often data driven. The data that are collected help determine safety performance and can be used to identify hazards or system safety deficiencies. The data may be found anywhere: the operating environment, the equipment used, the people involved in the operation, work procedures, the human/equipment/procedures interactions, etc.

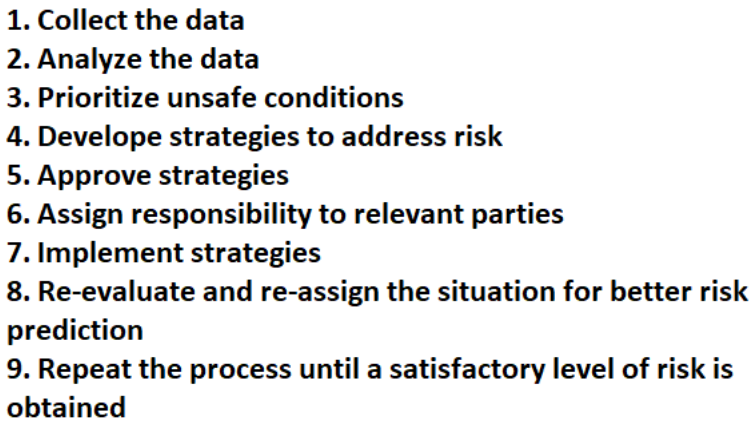

Figure 9 Quantitative Risk management process [15]

If the risk cannot be reduced to or below the fully acceptable level, it may be regarded as tolerable if:

- The risk is less than the pre-determined unacceptable limit.
- The risk has been reduced to a level that is as low as reasonably practicable.

- The benefits of the activity or operation are sufficient to justify accepting the risk.

Step 4: As Low as Reasonably Practicable (ALARP)

Before granting the permission for flight, the flight regulators must ensure that the applicant has taken all reasonable steps to ensure health and safety risks arising from their activities as low as reasonably practicable. ALARP [1] is a principle in the regulation and management of safety-critical and safety-intensive systems**.** The principle states that the residual risk shall be reduced as far as reasonably practicable level. The applicant will have to make a demonstration of ALARP within the safety case required as part of the application process for clearance to fly. The regulatory approval will be based on the residual risks if they are within acceptable level.

ALARP is the most common risk management technique adopted in aviation. The acronym ALARP is used to describe a risk that has been reduced to a level that is as low as reasonably practicable. In determining what is reasonably practicable level, consideration should be given to both the technical feasibility of further reducing the risk, and the cost. This might include some level of cost-benefit study. Determining that the risk is as low as reasonably practicable means that any further risk reduction is either impracticable or is grossly disproportioned by the costs. Also, it should be kept in mind that when an individual, operator or society accepts a risk value, this does not mean that the risk is eliminated, and safety entails. This is a false sense of safety. In reality, some residual level of risk still remains. However, the individual, operator or society has accepted that the residual risk is sufficiently low that it is outweighed by all the benefits. Unfortunately, it is often only after an accident that individuals, operators, or a society is able to ascertain the acceptability level of risk, using hindsight perspectives for using retrospective analysis.

In assessing risk and developing a mitigation criterion, the risks are often considered in three broad categories.

1. The risks are so high that they are unacceptable.
2. The risks are so low that they are clearly acceptable.
3. The risks are between the two categories and consideration needs to be given to managing the risks, so the benefits can be realized.

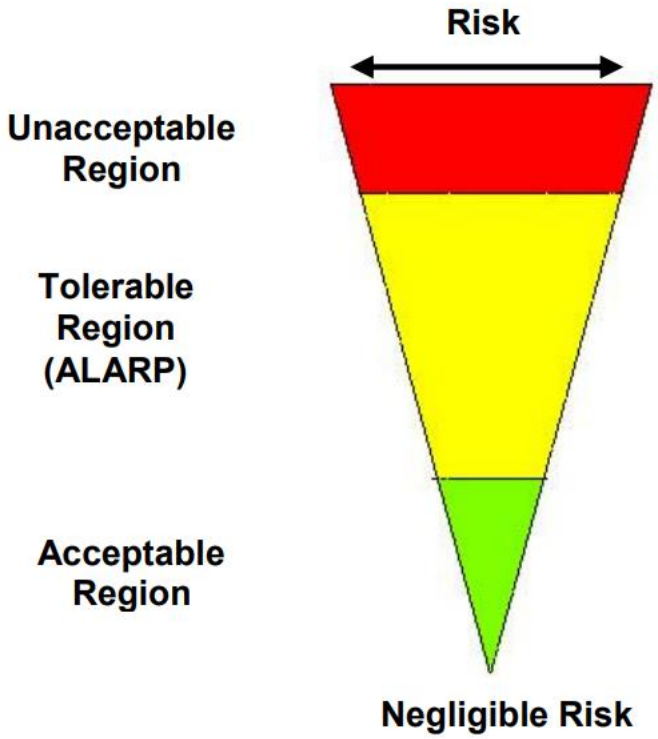

Figure 10 A typical ALARP based risk picture used in aviation domain [1]

If the risk does not meet the pre-determined acceptability criteria, an attempt must always need to be made to reduce it to a level that is acceptably possible by using appropriate mitigation plans and procedures.

3.3 RISK MANAGEMENT IN MANAGERIAL DECISION MAKING

Figure 11 Ideal management outcome [9]

Risk management also helps to strike a balance between protection of resources to safe production of resources by implementing policies and procedures, hazard or incident reports, audit committee meetings, or audit findings that suggest a weakness in the existing policies and procedures for managing safety that may need to be treated with much higher priority than in the non-frequent ones. Figure 11 indicates an ideal management outcome expected, i.e., to balance various dependencies and move the business in right direction thereby respecting overall sentiments of all stakeholders present in the system without compromising safety aspects.

A performance-centered SMS uses sophisticated risk management approaches to reduce safety risks to a level as low as reasonably practicable. It is done in a manner that takes full account of Reason‘s model of accident causation, where latent conditions and organizational level system safety deficiencies are given the root cause reasons of occurrence of hazards and hence, it would lead to risk that needs to be managed. Risk management approaches are considered as the means by which an SMS is better aligned according to the size and complexity of the organization or operation.

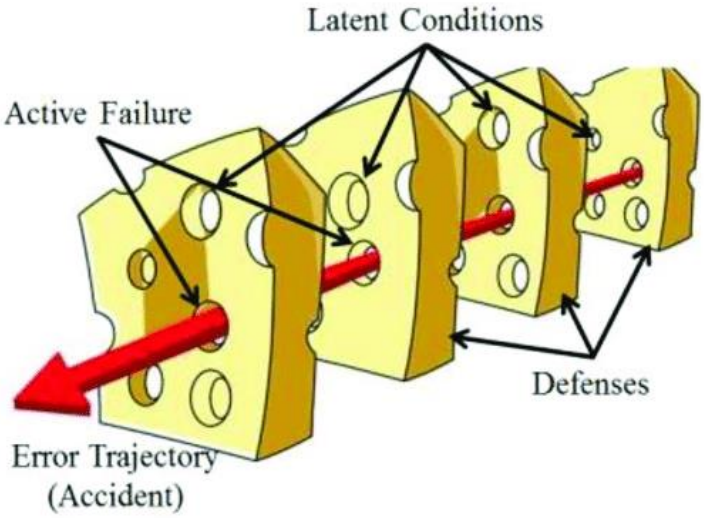

Figure 12 Accident or error trajectory from Reason's model [12]

3.4 SAFETY ASSESSMENTS TECHNIQUES IN SYSTEM-LEVEL SAFETY ASSURANCE

The usage of safety assessment techniques in system-level safety assurance of aircraft is different from risk management perspective of dealing with overall safety of aircraft including different stakeholders. Hence Risk Management techniques has a broader application scope, while safety assessment has a narrower but significant relevance in system-level assessments.

In aviation systems side, the objective of performing safety assessments is to assist the designers and management in making informed decisions to timely act or steer towards realizing safety objectives. Safety assessment acts as support in determining the numerical values to be assigned to secure the intended safety target (acceptable probabilities of occurrence) mentioned in the requirements by airworthiness authorities. One approach in this direction is to rely totally on previous accident rates (FAR or probabilities) to justify that system concerned is within the acceptable level. But when accident statistics are not available, or complexity of the system is very high, risk assessment approaches are adopted. Safety assessment must make clear on what the critical features of each system are and upon with special manufacturing techniques, inspection, testing, crew trainings, and maintenance practice that they are critically independent. Also, the expectations from risk assessments are that it provides enough decision support to regulators especially on the practical operational aspect of the aircraft that it may demand that the aircraft be able to takeoff and fly safely with various defects and shortages present in it. The purpose of safety

assessments in aviation is not only to demonstrate safety to airworthiness authorities but also to clearly state those aspects on which safety is inherited which needs to be upholded by everyone associated with any stage of the aircraft lifecycle. Safety assessment is not a standalone activity, but it is a part of total design process, not just something that is done at the end of the development, but something that lives alongside of the development with clearly stated objectives so that all concerned are aware of them at right instance.

Safety analysis helps to identify some of the worst accidents caused by cascade failures and other common mode failures. Safety analysis provide a holistic safety perspective especially into how the aircraft is going to behave as an integrated system. Such installed aircraft components as a single system provide knowledge of necessary safety precautions required to be considered in the design due to secondary effects such tire bursts, engine explosions, or structural integrity failures which are themselves alone are not catastrophic. Such a knowledge earlier in the design stage helps to avoid costly re-design activities of future. It is necessary to make hazard analyses throughout the design process to identify and eliminate hazards.

High levels of inherent safety needed from essential systems are achieved by some form of fail-safe system design incorporating redundancy. For example, in the case of structural members of systems the redundancy is achieved in the form of alternative load paths or the use of crack stoppers. In the case of electrical and hydraulic supply systems, redundancy is achieved through three or four channels powered by the main engines or by other backup electronic pumps or generators. The degree of redundancy is usually determined by the required level of safety and by the extend of single event failure scenarios that could possibly cause a delay or cancellation in flights during its continued operation.

The intensity of safety assessment will vary depending upon factors such as complexity of the system, criticality of the system to the basic functioning of aircraft, the depth of experience available on the type of system used, and methods and technologies are being introduced. So before delving into detailed safety assessment a preliminary hazard analysis (PHA) would help to determine the depth of assessment required. Understanding of the system from PHA would help to define safety objectives of the system before entering detailed investigations.

ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment is an Aerospace Recommended Practice from SAE

International. This Recommended Practice defines a process for using common modeling techniques to assess the safety of a system being put together is as below.

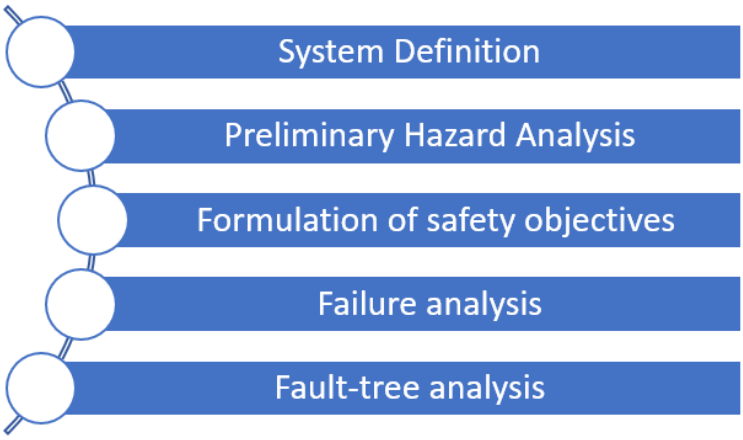

Figure 13 System-level safety assurance process

3.4.1 Definition of system

In order to establish a meaningful safety objective, it is first necessary to establish a proper definition of each system. This definition should include,

- Physical boundaries of the system and its associated components.
- The environmental conditions which the system will need to withstand.
- The interfaces with all other major systems, e.g., human element.
- Functional block diagram of systems and its interfaces.
- Intended functions of the system including its modes of operation
- System performance parameters and their allowable limits.

3.4.2 Preliminary Hazard Analysis (PHA)

Once safety definition established the next step is to make a Preliminary Hazard Analysis. This is majorly concerned with aspects of functions and vulnerabilities of the system rather than costly, time taking detailed analysis of the system. At the end of PHA, a definition of failure condition of the system would be arrived at. PHA would help to answer the following questions,

1. What are the consequences of failure of the system to the aircraft and its occupants when the system was functioning within its specified performance limits.

2. Consequences of other malfunctions of the system (e.g, overheating) and their effects on other systems or parts of the aircraft.
3. Identification of all possible common-mode or cascade failures which needs more detailed assessment.
4. Identification of all possible sources of human error during flying or maintenance.

Having completed PHA, the next step would be to decide which features of the system need detailed assessment, the extend of assessment required, and what test programs are needed to confirm assumptions made in the analysis.

3.4.3 Formulation of Safety objectives

Having identified the hazards, the next step would be to formulate a set of safety objectives appropriate to each defined system or function. Safety objectives must be aligned to requirements. Safety objectives should be expressed in more detailed engineering terms appropriate to the particular functions and features of the system under consideration. Safety objectives can be defined in terms of purely numerical terms or simple engineering terms depending upon the reliable statistical evidence available.

Description of failure condition	Severity of effect	Risk of catastrophe	Objective
Short touchdown on runway	Hazardous	1/30	<3E-8
Touchdown with one wheel off the side of runway	Hazardous	1/30	<3E-8
Touchdown on the runway but one wheel runs off the side of runway	Hazardous	1/30	<3E-8
Landing gear collapse	Hazardous	1/30	<3E-8
Wing tip touches ground before wheels	Hazardous	1/30	<3E-8

Tail end hitting runway upon takeoff condition	Hazardous	1/30	<3E-8

Table 2 Example of Safety objective definition

3.4.4 Failure analysis

SAE Aerospace Recommended Practice ARP926A mentions about two methods of making failure analysis: Top-down and bottom-up methods. The top-down or functional approach starts by identifying the failure conditions to be investigated, and then proceeds to derive those failure modes and combinations of failure modes which can produce the failure condition which is being investigated. The bottom-up or hardware method starts with the hardware failure modes which can occur, and analyses the effects of these on the system and the aircraft in order to determine the failure conditions which can possibly occur. In both cases, one studies the effects of the resultant failure conditions on the aircraft, and determines their seriousness and whether the safety objectives are fulfilled.

The decision to use functional or hardware method depends on the nature and complexity of the system under consideration. Usually, combinations of the two approaches are adopted for complex systems. “Functional” approach is used to deal with combinations of failures, and a “Hardware” approach is used to determine critical single failure modes. For examining common-mode and cascade failures, a combined “Functional” and “Hardware” approaches are followed. One first determines those multiple failures which will hazard the system and then forecasts the ways in which these multiple failures can be produced.

3.4.5 Fault Tree Analysis

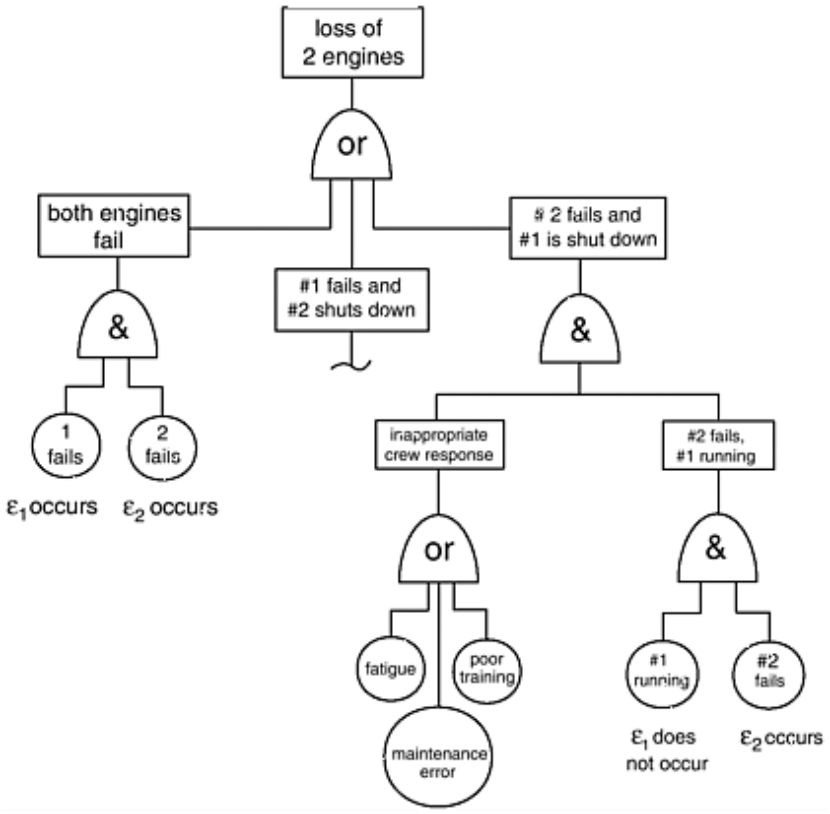

Figure 14 An example for typical Fault-Tree analysis

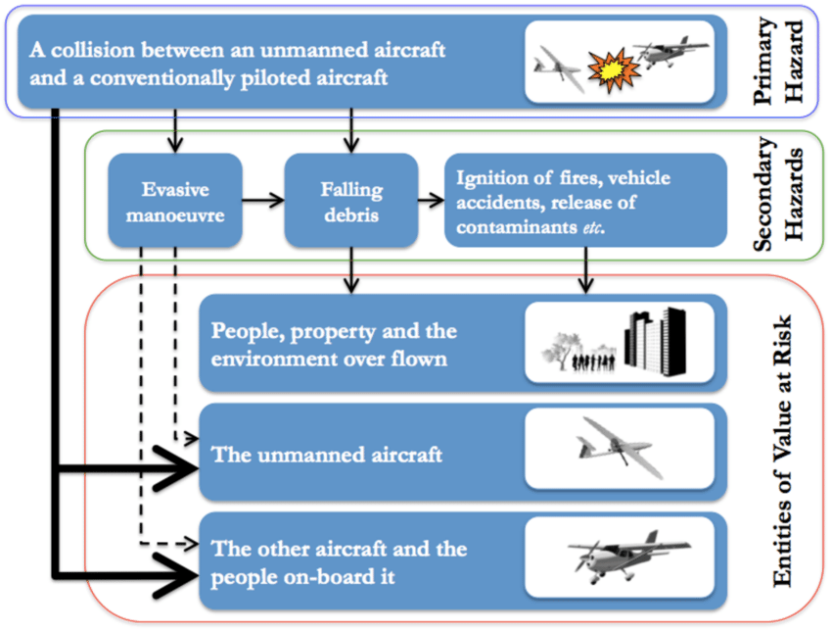

Figure 15 Typical example for dependence diagram

Fault trees (Figure 14) and dependance diagrams (Figure 15) are the two methods of presentation of failure which are commonly used in USA and Europe. Fault tree (Figure 14) is a graphical method of expressing the logical relationship between a particular failure condition and the failures or other causes leading to the particular failure condition. The method uses specific symbols to represent top failure events leading to individual failure conditions. Though this form of analysis is tedious to prepare it has the advantage that it gives a visual representation of sequences and combinations of failures in an easy to track manner. Each block of this diagram will be supported by further dependance diagrams, and the probabilities on the various parts of the system can readily be seen. Then the overall probability of failure condition can be calculated.

Systematic safety assessment approaches are available in the form of airworthiness standards recommended by Civil Aviation Authority (CAA) UK and similar organizations like International Civil Aviation Organization (ICAO), Federal Aviation Administration (FAA), European Union Aviation Safety Agency (EASA), etc through their several years of addressing or analyzing pressing issues of those times which has gradually culminated in engineering know-how of the safety aspects of flying. But there must have an improved thinking to address emerging risks scenario of now which are more dynamic in nature due to the pace of technological advancement and easy availability of technology. Existing standards are static in the sense of not able to incorporate all sorts of airborne devices of any size and capacity. Aviation systems are unique technical systems which poses joint air and ground-based threat scenario in a socio-technical environment where less margin of error is tolerable. Hence, rather than standalone risk assessments there is a need to incorporated risk-based governance. There are several instances where entire aircraft program is put on hold or scrapped due to unexpected and unanticipated safety incidents which put public sentiments against it. Being a high consequence probable socio-technical system, the regulators face significant challenges to meet the safety standards due to its emerging nature of risks and regulatory challenges due to not able to generalize or authoritatively state a full technical boundary to enable them to generalize the approval process as a standardized approach. Airworthiness certification is the existing approach regulators adopt to certify the aircraft systems and aircraft.

4 CONCLUSION

Safety is an emerging property of any system which emerges through an integrated perspective, especially a complex socio-technical system. Both system level and management level safety considerations are significant. In aviation domain, system-safety, organizational level, and human factor safety considerations merge through Safety Management System (SMS) framework. Risk management techniques and approaches provide a greater insight at various stages of safety assurance process of SMS. Safety Management System was being looked at as a significant aviation level safety assurance framework in this thesis. Great insights into safety assurance process of aviation safety and insight into the risk implementation and assessment of various issues pertinent to aviation safety area and how it is treated in methodological fashion rather than too much focus into implementation of different techniques itself would be the significant outcome of this thesis.

A future study into the same theme could bring the inter-operability aspects of various technical elements and risk treatment techniques of SMS would be aligned to added dimension with respect to security aspects related issues and challenges of aviation domain.

REFERENCES

[1] “ALARP Guidance Note”, N-04300-GN0166. Revision 6. June 2015. NOPSEMA. https://www.nopsema.gov.au/assets/Guidance-notes/N-04300-GN0166-ALARP.pdf

[2] Ansell, C., and J. Torfing. (2016). “Introduction: Theories of Governance. Handbook on Theories of Governance”. 1–18. Cheltenham: Edward Elgar Publishing.

[3] Aven, T., and O. Renn. (2010). “Risk Management. Risk Management and Governance”. 121–158. Berlin: Springer Science+Business Media.

[4] Boholm, Åsa, Herv e Corvellec, and Marianne Karlsson. (2012). “The Practice of Risk Governance: Lessons from the Field.”, Journal of Risk Research 15(1): 1–20.

[5] Civil Aviation Authority-Safety Regulation Group. (2008). “Safety regulation: Safety management systems”.

[6] Department of Transportation (DOT) Canada. (2004). “TP14135E safety management systems for small aviation operations - A practical guide to implementation”. Ottawa, ON, Canada: Department of Transportation (DOT) Canada.

[7] Dong, L., Neufeld, D., & Higgins, C. (2009). “Top management support of enterprise systems implementations”. Journal of Information Technology, 24, 55–80.

[8] “Fatal Accident Statistics for Passenger Air Transport Services 1960-1967”, CAA Paper 77027, Civil Aviation Authority (UK).

[9] Peters, G.A. (1979), “How to Design a Safe Aircraft”, Hazard Prevention, (The Journal of the System Safety Society).

[10] ICAO (2008). “Training: ICAO SMS Module 02 - Basic safety concepts”.

[11] International Civil Aviation Organization (ICAO). (2008). “Safety Management Systems (SMS) course module 4 hazards”. International Civil Aviation Organization.

[12] International Civil Aviation Organization (ICAO). (2009). “ICAO safety management SARPs”. In Safety Management Manual (Doc. 9859) (2nd ed.). Montreal: International Civil Aviation Organization (ICAO).

[13] Reason, J. (2000). “Human error: models and management”. In: BMJ 320.7237, pp. 768–770. url: https://www.bmj.com/lookup/doi/10.1136/bmj.320.7237.768.

[14] Øien, K. (2001). “A framework for the establishment of organizational risk indicators”. In: Reliability Engineering & System Safety 74.2, pp. 147–167. issn: 09518320. doi: 10.1016 / S0951-8320(01)00068- 0.

[15] McFadden, K. L., & Hosmane, B. S. (2001). “Operations safety: an assessment of a commercial aviation safety program”. Journal of Operations Management, 19(5), 579–591.

[16] “MIL-HDBK-217B – Reliability Prediction of Electronic Equipment”, Department of Defense, USA.

[17] Renn, O. (2005) “Risk Governance: Towards an integrative framework”, p. 157.

[18] Bell, R. and Reinert, D. (1992) “Risk and system integrity concepts for safety-related control systems”. In: Safety Science 15.4, pp. 283–308. issn:09257535. doi: 10.1016/0925-7535(92)90021-Q.

[19] Skybrary. (2013a). “Risk management”. Von Skybrary.

[20] Stolzer, A. J., Halford, C. D., & Goglia, J. J. (2008) “Safety management systems in aviation”. Aldershot: Ashgate Publishing Ltd.

[21] Tjerhom, B. and Aase, K. (2007) “Safety and changes in the Norwegian aviation transport system - What is the role of the legislator and the regulator?”, In: T. Aven and J.E. Vinnem (eds.) Risk, Reliability and Societal Safety, Vol. 3, London: Taylor & Francis, pp. 2143-2149.

[22] Van Dam, R., Masson-Zwaan, T., & Mendes de Leon, P. (eds) (1992) “Regulating International Civil Aviation – an ICAO Perspective”, Ann. Air & Space L. 11.

[23] Vaughan, D. (2005) “Organizational rituals of risk and error”. In: B.M. Hutter and M. Power (eds.) Organizational Encounters with Risk. Cambridge, UK: Cambridge University Press.

[24] Webler, T., Rakel, H. and Ross, RJ.S. (1992) “A critical theoretical look at technical risk analysis”. Industrial Crisis Quarterly 6: 23-38.

[25] Weiss, G. T. and Wilkinson, R. (2015) “Introduction: Drivers and Change in Global Governance” 29 EIA 391.

[26] Westrum, R. (1996) “Human factors experts beginning to focus on organizational factors in safety”. I CAO Journal 51(8): 6-8, and 26-27.

[27] Wilpert, B. (2008) “Regulatory styles and their consequences for safety”. Safety Science 46(3): 371-375.