TÉCNICO LISBOA

Cross Domain Within EASA Safety Management Systems Environment

Manuel Nunes Faria

Thesis to obtain the Master of Science Degree in

Aerospace Engineering

Supervisors: Prof. Pedro da Graça Tavares Álvares Serrão
Mr. Joel Hencks

Examination Committee

Chairperson: Prof. Filipe Szolnoky Ramos Pinto Cunha
Supervisor: Prof. Pedro da Graça Tavares Álvares Serrão
Member of the Committee: Prof. Sérgio David Parreirinha Carvalho

July 2018

Acknowledgments

First and foremost, I would like to thank my Lisbon University supervisor, Dr. Pedro Serrão, whose technical advice and moral support are greatly appreciated throughout the duration of this study. Additionally I would like to thank my external supervisor from AeroEx, Mr. Joel Hencks in particular for his insight, share of knowledge and sturdy hand in defining the approach during the early days

This Thesis would not have been possible without the collaboration and support of different experts in the aviation safety domain from various organizations.

I would like to thank the many colleagues and friends I met during my studies in Lisbon and Naples that helped me grow as a person and were always there for me during the good and bad times in my life.

Last but not least, I wish to thank my parents and family for their enduring encouragement and for giving me the confidence to undertake this Masters.

To each and every one of you – Thank you.

Abstract

Aviation is safe critical industry with the goal of delivering a service. However, it is impossible to guarantee that one finds an environment, specially in a a system with human input, completely free of hazards and risks. Therefore, safety has to be a dynamic characteristic of the system where risks to safety need to be constantly mitigated.

Provided safety risks are kept under an appropriate level, the aviation system can be expected to maintain the appropriate balance between production and protection. Organizations that have Safety Management System (SMS) implemented have significantly lower accident rates. As such it is interesting to see SMS in action.

The purpose of this research is to determine the impact of SMS on a commercial aviation operation using a case study. This study starts with the definition of safety and its evolution in aviation as well as its implementation. Then, a review of the status of the SMS with European Aviation Safety Agency (EASA) is made and a case study which actively involves different organizations is presented.

The results showed how organizations, Air Navigation Service Provider (ANSP), Operators and Airport authorities have indeed recognized the importance of the SMS and that each organization has customized their SMS to fit their needs. Furthermore, variations were identified between the International Civil Aviation Organization (ICAO) SMS model and the models adopted by EASA. In addition, it also concluded that, safety assessments will always be a subjective methodology, highly dependent of the expertise of those participating in it.

Keywords

Safety; SMS; Risk assessment; Hazard identification.

Resumo

A aviação é uma indústria com uma componente de safety crítica e que tem como objetivo a prestação de um serviço. Apesar disto, é impossível garantir que se encontre um ambiente, especialmente num sistema com input humano, completamente livre de perigos e riscos. Assim, safety deve ser uma característica dinâmica do sistema, onde os riscos são constantemente mitigados.

Desde que os riscos de segurança sejam mantidos sob um nível apropriado, espera-se que um equilíbrio adequado entre produção e proteção. As organizações que implementaram o SMS têm taxas de acidentes significativamente mais baixas pelo que é interessante ver o SMS em ação.

O objetivo deste trabalho é determinar o impacto que o SMS tem nas operações de aviação comercial através dum caso concreto. Este estudo começa com a definição de segurança e a sua evolução, bem como sua implementação. Em seguida, é feita uma revisão dos requisitos do SMS por parte da EASA e é apresentado um caso que envolve diferentes organizações.

Os resultados mostraram como as organizações, ANSP, operadores e autoridades aeroportuárias reconhecem a importância do SMS e que cada organização personaliza os seus SMS para atender às suas necessidades. Além disso, foram identificadas variações entre o modelo SMS da ICAO e os modelos adotados pela EASA. Concluiu-se também que as avaliações de segurança serão sempre uma metodologia subjetiva, altamente dependente da experiência e conhecimento dos analistas.

Palavras Chave

Safety; SMS; Análise de risco; Identificação de perigos.

Contents

List of Figures

List of Tables

List of Variables

Symbol	Description
HR	Human reliability
HU	Human unreliability
HE	Human error
PR	Probability of recovery
p_t	Overall probability
p_t	Probability each single event
n	Number of causal barriers
R	Risk
s_i	Scenario identification or description
p_i	Scenario likelihood
x_i	Measure of damage

Acronyms

AAIB	Air Accidents Investigation Branch
ACMI	Aircraft, Crew, Maintenance and Insurance
AltMoC	Alternative Means of Compliance
AMC	Acceptable Means of Compliance
AMO	Approved Maintenance Organization
ANAC	Autoridade Nacional da Aviação Civil
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
AOC	Air Operator Certificate
ATC	Air Traffic Control
ATM	Air Traffic Management
ATO	Approved Training Organization
ATPL	Airline Transport Pilot License
BR	Basic Regulation
CAA	Civil Aviation Authority
CAT	Commercial Air Transport
CAMO	Continuing Airworthiness Management Organization
CMPA	Complex Motor Powered Aircraft
CPL	Commercial Pilot License

CR	Common Requirements
CRM	Crew Resource Management
CS	Certification Specifications
EASA	European Aviation Safety Agency
EASP	European Aviation Safety Programme
EC	European Comission
EFTA	European Free Trade Association
EoSM	Effectiveness of Safety Management
EU	European Union
FAA	Federal Aviation Administration
FCL	Flight Crew Licensing
FIR	Flight Information Region
FO	Foreign Object Debris
FOD	Foreign Object Damage
GM	Guidance Material
GPIAAF	Gabinete de Prevenção e Investigação de Acidentes com Aeronaves e de Acidentes Ferroviários
ICAO	International Civil Aviation Organization
IR	Implementing Rules
ISO	International Organization for Standardization
JAA	Joint Aviation Authorities
LOFT	Line Oriented Flight Training
NAA	National Aviation Authority
NCC	Non Commercial Complex
NPA	Notice of Proposed Amendment

OPS	Operations
PCI	Pavement Condition Index
PIC	Pilot in Command
RTO	Rejected Take-off
SARP	ICAO Standards and Recommended Practice
SMS	Safety Management System
SMICG	Safety Management International Collaboration Group
SMM	Safety Management Manual
SPO	Specialized Operations
SSP	State Safety Program
TCO	Third Country Operators
TESEO	Tecnica Empirica Stima Errori Operatori
TRM	Team Resource Management
UK	United Kingdom

1

Introduction

Contents

The origin of mankind's desire to fly goes all the way back to prehistoric times but it wasn't until the first power-driven flight by the Wright brothers that our way of life was forever changed. Ever since, the aviation industry has been steadily expanding due to the growth of air transportation demand supported by the world's economic growth.

The prestige of this industry is deeply affected by safety. Any accident becomes the centerpiece of the media, filling the headlines of newspapers and TV news segments. The public expects nothing short of immaculate safety records. Thus, safety is paramount. It's the priority of every entity involved in the air transport industry.

These efforts led to a sharp reduction in the accident rate over the years as seen in Fig.1.1.

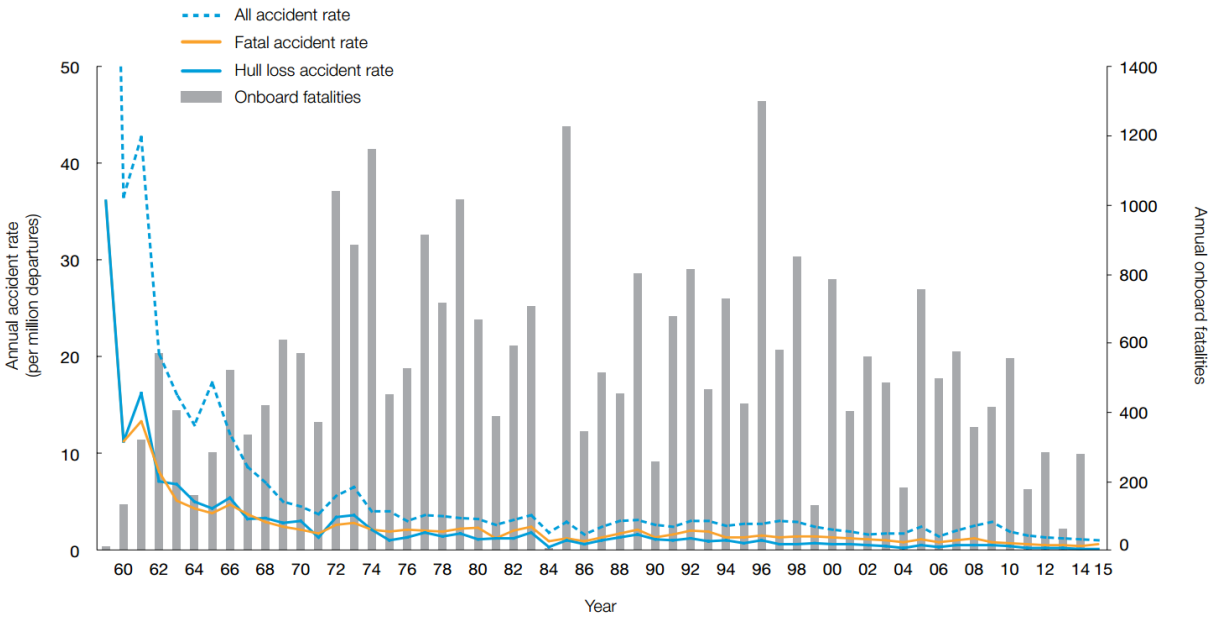

Figure 1.1: Accident Rates and Onboard Fatalities by Year Worldwide [1]

Aviation is now experiencing a paradigm shift regarding safety. From a traditional reactive approach, the industry is evolving to implement proactive and innovative SMSs.

In order to further improve the already good safety record obtained in the civil aviation industry, ICAO has promoted the principles of safety management. These principles revolve around the implementation of a SMS in industry organizations and a State Safety Program (SSP) in Contracting States.

The implementation of a safety management system should lead to an overall improvement of the processes of a company, and should contribute to one of civil aviation's key business goals: enhanced safety performance, aiming at best practices and moving beyond full compliance with regulatory requirements.

1.1 Research Background

There has been a growing interest for SMS since the ICAO mandated that its entire member states implement SMS programs.

In 2006, following the ICAO signing of the international standard for SMSs in aviation, the EASA started to draft regulations in the SSPs and SMSs covering the areas of Air Operations (OPS) and Flight Crew Licensing (FCL). This led to the development of a distinct set of regulations for both authorities and organizations.

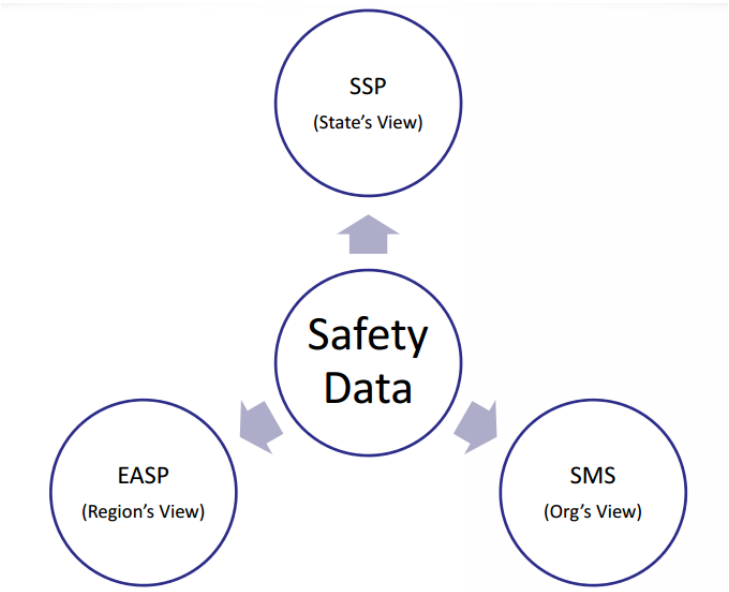

Figure 1.2: Overview of safety data at the European level

Authority requirements support the European Aviation Safety Programme (EASP) and SSP/SMS, in particular by focusing on specific critical elements of a safety oversight system defined by ICAO namely:

- CE-3: State civil aviation system and safety oversight functions
- CE-4: Technical personnel qualification and training
- CE-5: Technical guidance, tools and the provision of safety-critical information
- CE-6: Licensing, certification, authorization and/or approval obligations
- CE-7: Surveillance obligations
- CE-8: Resolution of safety concerns.

while serving the standardization objective set out in the Basic Regulation (EC) No 216/2008 [2]. They further include elements that are crucial to institute a comprehensive SMS at EU level.

Organization Requirements include consolidated general requirements for management systems, designed to embed the ICAO Standards and Recommended Practices (SARPs) in a way as to ensure compatibility with existing management systems and to encourage integrated management. These requirements and related Acceptable Means of Compliance (AMC)/Guidance Material (GM) set out what is needed in terms of the organization's management system. Together with the relevant provisions of the Basic Regulation 216/2008 [2], these fully cover the existing ICAO SMS Standards and encourage integrated management.

Furthermore, addressing the security part of risk management, regulation European Comission (EC) 300/2008 [3]on common rules in the field of civil aviation security sets the basic principles of what has to be done in order to safeguard civil aviation against acts of unlawful interference without going into the technical and procedural details of how they are to be implemented.

This research background induces the research issues needed to be addressed in the next chapter.

1.2 Motivation

The importance of hazard identification, risk management and mitigation are crucial in SMS. It is one of its central components.

In aviation, in virtue of the nature of the operations, risks are more often than not shared among different organizations. Sometimes the organization that suffers the most damaging effects isn't the one responsible for actively dealing with that hazard, it can be an external hazard monitored by a third party. However, this organization, which doesn't have an effective role in mitigation might be aware of abnormal situations that would be very useful to improve another organization's SMS.

Therefore it is pertinent to study how the SMS, after being implemented and their structures clearly defined and coherent across domains, of different organizations interact.

When a disturbance is introduced in any system, it has to be carefully analyzed as it can have effects on the delivery of the service and influence the safety of the organization operations. These analyses, are done in the aviation industry through the implementation of SMS since safety is one of the most important aspects. This implementation must be continuously developed and applied to all procedures in the system.

In order to analyze safety, the definition of risk assessment is necessary because it can help to maintain an high level of workability and it increases the mission success. Furthermore, safety cannot be analyzed from one organization's perspective but it should take into consideration the system as a whole.

1.3 Research Objectives

This thesis is designed to contribute to the pool of knowledge by analyzing the interoperability of safety management systems under the scope of EASA.

This project is focused on the analysis of the hazard that foreign object debris are in aviation. The methodology applied for the risk assessment focuses on the human reliability analysis evaluated through the application of Tecnica Empirica Stima Errori Operatori (TESEO).

It aims to present a clear, coherent, complete and integrated approach to aviation organizations of SMS and how it can manage hazards and provide an inherently safe environment for operations to take place.

In order to provide a solid scientific basis, an extensive literature review has been made which focuses not only in the regulations but also on the different aspects of safety and risk management.

1.4 Thesis Outline

In keeping with the aims of this research project, this thesis is divided into five chapters.

Chapter 1 which serves as the blueprint of the thesis involves a brief introduction note, the background to the research, the research and the outline of the thesis.

Chapter 2 involves the review of the literature. It provides a theoretical background of risk and safety management creating the basis for the understanding of the subject.

Chapter 3 presents safety management from the oversight perspective, exposing the current current rule-making status under the scope of EASA.

Chapter 4 starts with information about the companies that contributed for the elaboration of this thesis. It then introduces the foreign object debris hazard, presenting an incident which shows some of its potential consequences. To this very same incident, the TESEO methodology is applied. Lastly, possible mitigation actions are presented.

Chapter 5 involves the conclusion and the implications of the study. It will consist of three sections. The first section showcases the similarities between the SMS and the second section the dissimilarities. The last section deals with possible future research.

2

Literature Review

Contents

This chapter is on the literature review. The literature review serves many different purposes and entails a wide variety of activities. Hence, literature review has been defined in a number of ways. But one of its main functions is to identify theories and the previous research which influence the research topic, methodology being applied and the identifications of the problem to research.

2.1 Current issues

The number of airline departures has risen dramatically in the past few years, with air traffic projected to double in the next 15 years. Therefore, there is a need to employ new methods and programs that ensure that this significant capacity expansion is carefully managed and supported.

There is much that speaks for a further increase in capacity in many parts of the world and to be able to meet this demand. It is important that the industry is best suited for the future development. For the regulators, it is an important step and opportunity to develop modem oversight methods and the development of performance based safety oversight, also known as risk-based oversight across all domains.

There is no globally harmonized standard for SMS, however the ICAO Safety Management Manual Doc 9859 provides generic guidance which has been unilaterally accepted by the aviation community [4].

2.2 Role and definition of safety

Defining what safety is could be the topic of a thesis and many discussions are currently held concerning the topic. This is due to a shift between what has become coined as Safety I and Safety II that is underway.

Traditionally, safety has been defined as a condition where there is absence of harm [5]. Or, more precisely, since we know that ensuring that nothing goes wrong is impossible, as a condition where the number of things that go wrong is acceptably small. This is an indirect definition, defining safety by what happens when it is missing. Subsequently, safety is also measured indirectly, by the consequences of its absences instead as of a quality in itself.

The starting point for safety concerns has been the occurrence, potential or actual, of some kind of adverse outcome, whether it has been categorized as a risk, a hazard, a near miss, an incident, or an accident. Historically speaking, new types of accidents have been accounted for by introducing new types of causes. First by addressing risks related to technology then by bringing up the role of human factors and finally further extending the causes to including the influence of organizational failures and safety culture following the Challenger and Chernobyl accidents. By introducing causes, we became accustomed to explain accidents in terms of cause-effect, rather than by challenging or changing the

basic underlying assumption of causality. This lead to, regarding safety, putting the onus on what goes wrong and overlooking things that go right.

When things go right, the outcome is as expected. Therefore, nothing that draws attention extra into it. The concern, as to why success is overlooked, lies in the fact that there is not any motivation to understand why things went well since the system, people and technology, worked as it should and no adverse event that could change the outcome happened.

The tendency to focus on what goes wrong is reinforced in many ways. It is often required by regulators and authorities, resulting in abundant information about how things go wrong and how to prevent it from happening. This leads to a reactive, find and fix approach. Looking for failures, finding the causes and eliminating or building up barriers. A consequence of this is that safety investments are seen as costs which can be hard to undertake or justify as safety and the core business compete for resources. Furthermore, learning is limited to a fraction of the total data pool.

In contrast, there is no demand from regulators and authorities to look into what goes well and the literature on how human and organizational performance succeeds is scarce as it clashes with the traditional approach. However, in this perspective, safety and core business are positively correlated, what benefits one also benefits the other. Analogously, by focusing on what has gone right, the data pool available for learning is exponentially greater.

2.2.1 Safety I

Safety I is usually described as of the design of safe system that is able to eliminate, adequately control or mitigate all the adverse outcomes [6]. The purpose of managing Safety I is to achieve and maintain that state. ICAO defines safety as “the state in which 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 risk management.”

The logic of Safety I is illustrated in Figure 2.1. A binary view is promoted, success or failure of the activities. When in normal functioning, everything works as it should and the outcomes will be acceptable. The number of adverse events is small and acceptable. When something goes wrong, when there is a malfunction, human or otherwise, this will lead to an unacceptable outcome. The key question lies in how the transition from normal to abnormal occurs e.g., whether it happens through an abrupt or sudden transition or through a gradual drift into failure. According to this philosophy, if this transformation can be blocked, safety and efficiency can be achieved.

Safety I assumes that these systems are thoroughly designed and maintained, that the designers can anticipate even the smallest contingencies, the processes are adequate and complete and that all participants behave as they are expected to as per training. This reflects in the way work is carried out by a stress on compliance. Furthermore, these systems feature high reliability equipment, with vigilant

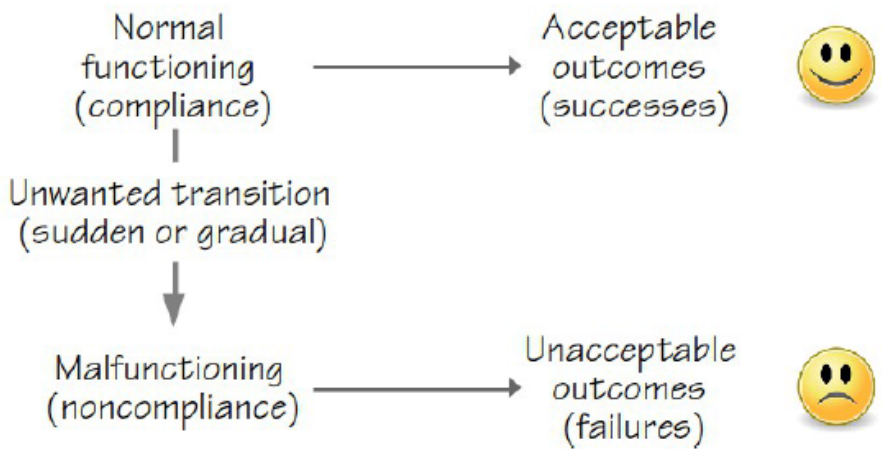

Figure 2.1: Safety I

and diligent staff in their procedures, observations and operations, with clear operating procedures and enlightened management. If these assumptions are true, then the natural performance variability of humans makes them a liability. Following the said logic, the goal can be achieved by constraining all kinds of performance variability e.g, training, standardization, rules, regulations. In the past these solutions were looked at with optimism. However, with the dramatic changes in the work environment, the assumptions of the past might be no longer valid.

2.2.2 Reactive safety management

Reactive safety management, which is based in the Safety I definition, is often equated with the "fly-fix-fly". This approach is reactive because it is forensic in nature. It tries to respond to adverse events by trying to understand the relevant factors that originated it, or by improving detection and recovery from these events.

The purpose of this traditional approach is to ensure that the number of adverse outcomes are as low as possible, or as low as reasonably practicable. In order to achieve this, it reacts when unacceptable events take place, following a causality philosophy. Accidents/Incidents happen when something goes wrong. These have causes which are to be found and treated.

Reactive safety management works as long as the frequency of adverse effects is not high enough. With the increase of the number of adverse effects, it the organization will struggle to take care of its primary activities. The shear capacity to react to those events means that reactions will lag behind the process and become inadequate. This severely damages the effectiveness of the safety system.

In order for reactive safety management to provide an effective and adequate response, the events must be recognized as quickly as possible so that a response is prepared with minimal delay. The worst

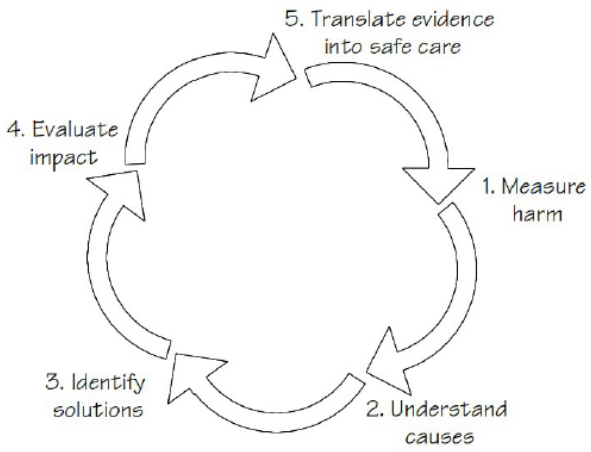

Figure 2.2: Reactive safety management cycle

case scenario is when an unknown event takes place and time and resources need to be spent before a response can be given this is why anticipation and proper problem recognition are so important.

2.2.3 Safety II

The view held by Safety II is that “Safety is more than the negation of risk” and “Safety is a dynamic non-event and non-events cannot be characterized or counted” [7].

The definition of safety depends on where in the scale of safety the system exists. If there is an abundance of accident data, the safety should be focused on analyzing and removing the apparent risk that these indicators prove. But as the number of negative occurrences is lowered, a shift must be made to the focus of Safety II.

Furthermore, the models and methods of Safety I assume that the systems are well behaved and understood. In contrast, the work environment is becoming increasingly intractable (an environment in which principles of functioning are partially unknown [8]. Consequently, Safety I methods are less and less effective. Safety II recognizes that these systems are in fact intractable and proposes a definition shift in safety from avoiding unacceptable outcomes to ensuring things go right.

Therefore, Safety II, sees the human factor as an asset because people can adjust their performance accordingly to match the conditions of work. People can detect and correct when something goes wrong or is about to, intervening before the situation escalates. Performance variability is seen by Safety II as positive factor since it represents adjustments necessary for safety, instead of a deviation from standards, as per Safety I.

Safety II seeks to manage this performance variability by acknowledging its presence, by monitoring and controlling it thus the emphasis is in anticipation rather than reaction.

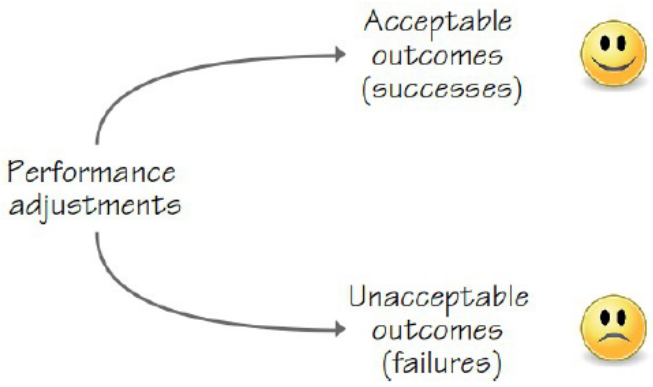

Figure 2.3: Safety II

2.2.4 Proactive safety management

From the Safety II perspective, the goal of safety management is to reduce failures and ensure acceptable outcomes. Proactive risk management deals with issues before they come up and therefore affecting how they happen or even prevent them from happening. More specifically, proactive safety management, tends to use history patterns to make policy/procedure decisions based on anticipation.

A big advantage is that by providing an early response, a smaller effort will be required since the consequences of the event had little time to develop and spread, saving valuable time and resources.

On the other hand, such type of safety management requires a deep understanding of how the system works, how it interacts with an ever evolving environment and its inter-dependable processes. This is why patterns are so important. They give insight on relations across events. Furthermore, since the future is uncertain, predictions can fail or be imprecise, leading to wrong or even unnecessary provisions.

Proactive safety management requires taking a degree of risk, allocating resources to provide early responses and predictions that might fail. However, if this approach isn't pursued, the aftermath of some serious adverse outcome happening will be far more costly.

2.2.5 Predictive safety management

Growing from reactive and proactive safety management, predictive safety management emerges.

Predictive safety goes a step further when comparing it with proactive safety. It uses normal operational data, and not only significant, accident data, to determine the potential risk and avert an accident that has not happened (yet).

Figure 2.4 depicts a scale of how the definitions presented in the previous subsections may be viewed with reactive at one end and predictive at the other.

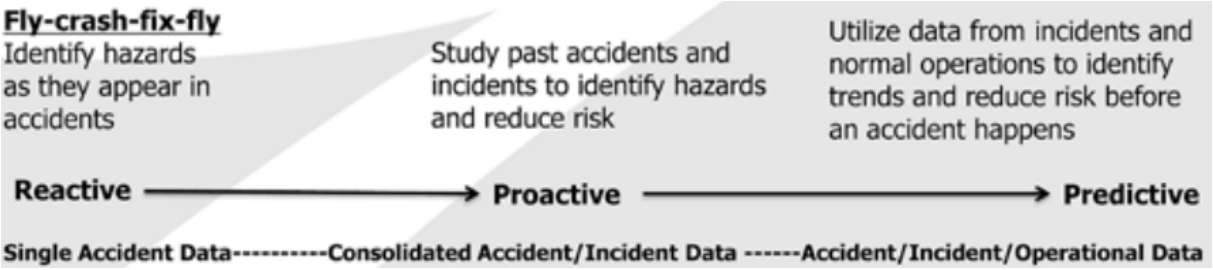

Figure 2.4: The spectrum of safety [9]

Basic risk management tells us that identifying hazards, and then evaluating the probability and severity of the hazard, enables us to determine the risk.

The key in predictive risk management is data. Data allows us to use predictive capabilities to further reduce risk. Decision makers including individuals, organizations, and the safety and regulatory systems themselves, are reactive by nature [9]. Making use of the multitude of normal operational data available coupled with today's data analysis capabilities we can identify hazards previously only discovered by an accident or a serious incident. In order to be predictive we must be able to use this normal day to day operational data and modern data processing tools to show the potential risks and what the current risk trends are.

Our current safety system focuses on negative outcomes, not events. If we act on negative outcomes only, we will, at best, be in proactive and normally in reactive risk management. However, if we use incident and normal operational data in our prediction process we will be able to show that we reduced the risk of an accident without having to react to one.

2.3 Safety management system

A SMS is a term used to refer to a system that deals with safety characteristics throughout an organization. The system offers a systematic way of categorizing hazards and managing risks guaranteeing that these controls are effective. A SMS is expected to be assimilated into an organization and becomes part of the culture; the manner people do their job.

A SMS can be defined as:

" (...) a businesslike approach to safety. It is a systematic, explicit and comprehensive process for managing safety risks. As with all management systems, a safety management system provides for goal setting, planning, and measuring performance. A safety management system is woven into the fabric of an organization. It becomes part of the culture, the way people do their jobs." [10]

It is universally accepted that safety is the number one priority in aviation. Howbeit, it is no secret that

the main purpose of the industry is to make money, to achieve production objectives, to deliver a service and to eventually deliver dividends to stakeholders. The truth is that aviation organizations are business companies and that none has been created to deliver only safety. Keeping this in mind, in order to give safety the same importance of other functions, it has to be considered as a specific organizational process delivered through a dedicated management system.

There are four components of a SMS that represent its two core operational processes as well as the organizational arrangements that are necessary to support it. These four pillars are:

- Safety policy;
- Safety risk management;
- Safety assurance;
- Safety promotion.

The main activities are safety risk management and safety assurance, but they can only be in place under a set of declared policies which have in turn to be supported by safety promotion.

Table 2.1: SMS components

Safety policy and objectives
Management commitment and responsibility
Safety accountabilities
Appointment of key safety personnel
Coordination of emergency response planning
SMS documentation
Safety risk management
Hazard identification
Safety risk assessment and mitigation
Safety assurance
Safety performance monitoring and measurement
The management of change
Continuous improvement of the SMS
Safety promotion
Training and education
Safety communication

Each one of these four components is divided into elements, which encompass the specific subprocesses, tasks or tools that the actual management should engage or use.

By extending the responsibility for safety, through these four pillars, across all levels of the organizations the chance of a threat endangering the organization is greatly reduced. This follows Reason's Swiss Cheese Model Fig. 2.5 which likens human-machine systems to multiple slices of swiss cheese. [11] These layers stacked side by side, in which the risk of a threat becoming a reality is mitigated by the differing layers and types of defenses which are "layered" behind each other. Therefore, in

theory, lapses and weaknesses in one defense do not allow a risk to materialize, since other defenses also exist, to prevent a single point of weakness.

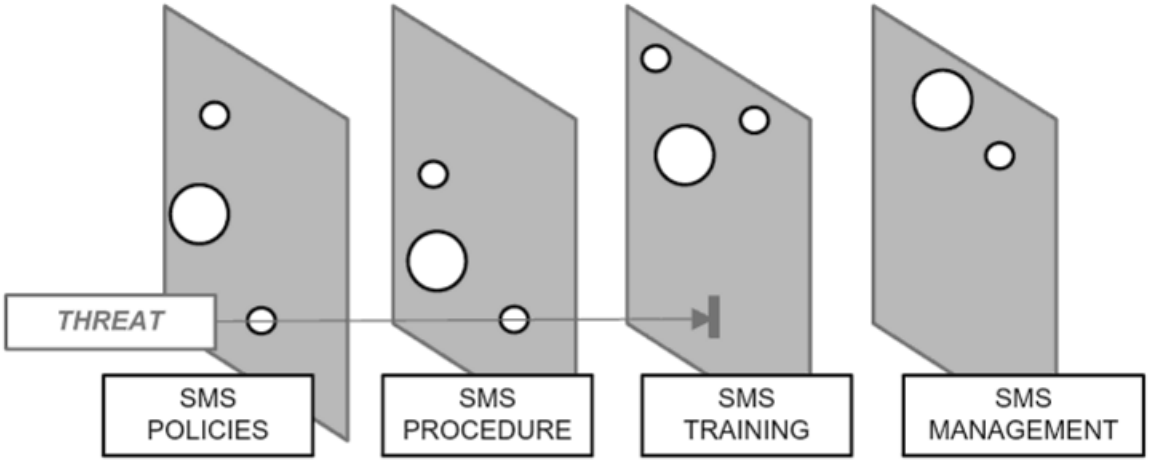

Figure 2.5: Example of successive layers of safety in a proactive SMS, with a threat affecting policy and procedures but being blocked by proper safety training. [12]

2.3.1 Safety policy

This first element can often appear as a sterile declaration of intents but every type of management system must have its policy, organizational structures and procedures defined to achieve its goals. These policies and procedures must explicitly describe responsibility, accountability, authority and expectations. The safety policy manifesto of an organization is usually composed by:

- Management commitment and responsibilities;
- Safety accountabilities;
- Appointment to key safety personnel;
- Coordination of emergency response planning;
- SMS documentation.

Fundamentally, safety must be a core value in for the organization. The SMS policy must be clear in including requirements for all areas to document their procedures, training and management systems. Principles of quality management are extensively used but the requirements to be managed are based on a safety risk assessment rather than conventional commercial goals such as customer satisfaction. It outlines the kind of resources, both human and financial, which are to be reserved to SMS, to commit to the highest standards of safety and to be compliant with national and international regulations.

Furthermore, SMS recognizes the complex and ever evolving industry environment in which different agencies and organizations are responsible for maintaining the highest levels of safety. Therefore, the roles, responsibilities and relationships of the difference stakeholders should be thoroughly described being every interface between different domains be clearly identified.

All members within the organization must know their responsibilities and be actively involved with respect to safety. However, the ultimate responsibility cannot be delegated. As a result, executive senior management involvement in safety activities is a crucial requirement in SMS policy documentation. This involvement can be translated in incorporating safety in strategic plans and laying out the steps needed to reach them. Safety performances targets, action plans and safety performances indicator and periodic management review of the SMS further demonstrate this engagement.

This document is the starting point to ensure efficacy and efficiency to the organization's SMS.

2.3.2 Safety Risk Management

A SMS is, at its core, a dynamic risk management system. According to ICAO Doc 9859, risk management is:

"The identification, analysis and elimination (and/or mitigation to an acceptable or tolerable level) of those hazards, as well as the subsequent risks, that threaten the viability of an organization." [13]

In aviation operations, not all of risks can be eliminated, some risks can be accepted and some can be reduced do an acceptable level. Figure 2.6 demonstrates the sequential procedures to a robust SMS. These are the processes by which risk can be identified, measured, evaluated and controlled so that the highest standards of safety can be achieved. The whole process follows a logical pattern. Firstly, the organization defines the parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

Then, the hazards are identified. The third step is to assess the risk stemming from hazardous activities and determine whether the organizations are prepared to accept the risk. The fourth step is to find and identify the defenses that can control the risk. The fourth step is to examine whether risks are appropriately managed and use the feedback information to evaluate organizational changes.

Furthermore, effective Risk Management requires that the safety "cost-benefit" of the planned and implemented course of actions is analyzed, including the case of choosing a "do nothing" strategy. If it is decided to act for limiting the exposure to the identified risks, each risk control measure needs to be evaluated, to reveal possible latent hazards and dormant risks that may arise from activating that measure. Once these control measures are implemented, the organization needs to ensure they are engaged in a correct way, and this is achieved through a set of arrangements, processes and systematic

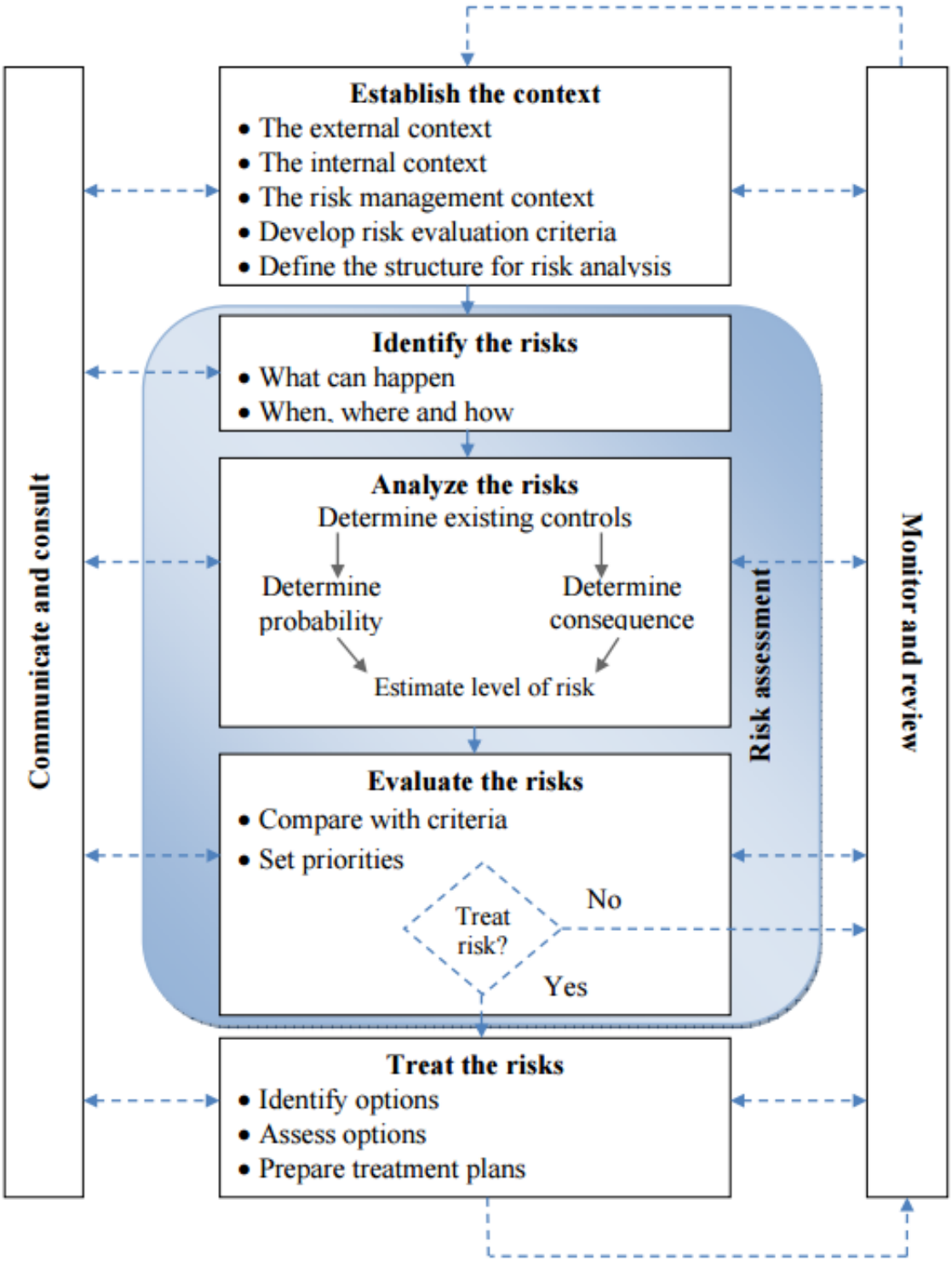

Figure 2.6: The Risk Management process according to ISO 31000 [15]

actions, which build the Safety Assurance domain of the SMS.

The risk management concept is equally important in all aviation sectors and should be implemented in a consistent manner by airline operators, air navigation service providers, certified aerodrome operators, maintenance and training organizations.

In other words, risk management is SMS in the making. It is effective risk management that contributes to a robust SMS.

Hazard vs Risk

Before going further into Risk Management, it is important to concretely understand the terms hazard and risk. These are oftentimes a source of confusion, but are crucial to the understanding of a SMS.

According to ICAO Doc. 9859: "A hazard is defined as a condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function." [13]

A hazard isn't necessarily something with a negative connotation. Hazards are an integral part of operational contexts, and their consequences can be addressed through various mitigation strategies to contain the hazard's damaging potential. Hazards can be found in all aspects which have a direct influence on aircraft operations and they do have the potential to cause harm.

Hazards may be classified as:

- Physical (mountains, obstacles);
- Human behaviors;
- Political;
- Environmental (weather);
- Legal;
- Technological;

In any case, hazard is something belonging to the present, it belongs to the system and its context, and it is in place before operational personnel "show up". On the other hand, consequences belong to the future; they do not manifest until an hazard interacts with the context. A hazard is the condition or circumstance that can lead to physical damage or loss. Therefore, it is of the up most importance to identify hazards and keep them under control.

Risk is an uncertain event or condition that, if it occurs, has an effect on at least one objective. Therefore, talking about risks also means the dispersion around an expected value.

ICAO defines “Safety risk as the assessment, expressed in terms of predicted probability and severity, of the consequences of a hazard, taking as reference the worst foreseeable situation”. [14]

The official definition of safety risk by ICAO takes into consideration the identified hazard and classifies it into two categories “probability” and “severity”. Safety risk is thus the scenario that follows when a hazard is accepted.

For example, an volcanic ash en route composes a hazard. This hazard could lead to at least three safety risks. The first safety risk would be that an aircraft might lose one or multiple engines while inside the ash cloud. The second safety risk is that the pilot, being aware that he/she is in an ash cloud, tries to climb out of it, further damaging the engine. The third safety risk is that the windshield and or electrical equipments are damaged and the pilot if forced to perform an emergency landing in an unknown airfield. In order to know the outcome of the hazard, where this might lead and what actions need to be taken, the safety risk has to be assessed.

2.3.2.A Hazard identification

Hazard identification represents the beginning of SMS practical activities. It is a systematic identification of undesired or adverse events that can lead to the occurrence of a hazard and the analysis of mechanisms by which these events may occur and cause harm.

The goal of hazard identification is to establish safe and effective procedures and practices by examining potentially hazardous activities. This can be achieved by both reactive (e.g., following the aftermath of an adverse outcome) and proactive (e.g., through safety events) methods and techniques.

Due to its daily nature, in order to keep an updated organization hazard list, it is of the utmost importance to put in place a smooth, simple and detailed data collection system which can gather data frequently at all company levels.

2.3.2.B Risk Assessment

Risk assessment is an evaluation in terms of criticality of their harmful effect and ranked in order of their risk-bearing potential. In other words, it determines the probability and consequences of a negative impact and then estimates the level of risk by combining the probability and consequences.

If the risk is considered acceptable, operation continues without further intervention. If it is not acceptable, the risk mitigation process is initiated.

In assessing the likelihood probability, all potentially valid perspectives have to be evaluated, making use of historical data and quantitative methods to mathematically access the probability of a risk event happening. The probability ranges are decided upon the annual average aircraft movements on the airport runway (i.e., 50,000 aircraft movements/year. An event is considered “extremely remote” if it occurs once a year.

Table 2.2: Likelihood of occurrence [16]

Quantitative Definition	Meaning	Value
Frequent ($x > 10^{-2}$)	Likely to occur many times.	5
Occasional ($10^{-2} > x > 10^{-3}$)	Likely to occur sometimes.	4
Remote ($10^{-3} > x > 10^{-4}$)	Unlikely, but may possibly occur.	3
Improbable ($10^{-4} > x > 10^{-5}$)	Very unlikely to occur.	2
Extremely improbable ($x < 10^{-5}$)	Almost inconceivable that the event will occur.	1

The other element, the risk-bearing potential, severity, has no models to express it in analytical terms. Thus, its evaluation is manly given by expert judgments.

Severity is given on a scale in numbers, as in Table 2.3.

Table 2.3: Severity of consequences

Aviation definition	Meaning	Value
Catastrophic	Aircraft / Equipment destroyed. Multiple deaths	5
Hazardous	A large reduction in safety margins, physical distress or a workload such that organizations cannot be relied upon to perform their tasks accurately or completely. Serious injury or death to a number of people. Major equipment damage.	4
Major	A significant reduction in safety margins, a reduction in the ability of organizations to cope with adverse operating conditions as a result of an increase in workload. Serious incident. Injury to persons.	3
Minor	Operating limitations. Use of emergency procedures. Minor incident.	2
Negligible	Little consequence.	1

In order to interpret the combination of risk probability and risk severity, the data is usually presented in a risk matrix. This matrix is custom created for the organization, encompassing the company's objectives, its environment, its production processes, its possible hazards. If the severity chart does fully represent the characteristics of the organization, its conclusions will be hard to interpret which will refrain us from designing proper mitigation actions.

Both the probability and severity columns are divided into a number of levels, each one of them characterized either by a range of values of probability, or by the description of the damages that can occur.

The risk classification usually falls in 3 categories:

- Acceptable: The consequence is so unlikely or not severe enough to be of concern; the risk is tolerable. However, consideration should be given to reducing the risk further to as low as reasonably practicable in order to further minimize the risk of an accident or incident.
- Review: The consequence and/or likelihood is of concern; measures to mitigate the risk to as low as reasonably practicable should be sought. Where the risk is still in the review category

Table 2.4: Risk tolerability matrix [16]

Catastrophic	5	5 Review	10 Unacceptable	15 Unacceptable	20 Unacceptable	25 Unacceptable
Hazardous	4	4 Acceptable	8 Review	12 Unacceptable	16 Unacceptable	20 Unacceptable
Major	3	3 Acceptable	6 Review	9 Review	12 Unacceptable	15 Unacceptable
Minor	2	2 Acceptable	4 Acceptable	6 Review	8 Review	10 Unacceptable
Negligible	1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Review
		Extremely Improbable	**Improbable**	**Remote**	**Occasional**	**Frequent**
		1	2	3	4	5

after this action then the risk may be accepted, provided that the risk is understood and has the endorsement of the individual ultimately accountable for safety in the organization.

- Unacceptable: The likelihood and/or severity of the consequence is intolerable. Major mitigation will be necessary to reduce the likelihood and severity of the consequences associated with the hazard.

If the risk falls in the red or yellow areas, then control measures have to be taken to increase the level of defenses against that risk or to avoid or remove the risk. In the red areas immediate action is required. In the case of the tolerable region, it is important to do a cost benefits analysis so the best compromise between safety, costs, and production can be found. This is important since it helps management establishing a balance between resources allocated to production and protection efficiency and safety.

The competition for the allocation of resources may lead to a management dilemma named the ”dilemma of the two Ps”. The ”dilemma of the two Ps” can be described as the conflict that arises at the management level due to the perception that resources must be allocated on an ”either basis” to what are believed to be conflicting goals: production goals (delivery of services) or protection goals (safety).

Figure 2.7 depicts a balanced allocation of resources to production and protection goals that results from organizational decision-making processes based on safety management as a core business function. Because the management of safety is considered just another organizational process and safety management just another core business function, safety and efficiency are not in competition, but closely intertwined. This results in a balanced allocation of resources to ensure that the organization is protected while it produces.

Regrettably, the history of aviation shows that effective resolution of the dilemma has not been commonplace. What history shows is a tendency for organizations to drift into an unbalance in the allocation of resources because of the perception of competition between production and protection. In cases

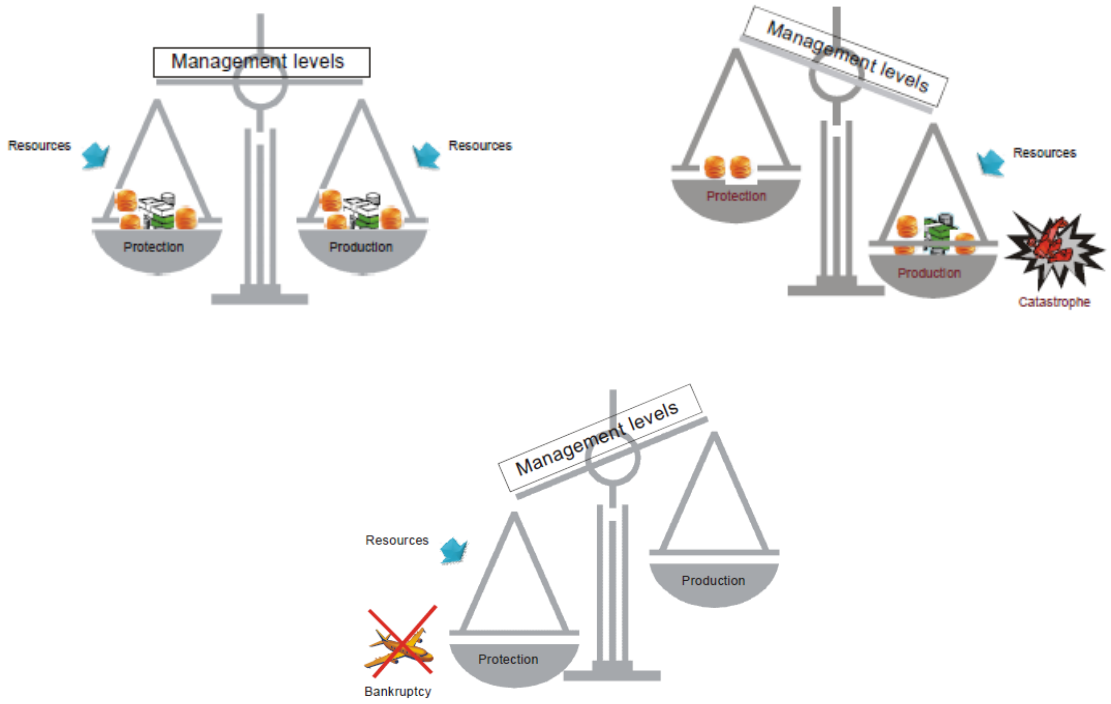

Figure 2.7: The dilemma of the two Ps [13]

when such competition develops, protection is usually the loser, with organizations privileging production objectives (albeit introducing numerous caveats to the contrary). Inevitably, as shown in Figure 2.7, such partial organizational decision making leads to a catastrophe. It is simply a matter of time.

Figure 2.7 shows an alternative to the partial allocation of resources discussed in the two previous paragraphs. In this case, the bias in the allocation of resources is towards the protection side of the balance, thus leading to bankruptcy. Although this alternative is hard to find in the annals of aviation history, it nevertheless alerts one to the importance of sensible organizational decision making regarding allocation of resources. In the final analysis, it is clear that the development of the "dilemma of the two Ps" is denied by an organizational perspective that focuses on safety management as a core business function, at the same level and with the same importance as other core business processes. In this way, safety management becomes part of the fabric of the organization, and an allocation of resources commensurate with the overall resources available to the organization is ensured.

2.3.2.C Controls

So far, the first two steps in safety risk management, hazard identification and risk assessment have been reviewed. The third major component is controls. Although safety risk management is the broadest concept in SMS controls are often a neglected part in literature. Since control of hazards is the ultimate

goal of safety risk management, it deserves the attention of SMS practitioners and is therefore, pertinent to be addressed.

Hazard control has four primordial steps:

- Ensure that the hazard is recognized and identified;
- Determine and select hazard controls;
- Assign responsibility for implementing control;
- Measure and monitor the effectiveness of the control.

The first step was discussed in section 2.3.2A and the fourth represents the third pillar of the SMS being presented in section 2.3.3. This subsection will focus on the remaining two steps.

Controls, also known as mitigations, are the last step of safety risk management. [4]. First of all, hazards are identified with its potential outcomes being then described. After this, the risk of those potentials is assessed and then, in order to mitigate the risk, controls are considered. Finally the risk is recalculated to determine if the residual risk is acceptable or not. These are the standard steps undertaken when assessing risk for new situations, in which there is little historical data.

However, aviation has decades worth of historical information. Using this information, one can more quickly see the relationship between existing hazards and controls. Because controls have been implemented in aviation since the beginning, a more intuitive way of addressing hazard control is to make use of decades' worth of development in this field. It is, therefore, interesting to enumerate hazards and controls together, as they often exist together, and then proceed to evaluate the effectiveness of those controls. This means that using this hazard/control pair method, instead of describing the potential outcomes of the hazards and finding controls to mitigate them, we identify existing controls associated with these hazards. It is however important not to neglect the importance to identify new hazards or inventing new controls. If we were to use the standard method, we would have to look at all this from ground zero, having to list all hazards associated with operations.

There is nothing wrong about the standard method approach but it is quite intellectual. Nowadays' reality is that there are already controls put in place to mitigate risks coming from most hazards. If these controls are effectively applied, the risk of a negative outcome is very low. The important point is that rather than focusing on a problem that has been solved before, we can concentrated the resources on the important questions concerning the effectiveness of our controls and the residual risk should those controls fail.

The hazard/control pair arises some interesting questions like "what controls do we presently have in place for controlling this hazard?", "what is the range of effectiveness of our controls for this hazard?", and "what is the residual risk if the controls fail"? Since no control system is 100 percent effective,

the SMS analyst should describe the controls' failure modes and to what extent the system can be compromised by those failures.

When the risk controls are determined they should be described in a clear, synthetic way and be implementable. This is, they should be ready to be used to diminish the organization's risk. Furthermore, risk controls ought to be duly documented so that someone unfamiliar with the process can gain an understanding of how and why certain controls were selected. Finally, responsibility for implementing the controls must be assigned to the appropriate people.

2.3.2.D Bowtie Method

One of the most effective ways of approaching risk and risk management in SMS is the Bowtie Method. This particular method is particularly relevant to the scope of this thesis since it as a structured one which assesses risk when a quantitative approach is not possible or desirable. Furthermore, it allows us to gain a greater visual understanding of hazards and how these are controlled both through preventative and mitigative measures.

The name Bowtie comes from the shape of its structure. It moves from an amount of different causes upstream to a single event and then, again, downstream to a number of consequences this resembles a Bowtie. The theory that supports the Bowtie methodology is the "Swiss cheese model" by Reason. [11] The beauty of the Bowtie model's concept is that it combines the causes (fault tree) and the consequences (event tree). [18] In this way, both the controls needed to prevent an undesired state, as well as how to mitigate the consequences if controls fail and the event occurs, are take in consideration.

At the top level, the Bowtie method is composed by two items, the hazard and the event that will accrue when the hazard is realized. As mentioned in section 2.3.2., a hazard is something which has the potential to cause damage. These can be found and listed through hazard identification. This is the first step in this iterative method. It is noteworthy to mention that only the hazards with the highest risks are selected for the Bowtie method. Normally these hazards are first classified using risk matrices as in Table 2.4. The event is the undesired event that results from the before determined hazards. This is the specific state that the organization is trying to avoid and it is typically the moment when control over the hazard is lost.

The threats, presented on the left in Figure 2.8 represent the conditions that lead to the event. On the right side we have the consequences that result from the event.

Every line through the Bowtie represents a different potential incident. In such a diagram, a proactive approach is clear: not only past incidents are represented but there is also room for occurrences that haven't happened before.

After assessing the threats and consequences it is important to know how to control these unwanted scenarios as an organization. In order to control these situations, barriers are used. Controls make their

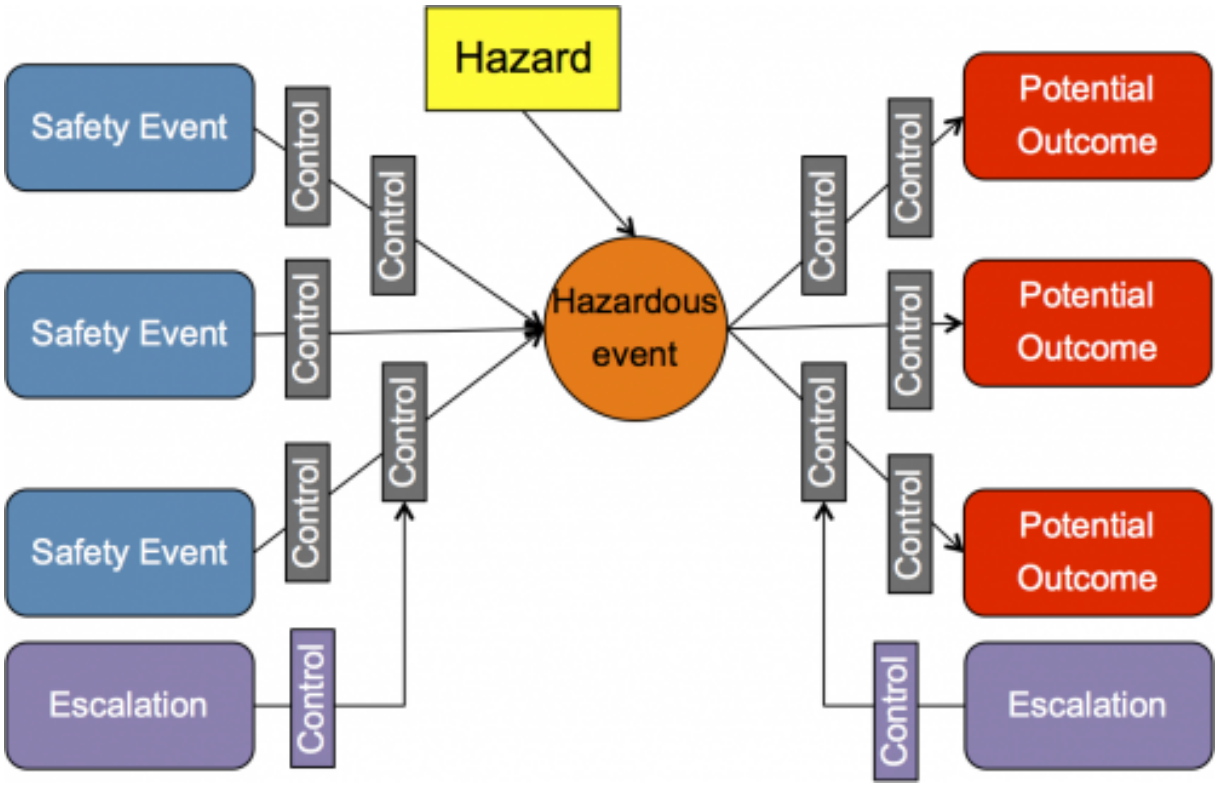

Figure 2.8: The Bowtie process involves the systematic identification of hazards and effects, assessment of the associated risks and the specification of the control and recovery measures which must be in place and maintained in place.

way on both sides of the Bowtie. They are subdivided in:

- Preventive controls: in the form of threat barriers mapped to each threat. They describe measures that either eliminate the hazard altogether or prevent the threat or top event;
- Recovery controls: in the form of mitigation or recovery barriers. They are linked to each consequence, indicating controls that reduce the probability or severity of the specific consequence.

Finally, there are escalation factors, that is, something that will make a barrier fail. So specific controls are designed to handle these factors, the so-called escalation factors barriers.

2.3.2.E SHELL Model

The SHELL model is named after the initials of its components, Software, Hardware, Environment, Liveware. it indicates relationships between people and other system components providing a framework for optimizing the relationship between people and their activities within aviation.

In the center of the model is the Liveware, which refers to the human beings in and affecting the system. The SHELL model is normally represented through 5 different squares encompassing each one

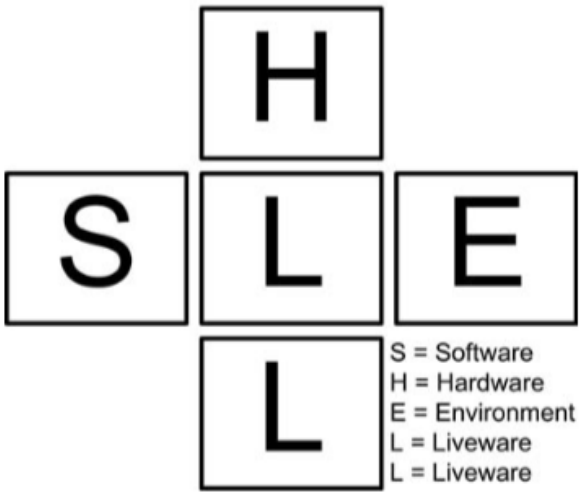

Figure 2.9: The SHELL model

of the components as in Figure 2.9. It is interesting to think of these squares not as regular shapes but as irregular ones, underscoring that people do not interface perfectly with other elements of the system. This requires an understanding of physical, physiological, psychological and psycho-social factors issues that all of us experience.Therefore, special attention has to be put on how humans interface with the system when predicting hazards and planning controls.

Liveware is at the center of the model and thus relates with all the other elements of the system.

- Liveware $\leftrightarrow$ Liveware - This is the interface between people. In aviation there are countless relations between people and groups in the workplace, including flight crews, air traffic controllers, management, airport authorities, regulatory authorities, amongst others. In this interface, we are concerned about communication styles, and personality differences, leadership. There is standardized training for certain aspects of this area, through different programs such as Crew Resource Management (CRM), the ATC equivalent - Team Resource Management (TRM), Line Oriented Flight Training (LOFT) etc. An example of a mismatch at the Liveware $\leftrightarrow$ Liveware interface is communication errors due to misleading, ambiguous, inappropriate or poorly constructed communication between individuals.

- Liveware $\leftrightarrow$ Software - This linkage refers to the relationships between the human and non-physical aspects of the system such as laws, rules, regulations, standard operating procedures conventions and the normal way things are done. It also concerns the computer-based programs developed to operate automated systems. An example of a potential hazard derived from the Liveware $\leftrightarrow$ Software relation is the misinterpretation of a checklist.

- Liveware $\leftrightarrow$ Hardware - Is the interface of the human operator and machine. The number of ways

in which we connect with our machines is nearly endless. Mismatches at this level may occur through badly designed or improperly used interface devices which can be a source of hazards. For example, the old 3-pointer altimeter was prone to improper reading as it was difficult for pilots to tell what information related to which pointer.

- Liveware $\leftrightarrow$ Environment This interface refers to the interactions between humans and the physical environment in which they operate. Political and economic considerations are also part of our environment. The appropriate matching of the Liveware $\leftrightarrow$ Environment interactions involve a wide array of disparate disciplines which adapt the environment to match human requirements Aviation is rich with examples of hazards and associated controls in this area. As an example, the reduced performance and errors stemming from disturbed biological rhythms due to long-range flying and irregular work-sleep patterns

Unless all potential effects of a change in the aviation system are properly addressed, it is possible that even a small system modification, as the introduction of a new hardware piece in the cockpit, may produce undesirable consequences. This is why it is important, upon the introduction of a change, assessing the impact of the change on operations and maintenance personnel (Liveware $\leftrightarrow$ Hardware) and the need for new or different procedures/training programs (Liveware $\leftrightarrow$ Software). Furthermore, the constant changes in the environment in which aviation works on demands a continuous review of the Liveware $\leftrightarrow$ Environment interface. All in all, the SHELL Model can be used to help clarify human performance needs, capabilities and limitations thereby enabling competencies to be defined from a safety management perspective. [20]

2.3.2.F TESEO

Quantitative methods are used in modern safety management and risk assessment. These methods are based on human behavior models and they are the product of years of studies as some of the parameters are empirical.

In this thesis, the TESEO (Tecnica Empirica per la Stima degli Errori degli Operatori) method is used to give a quantitative analysis to the case study. This method was developed in 1980 by Bello and Colombari [21]. The Human Reliability (HR) calculates the probability of an operator successfully completing the action in question. HR is calculated as:

$$HR = 1 - HU \tag{2.1}$$

where HU stands for Human Unreliability. Two important factors to take into consideration is that the operator can correct errors with a recovery and that an unsuccessful result occurs only when there is an uncorrected error.

Two other important concepts to introduce are the Human Error (HE) and the Probability of Recovery (PR). HE is the probability that the person makes a mistake, while PR is the probability to correct it. HE and PR are correlated using the following equation:

$$HU = HE(1 - PR) \tag{2.2}$$

There are different sources of data that can be used to define the TESEO method:

- data from experience of operation in real conditions;
- data from simulations;
- data from studies;
- data from experts through interviews.

The first type is preferable even if it is hard to come by. The second and third types are easier to obtain but these data must be corrected through coefficients. The last type requires expert analysts to analyze the data. Even after collecting the data, it is often times hard to compute HR and PR.

However, using the hypothesis that HE and PR can be represented as a function of the operator skills, the operator's failure probability can be computed as a multiplicative function of five parameters linked to:

- The type of activity to be carried out (K1);
- The time available to carry out this activity (K2);
- The human operator's characteristics (K3);
- The operator emotional state (K4);
- The environmental ergonomics characteristics (K5).

$$HU = K1.K2.K3.K4.K5 \tag{2.3}$$

If the value of HU is more than one, it will be assumed that $HU = 1$. This means that the likelihood of the operator successfully accomplishing the task is zero.

The values of each parameter can be obtained by consulting standard tables.

Table 2.5: Activity's typological factor [21]

Type of activity	K1
Simple, routine	0.001
Requiring attention, routine	0.01
Not routine	0.1

Table 2.6: Temporary stress factor for routine activities [21]

Time available (s)	K2
2	10
10	1
20	0.5

Table 2.7: Temporary stress factor for non-routine activities [21]

Time available (s)	K2
3	10
30	1
45	0.3
60	0.1

Table 2.8: Operator's typological factor [21]

Operator's qualities	K3
Carefully selected, expert, well trained	0.5
Average knowledge and training	1
Little knowledge, poorly trained	3

Table 2.9: Activity's anxiety factor [21]

State of anxiety	K4
Situation of grave emergency	3
Situation of potential emergency	2
Normal situation	1

Table 2.10: Activity's ergonomic factor [21]

Environmental ergonomic factor	K5
Excellent microclimate, excellent interface with plant	0.7
Good microclimate, good interface with plant	1
Discrete microclimate, discrete interface with plant	3
Discrete microclimate, poor interface with plant	7
Worst microclimate, poor interface with plant	10

Table 2.11 was built to detail the HU calculation for each event.

Table 2.11: Barrier failure table

Interaction type	Human factor	K1	K2	K3	K4	K5	Failure probability
L							
L-E							
L-S							
L-L							
Subtotal							

Where:

- L : liveware, the operator himself/herself;
- L-E : interaction between the operator and his/her work environment;
- L-L : interaction between operators working on the same task;
- L-S : interaction between the operator and all the non- tangible components involved in his/her job;
- L-H : interaction between the operator and tools used for the task;
- Human Factor: one or more human factors from the Dirty Dozen correlated to the operator's interaction
- K1, K2, K3, K4, K5: TESEO parameters;
- Failure probability : equals to HU
- Subtotal : the causal barrier/initial event final failure probability;

In order to decide the most adequate K factor, one should keep in mind how this specific human factor affects each k factor in order to make the barrier fail. It is important to recognize that events or human factor contributions can simultaneously occur. Therefore, they are non-mutually exclusive and independent. Thanks to probabilities rules, the total probability is given by the following equation:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{2.4}$$

Where:

- A and B : single event or human factor;
- $P(A)$: probability of event or human factor A, given through TESEO factors;
- $P(B)$: probability of event or human factor B, given through TESEO factors;
- $P(A \cup B)$: probability of not-mutually exclusive event;

- $P(A \cap B)$: probability of independent event, equals to $P(A).P(B)$.

Once that the probability of the initiating event and the success and failure probability of each causal barrier have been calculated, it is possible to evaluate the overall probability of occurrence of the incident sequence. since this sequence is composed by multiple elements, the interaction among them has to be classified. In this case, we simply consider the events as independent, being the final probability value given by:

$$p_t = \sum_{i=1}^{n} p_i \tag{2.5}$$

Where:

- p_t : overall probability;
- p_t : probability each single event
- n : number of causal barriers

2.3.3 Safety Assurance

Safety assurance measures and monitors the effectiveness of the controls. It ensures that organizations continuously practice their safety program and that their safety program remains effective, according to the safety policy, even as their operating environment changes. In order to do so, it monitors and evaluates and measures the activities performed for the delivery of services by the organization through internal auditing, analysis, and evaluation systems so integral to quality management.

Furthermore, this system contains a process to identify the need for new controls and manage possible changes, the so called management of change, that might affect the already established procedures. Safety assurance activities should ensure that these corrective actions are put in place, in a timely manner, so that the intended objectives are achieved.

Finally, the organization should develop a formal process to identify the causes of sub-standard performance of the SMS, determine the implications of sub-standard performance in operations, and eliminate such causes. Therefore safety assurance provides the feedback needed from risk management and completing the safety management cycle. This feedback is a good indication of the general performance of the SMS and will continually improve the safety performance of the organization.

2.3.4 Safety promotion

Safety promotion is an important part of an SMS setting helping to build a robust safety culture. This culture goes beyond merely avoiding accidents or reducing the number of incidents. It fills in the blank

spaces in the organization's policies, procedures and processes, providing a sense of purpose to safety efforts.

It is important that all employees take part in safety promotion and that they are supported and encouraged by senior management to actively report without fearing retaliation or any embarrassment among their peers.

Besides safety training and education which ensures that each one performs diligently performs their SMS duties, safety promotion relies in another element, safety communication. By disseminating lessons learned, the road to continuous improvement is opened.

The combination of training and communication strengthens and creates interactions between different domains of the organization, shortening the information journey, of safety-critical and "nice-to-know" information. Furthermore, it ensure that all staff are fully aware of the SMS and why particular actions are taken, namely change and/or introduction of safety procedures.

Finally it is important to note is that safety is continuously built by everyone's inputs and that reporting action should be encouraged, rather than punished, the so called "Just Culture", across all levels. The creation of a safety culture has a significant influence on the attitude and performance ("the professionalism") of the staff this will be reflected in their everyday work.

2.4 Human factors

The aviation industry can be viewed as a a socio-technical system. This notion means that safety management systems extend their interest not only to technical topics but also to human factors.

In order to ease the calculus of human failure probabilities, in the late 1980s, Transport Canada and the aviation industry identified 12 human factors, the so called "dirty dozen". These are human factors, elements that degrade one's ability to perform effectively and safely which could lead to maintenance errors. The components of this list are:

For the interactions between liveware and the working environment:

- Stress: Stress is the subliminal reaction to the requests set a person. We as a whole have some stress in our lives. This is natural and has no consequences until it becomes excessive. We must learn how to manage stress pressure, or it will highly increase the likelihood of a human error.

- Fatigue: It is considered the major factor to human error. It is easy to neglect it and to acknowledge exactly how much one's judgment is impeded until it is past the point of no return. This element can be coupled any of the other elements and aggravate it.

- Pressure: Pressure is always present in the aviation industry. Aviation professionals need to make many time sensitive decisions. Therefore, it is important to recognize and deal with pressure.

For the issues associated to an individual himself (Liveware):

- Lack of Awareness: The lack of awareness can be defined as the failure to be alert, vigilant or alert in the surrounding or in the job itself. Such incidents can lead to the failure to recognize the consequences of an action.
- Lack of Knowledge: This is an important element due to the constantly changing technology. Training is one of the best safeguards to counteract human error.
- Distractions: Distractions are common in one's life. Our mind often thinks ahead. This might take our mind off the job at hand even if for an instant.

For the interaction between the liveware and the hardware:

- Lack of Resources: A lack of resources can interfere with one's ability to complete a task give because there is a lack of supply and support. Low quality products also affect one's ability to complete a task.

For the interaction between individuals working together for the same purpose Liveware - Liveware:

- Lack of Communication: This is the failure to exchange information. Depending on the complexity of the message it might be effective to provide some form of written instruction such as a check-list.
- Lack of Teamwork: The larger an organization becomes, the more common this contributing factor is. The lack of teamwork can be define as the presence of a interdependent individuals who does not work together or communicate well with others to achieve a common set of goals.
- Lack of Assertiveness: This can be defined as how one is aware that certain method of doing is wrong but is not confident enough to question or clarify. However, assertiveness also calls for listening to the views of others before making a decision. Assertiveness is that middle ground between being passive and aggressive.

For the interaction between the individual and all the non-tangible components involved in his/her job (Liveware – Software):

- Norms: Norms are unwritten rules or behaviors, dictated and followed by the majority of a group. Norms can be positive and negative. A negative norm detracts from an established safety standard.

Finally, an universal human factor :

- Complacency: Complacency can be defined as how one gets over-confident in his work. This is often a self given satisfaction, one might think that since something has worked in the past, it will work the future. This is where the dangers of complacency kicks in. Typically, complacency is usually found in a person who has a lot of experience on the job or in one who has done a certain task multiple times.

2.5 Linking quality with safety

Understanding and recognizing quality in the spectrum of civil aviation is important.

Quality can be defined as "A measure of excellence or a state of being free from defects, deficiencies, and significant variations, brought about by the strict and consistent adherence to measurable and verifiable standards to achieve uniformity of output that satisfies specific customer or user requirements". [22]

From the customer point of view, quality has influence on travel demand and market share. For both regulators and carriers, the performance of carriers is of concern. Knowing the information and position can help to enhance the quality of carriers, especially when the outcomes of a specific aspect of quality, such as air safety, are engaging people's curiosity.

Quality programs and safety programs have the same components, this is, they are based on the same principles [23]. Using this idea, [24] defended that SMS and quality management system are in need of integrating together. Table 2.12 shows that quality and safety principles are essentially the same.

Table 2.12: The principles and relationship of quality and safety [24]

Safety	Quality
Goal: zero accidents	Goal: zero defects
Incident analysis	Event analysis
Written policies, procedures and guidelines	Documented policies, procedures and work instructions
Safety committees	Quality circles, employee involvement team
Employee participation	Empowerment
Statistical analysis	Control charts, statistical process control
All accidents are preventable	All non-conformances are preventable

Accordingly, based on the ICAO recommended practice [25], an operator ought to establish an accident prevention and flight safety programme, which may be integrated with the quality system, including programs to achieve and maintain risk awareness by all persons involved in operations.

In terms of organizational structure, Federal Aviation Administration (FAA) suggested that the Flight Safety Officer has a similar position to Quality Manager. When the management functions of safety and quality are the same, these two positions can be combined in one, as some airlines do. Also the United

Kingdom (UK) Civil Aviation Authority (CAA) states that in small and medium sized companies, the Flight Safety and Quality tasks will have many common points and both roles can be combined in one staff member [26].

Furthermore, the operator shall design and run a quality system to demonstrate regulatory compliance. In addition, the ISO 9000 offers important information, advising that procedures should be documented only where a lack of documentation may detract from quality. Yet it is worth noting that the decision as to whether or not it does detract from quality (or safety) is a crucial one and should only be taken by a person or committee fully competent to make such a decision.

3

EASA Regulatory Framework

Contents

3.1 EASA

The European Aviation Safety Agency EASA is an European Union (EU) agency established in 2002 and based in Cologne, Germany. The mission of the agency is to ensure a high and uniform level of protection of the European citizen in civil aviation by adoption of common safety rules and by measures ensuring that products, persons and organizations in the Community comply with such rules and with those adopted to protect the environment. [17]

EASA took over the responsibilities of the former Joint Aviation Authorities (JAA) which ceased to exist in 2009. EASA isn't, however a successor, in legal terms, to the JAA. EASA has legal regulatory authority within the EU through the enactment of its regulations through the European Commission and European Parliament, while most of the JAA regulatory products were harmonized codes without direct force of law. This means that the main difference between EASA and JAA lies in the fact that the first uses National Aviation Authorities (NAAs) to implement its regulations while the second relied upon the participating NAAs to apply its harmonized codes without having any force of law.

3.2 Relationships between production, SMS-Provider and SMS-Oversight

ICAO separates safety oversight, state's responsibility, a role of the regulatory authority, and safety performance monitoring, a responsibility of the operator and service provider. In Doc 9734-AN/959 [27], ICAO identifies the critical elements for a state oversight system:

- Primary aviation legislation.
- Specific operating regulations.
- Civil aviation structure and safety oversight functions.
- Technical guidance material.
- Qualified technical personnel.
- Licensing and certification obligations.
- Continued surveillance obligations.
- Resolution of safety issues.

Safety oversight is an integral component of an effective SMS program. Its purposes are:

- Demonstrate compliance with rules, regulations, standards, procedures, and instructions.

- Provide an additional method for pro-actively identifying hazards.
- Validate the effectiveness of safety actions taken.
- Evaluate safety performance.

In the case of the Portugal, the regulator is Autoridade Nacional da Aviação Civil (ANAC). While some of the functions identified by ICAO occur at the national level, many of them occur at the operational level. The state engages in oversight through rule-making, standards setting, accident investigation (in Portugal by Gabinete de Prevenção e Investigação de Acidentes com Aeronaves e de Acidentes Ferroviários (GPIAAF), enforcement (sanctions or fines), education, inspection (no-notice and scheduled), safety audits, and surveillance activities.

According to the size and complexity of an organization, different methods are used to monitor their safety performance. These means include:

- Safety audits. Develop identified safety performance indicators and targets.
- Quality assurance. It shows that quality related activities are effective, reducing risks. Furthermore, it assures that the necessary elements to ensure that a product meets the needs and requirements of customers are met.
- Vigilance. Training people to be vigilant is a key part of the work culture. Vigilance from all parties dramatically contributes to higher safety performance levels.
- Surveys. These are a good mean of assessing the attitudes towards safety and they can reveal systemic hazards that may compromise it.
- Inspections. They provide the opportunity for regulators and the organization itself to observe actual work practices and performance as well as and assess safety conditions.
- Data analysis. Establishing methods for collecting data that can be monitored and used to determine the safety performance of the organization.
- Systematically review all available feedback from daily self-inspections, assessments, reports, safety risk analysis, and safety audits.
- Communicating findings to staff and implementing mitigation strategies, and others.

Figure 3.1 represents the relationship of SMS-P (provider) and SMS-O (oversight). On the protection side of the model are the NAA SMS-O, with the goal of public safety, and the operator's SMS-P, which aims to control safety risk. These systems interact with one another through audits and approvals.

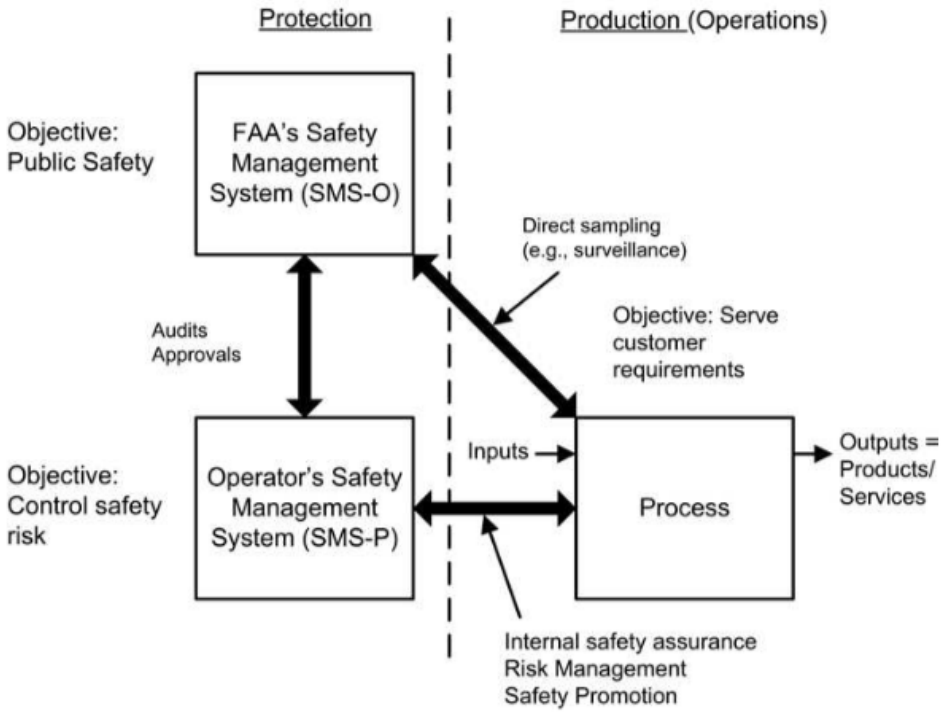

Figure 3.1: System relationships

The activities that produce products and/or services to serve the customer's requirements are on the production side. These processes interact with the SMS-O through direct sampling such as surveillance, and with the SMS-P through internal safety assurance, risk management, and safety promotion.

SMS programs implemented by the organizations and the NAA should relate to each other from the beginning. In this way, both programs can be connected allowing a greater degree of harmonization and compatibility, strengthening the relationship between the regulators and the aviation service providers. This can be achieved, for example, through procedures for data collection and sharing.

3.3 Safety State Program

An SSP is a method for a State to fulfill its safety responsibilities, by integrating its multi-disciplinary safety activities into a coherent whole. Developing an SSP requires 4 core components, also known as building blocks of an SSP and they are;

- State safety policy and objectives
- State safety risk management
- State safety assurance

- State safety promotion

Safety risk management and State safety assurance are known to be core operational activities of an SSP taking place under state safety policy and objectives, supported by the state safety promotion. The collaboration between the SSP and SMS promotes an effective interaction between the State and service providers in the resolution of safety concerns.

One of the main objectives of an SSP is supporting the implementation of an effective SMS by the service providers. Indeed, a service provider's SMS cannot be effective without a SSP to assess the service provider's adherence to the regulations when implementing SMS.

The acceptable level of safety to be achieved by an SSP shall be established by the State. The Level of safety is the degree of safety of a system. It is expressed through safety indicators. These are the parameters that characterize or typify the level of safety of a system. Safety indicators in aviation include, for example, fatal airline accidents and air proximity events.

3.4 Regulations structure

The Basic Regulation (BR) is part of the EU air transport regulatory framework. It is valid in the 27 EU and 4 European Free Trade Association (EFTA)[1] States.

BR covers different areas airworthiness and environmental protection of aircraft, pilots, air operations aerodromes Air Traffic Management (ATM)/Air Navigation Services (ANS) and Air Traffic Controllers. However the material scope of BR does not cover the situations in Table 3.1

Table 3.1: Situations not covered by Basic Regulation (EC) No 216/2008

Airworthiness and environmental protection of aircraft	- while carrying out military, customs, police, SAR, fire fighting, coastguard or similar services - when referred to in Annex II
Pilots and operations	- of aircraft referred to in Annex II, unless used for commercial operations
Aerodromes	- that are controlled and operated by the military - not open to the public, not serving commercial air transport, not providing operations using instrument approach or departure (or) having paved runway of less than 800m (unless exclusively serving helicopters)
ATM/ANS	- that are provided or made available by the military

[1] Iceland, Liechtenstein, Norway, and Switzerland

The main objective of BR is to establish and maintain a high uniform level of aviation safety in Europe. The structure, at the European level, of aviation regulations is summarized in Figure 3.2.

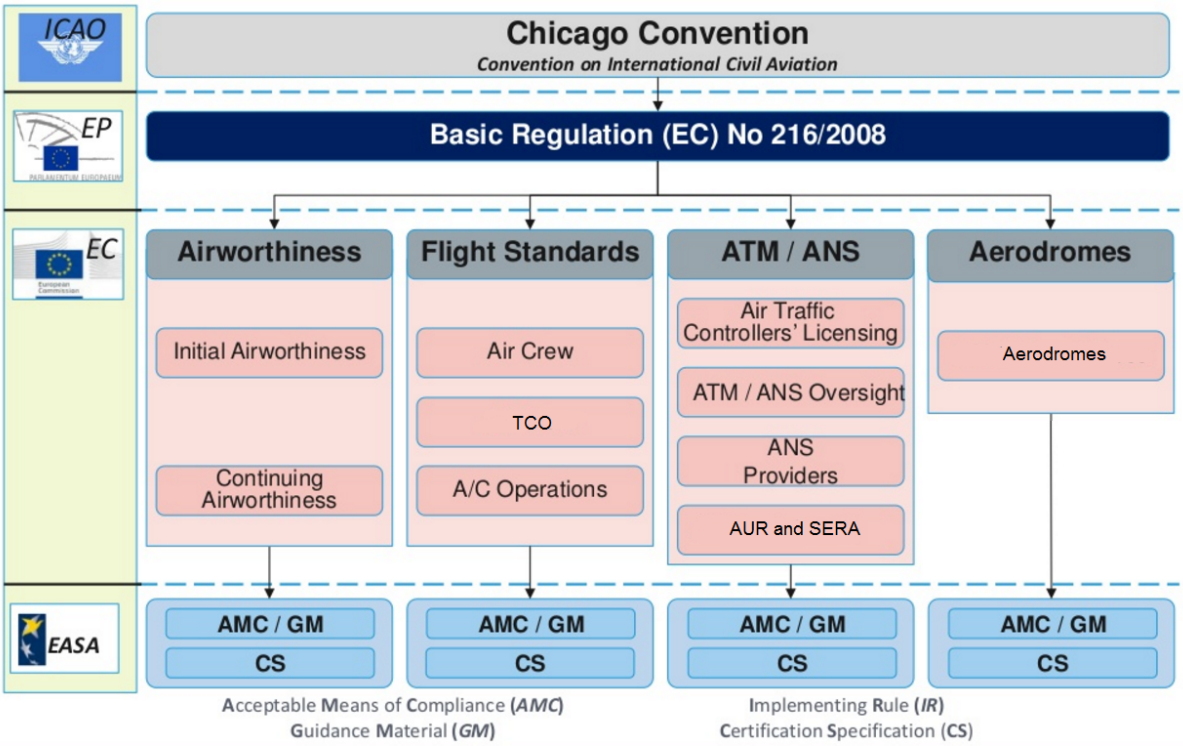

Figure 3.2: European aviation rule structure

The Implementing Rules (IR) are further subdivided in parts. Each part to each IR is composed by:

- AMCs are non-binding standards adopted by the Agency to illustrate means to establish compliance with the Basic Regulation and its implementing rules
- Alternative Means of Compliance (AltMoC) refers to those means that propose an alternative to an existing acceptable means of compliance or those that propose new means to establish compliance with BR and its implementing rules for which no associated AMC have been adopted by the Agency;
- GM means non-binding material developed by the Agency that helps to illustrate the meaning of a requirement or specification and is used to support the interpretation of the BR, its implementing rules and AMC.
- Certification Specifications (CS) are technical standards adopted by the Agency indicating means to show compliance with the BR and its implementing rules and which can be used by organizations for the purpose of certification;

These elements are amended along with the amendments of the regulations. They are called ”soft-law” as they are non biding and are written as EASA decisions.

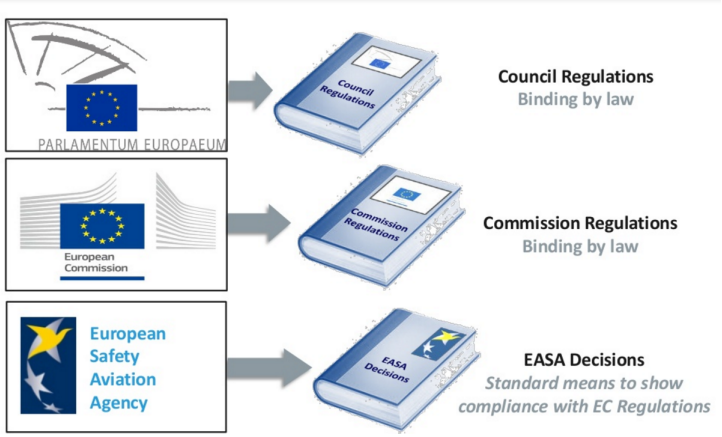

Figure 3.3: Decision levels

3.5 Current rule-making status regarding SMS

EASA is creating a performance based regulatory environment with common standards across all regulations which are enabled by EASA BR 216/2008 [2]. Specific Focus on Management and Safety Systems is evident.

The current EU Regulations that mandate SMS assessment are as follows:

- Commission Regulation (EU) 290/2012 [28] ”Aircrew”;
- Commission Regulation (EU) 965/2012 [29] ”Air operations”
- Commission Regulation (EU) 139/2014 [30] ”Aerodromes”;
- Commission Regulation (EU) 2015/340 [31] ”Air traffic controllers’ licenses and certificates”;
- Commission Regulation (EU) 2016/1377 [32] ”Common Requirements (CR) for ANSP and the oversight in ATM/ANS” require competent authorities to assess how organizations identify aviation safety hazards and how they manage the associated risks and to consider the effectiveness of the SMS as part of their oversight.
- Commission Regulation (EU) No 1216/2011 [33] and Regulation 390/2013 [34] ”Performance Scheme Regulation, for air navigation services and network function” require ANSP to periodically answer Effectiveness of Safety Management (EoSM) and Just Culture questionnaires.

In addition to the ANS Performance based IR requirements, EU Regulations will require (for those domains where SMS requirements have not yet been issued) organizations to monitor the effectiveness of their risk management and authorities to consider the effectiveness of the SMS as part of their oversight.

Apart from the ANS Performance based IR, EoSM and Just Culture questionnaires, the Safety Management International Collaboration Group (SMICG) has developed an evaluation tool, which was designed with the purpose of measuring the performance of an SMS. It is noted that:

- The SMICG evaluation tool has been developed to accommodate cross domain assessments and has been successfully tested in some EASA states. However, the tool does not meet the requirements of the ANS Performance IR objectives and is not fully aligned with the standards and recommended practices of ICAO Annex 19 [4].
- A gap analysis performed by the UK CAA regarding the differences between the SMICG evaluation tool and both the EoSM and Just Culture questionnaires identified many similarities.

Table 3.2: Status of SMS requirements for the different organizations

	Airworthiness	Flight Standards	ATM/ANS	Aerodromes
Implemented	x	✓	✓	✓
Currently applies	x	✓	✓	x
Applies by the end of 2017	x	-	✓	✓

3.5.1 Flight Standards

3.5.1.A Aircrew

Comission Regulation (EU) No 290/2012 [28], which lays requirements and administrative procedures related to civil aviation aircrew pursuant, applies to approved pilot training organizations. This regulation applies since April 2013 for Approved Training Organizations (ATOs) training for Airline Transport Pilot License (ATPL) and Commercial Pilot License (CPL).

Specifically in Annex VI, "Authority Requirements for Aircrew", Part-ARA, Subpart-Gen, the requirements for a SMS are set. Namely the oversight programme clearly explicits the need for:

- SMS documentation;
- Hazard identification;
- Safety performance monitoring, management of change, continuous improvement of the SMS;
- Safety communication.

3.5.1.B Third Country Operators

Any third-country operator that intends to perform Commercial Air Transport (CAT) operations into areas where BR applies require a Third Country Operators (TCO) authorization issued by EASA. A TCO authorization is not required for operators only overflying these territories without intended landing.

The TCO requirements cover such areas as: personnel licensing, rules of the air, operation of aircraft, airworthiness, dangerous goods, and Safety Management to include SMS. In order to release a TCO certificate, the Agency assesses the compliance of said operator with the above mentioned requirements which are stated in Comission Regulation (EU) No 452/2014 [35].

The TCO authorization process managed by EASA requires operators to comply with applicable ICAO standards and to make certain declarations to EASA. The applicable ICAO standards include those in Annex 19 (Safety Management) to the Chicago Convention. Annex 19 standards require Air Operator Certificate (AOC) holders authorized for international commercial air transport to establish an SMS acceptable to the State of the Operator, in accordance with the framework elements contained in Appendix 2 of Annex 19, and commensurate with the size and complexity of operations [4]. Comprehensive guidance on the implementation of the framework for an SMS is contained in the Safety Management Manual (SMM) (ICAO Doc 9859), including a phased implementation approach [13]. In this regard, EASA, in the ambit of TCO authorization, requires operators to establish an SMS and declare the maturity of their SMS corresponding to the four implementation phases proposed as per the ICAO SMS framework.

- Phase 1: Compliance document, planning group, system description, Gap analysis, SMS implementation plan, safety policy and objectives, means for safety communication
- Phase 2: Hazard identification and risk assessment and mitigation (reactive processes), training, relevant documentation
- Phase 3: Hazard identification and risk assessment and mitigation (proactive and predictive processes), training, relevant documentation
- Phase 4: Acceptable level of safety, safety indicators and targets, continues improvement, training and documentation to safety assurance

3.5.1.C Air Operations

The introduction of EASA Air Operations SMS requirements were the foundation for the Agency's move towards establishing a performance-based environment at a total system level, where safety is pro-actively driven to be ever more effectively managed.

Commission Regulation (EU) No 965/2012 [29] on Air Operations was published in October 2012 and applies since October of 2014.

Similarly to TCO, for CAT, Non Commercial Complex (NCC) and Specialized Operations (SPO), one of the most significant points is that operators need to demonstrate that they have a management system that can identify and manage the risks as appropriate to the size, nature and complexity of its operations.

3.5.2 ATM/ANS

Since the late 1990s due to the continuing traffic growth that ANS have been implementing SMS being the first domain to do so in aviation.

According to ICAO Annex 11 - Air Traffic Services, "States shall require, as part of their safety programme, that an air traffic services provider implements a safety management system acceptable to the State that, as a minimum [36]:

- identifies safety hazards;
- ensures that remedial action necessary to maintain an acceptable level of safety is implemented;
- provides for continuous monitoring and regular assessment of the safety level achieved; and
- aims to make continuous improvement to the overall level of safety."

Commission Regulation (EU) No 677/2011 [37] which is in force addresses these points.

In 2016, Commission Regulation (EU) No 2016/1377 [32] was published and will apply from 2019 onwards. It addresses SMS for both ANS and ATM further reinstating the need for an SMS for these domains as an integral part of the whole management system. This SMS should include the components presented in Table 2.1.

3.5.3 Aerodromes

For more than 10 years commercial aerodromes should have implemented a functioning SMS, based on ICAO requirements and Guidance Material (i.e. ICAO SMM Doc 9859 [13]), or national regulations.

With the introduction of Commission Regulation (EU) No 139/2014 [30] of 12 February 2014 EASA has now assumed responsibility on behalf of the member states to manage the criteria by which member states will demonstrate compliance with ICAO Annex 14 - Aerodromes [38].

The regulation contains the rules for the certification, management, operation and design of aerodromes. Furthermore the regulation is supported by AMC, CS and GM all provided by EASA.

Airports open for commercial air transport with at least one paved runway of 800 meters or more are affected by it. EASA pledges to achieve maximum conformity with Aerodrome Rules in ICAO's Annex 14 [38].

The focus of the new regulation and the forward view of EASA across the entire regulatory environment and its requirements is on a performance-based regulatory system which promotes an operational and management common safety standards for aerodromes across Europe.

As with other EASA regulations there are a number of concepts which are somewhat new to both the European Authorities and the Aerodrome Operators.

Key features, in line with Annex 19 [4], include the implementation of an effective management system which includes a system to manage safety - SMS as well as Quality and Compliance. This reflects the need to integrate the various sub-systems used for the management of the different activities of an aerodrome organization (e.g. management of aeronautical data and related activities).

As part of the management system, aerodrome operators are required to take a major responsibility for their own oversight, through performance monitoring and measuring.

The relevant provisions on the management system of aerodrome operators are laid down in Subpart D of Annex III of Regulation (EU) No 139/ 2014 [30](Part ADR.OR), as well as in the related AMC and GM.

During the transition period, NAAs and aerodrome operators will need to build an effective working relationship to achieve the transition on time, comply with all European rules and to maintain a useful basis for continuing oversight and certificate validity; fully understanding the new requirements is the first step of this process.

Competent authorities involved in the certification and oversight of aerodromes, aerodrome operators and apron management service providers shall comply with the requirements laid down in Annex II to this regulation before 31 December 2017.

3.5.4 Airworthiness

According to ICAO Annex 8 Airworthiness [39] is the measure of an aircraft's suitability for safe flight. Certification of airworthiness is initially conferred by a certificate of airworthiness from a national aviation authority, and is maintained by performing the required maintenance actions. The airworthiness of aircraft therefore ranges from the initial approval of a new aircraft design to ensuring an aircraft's on-going safety standards.

3.5.4.A Initial Airworthiness

Under the current Commission Regulation (EU) No 748/2012 [40] of 3 August 2012 which lays down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organizations, there are no SMS requirements.

When ICAO Annex 19 "Safety Management" [4] became applicable on 14 November 2013, Contracting States were obliged to mandate organizations responsible for the type design or manufacture of aircraft' (D& M organizations) to implement a SMS. Annex 19 [4] requires that the States establish a SSP to manage safety in the State, establishing and implementing State safety oversight over the State's aviation activities and functions. Thus, the aircraft type-certification function is subject to the State's safety oversight [27].

EASA, as the executive body of the EU in the domain of aviation safety, carrying out on behalf of the EU Member States the functions and tasks of the State of Design (and also the State of Manufacture or Registry) when related to design approval, is then obliged to to introduce the Safety Management principles of Annex 19 [4] into the implementing rules of Part-21 [41]. EASA's scope of implementation of Annex 19 SMS principles is wider than ICAO requires and also covers organizations designing and producing engines and propellers.

In March 2015, EASA released a Notice of Proposed Amendment (NPA) on "Embodiment of Level of Involvement into Part-21" NPA 2015-03 [42]. Meanwhile this implementation is tested in various pilot certification projects and the SMS will be addressed in a second stage.

3.5.4.B Continuing Airworthiness

There are currently no SMS requirements for Approved Maintenance Organization (AMO) and Continuing Airworthiness Management Organization (CAMO) for maintenance of aircraft and/or components in the last Commission Regulation (EU) 1321/2014 [43] addressing these organizations. It is important to stress that there are no ICAO SARPs considering a dedicated organization approval for continuing airworthiness management.

However, EASA is creating a new annex, Vc "Part-CAMO", that will supersede the current Subpart G of Annex I (Part M) to Commission Regulation (EU) 1321/2014 [43].

The SMS will only apply to organizations that are:

- managing aircraft used in Commercial Air Transport; and
- managing Complex Motor Powered Aircraft (CMPA).

An opinion from the Agency is expected in the end of 2018 with an amending regulation addressing these issues in 2019.

4

Cross Domain Assessment

Contents

As we saw in previous chapters, the majority of the organizations have already SMS requirements.

This chapter serves as a basis to assess how the above mentioned organizations would prevent the outcomes of the events presented in the case study or, in the case that they do happen, react. This specific case was chosen because it involves the participation of different organizations and where cross domain SMS is specially important for an effective risk management.

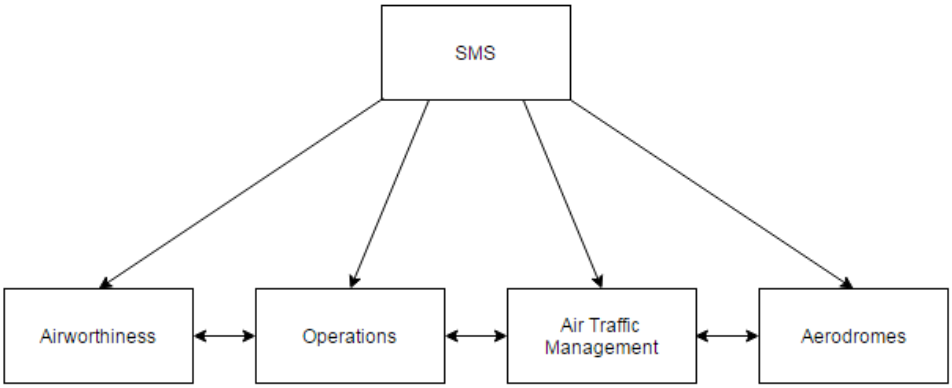

Figure 4.1: Communication between the different SMS

4.1 White Airways

White Airways S.A.is a Portuguese airline certified and licensed according to the applicable Portuguese and European standards. Since 2006, White is part of one of the biggest aviation groups in Portugal, OMNI Group.

White's fleet is composed by thirteen aircraft: two Airbus A319 CJ, one Airbus A320 for medium haul, one Boeing 777 for long haul, one Boeing 737 for medium haul and eight ATR 72 for short/medium haul [44].

The company serves mainly popular tourist destinations in South America, Europe and Africa. White does not sell tickets directly to the public. It specializes in Charter flights, Aircraft, Crew, Maintenance and Insurance (ACMI) and Wet-lease.

The aircrafts' maintenance is performed by Aeromec which a certified maintenance and engineering company part of OMNI group.

White Airways sets its mission as "To provide flexible and innovating solutions in an opportune time frame and with high standards of safety and quality within the scope of commercial air transport on a global scale, focusing on the requirements and expectations of passengers and clients, on the sustainable growth of the business, on the well being of employees and in social and environmental responsibility".

Furthermore, its vision is to ”be recognized by passengers, clients and the general public as an aircraft operator of reference in its business sector, for the high quality of its operation and for the flexibility, innovation and excellence of its services.” [45]

The values that orientate the management of White Airways and which represent its culture are:

- Safety - Respect for life and prevent occurrences which drive to personal injures or material damages as fundamental value and the first priority within the company;
- Passengers and Clients Satisfaction - Provide flexible and innovative solutions, with excellence standards, exceeding the expectations of passengers and clients and ensuring their loyalty;
- Innovation - Implementations of new or significantly improved solutions with the purpose of reinforce the competitive position, increase the performance, or the knowledge;
- Globalization - Operate on a global environment with the same safety and service excellence standards;
- Sustainability - Carry out the activities and utilize the resources on a conscientious manner, in order to ensure the company continuing viability and the employee's welfare;
- Social Responsibility - Respect for the health and well-being of employees, for the community and for the environment;
- Continuing Improvement - The permanent search for excellence, implementing the best practices and employing motivated and highly qualified persons.

4.2 ANA

ANA was funded in 1998 with the goal of running public airport service supporting civil aviation in Portugal.

In September 2013 was integrated in VINCI Airports International which manages a wide network of airports worldwide.

ANA manages 10 airports in mainland Portugal (Lisbon, Oporto, Faro and Beja Civilian Terminal), in the Azores (Ponta Delgada, Horta, Santa Maria and Flores) and in Madeira (Madeira e Porto Santo). In 2016, these airports accounted for 44,5 million passengers, an increase of 14,5% when compared to 2015 [46].

ANA also holds the total share capital of Portway, a handling company and a number of non-aviation businesses such as car rental and parking services. The turnover of the ANA group in 2016 was of 657,8 million euros.

ANA's mission is "to efficiently manage our airport infrastructures and to contribute toward the economic, social and cultural development of the surrounding communities". Furthermore it sets itself to provide a world-class service to its customers while motivating its collaborators and enthusing the shareholders.

ANA's vision statement is to achieve a profitable and sustainable business, by positioning our company among the best managed airport operators of comparable size, leveraging the relationship with customers and stakeholders.

The values which are sought to be incorporated into the company's culture are:

- Customer Satisfaction - Focusing on understanding the customers' needs and fulfilling them flawlessly.
- Integrity - Honoring the commitments with customers, communities, shareholders and stakeholders, in a professional and respectful manner.
- Innovation - Continuous strive for improvement, encouraging an open-minded and creative approach to management.
- Team Spirit - Aiming to learn, communicate, and share ideas and resources, prizing individual work as a crucial part of the whole organization.
- Employees - Support all opportunities for the professional and personal growth of the staff.
- Results - We are committed to meeting ambitious targets.

4.3 NAV

Funded in 1998 and headquartered at Lisbon International Airport, NAV Portugal is a state owned company with administrative, financial and assets autonomy.

NAV Portugal, aims to provide air navigation services in the Flight Information Region (FIR) under responsibility of the Portuguese State, Lisbon and Santa Maria. It ensures the compliance with the applicable national and international regulation and the best safety conditions, optimizing the capacities of airspace use and of the airport infrastructures, improving the efficiency of the services provided and promoting environmental sustainability.

In this context, NAV Portugal sets itself to provide a high quality and efficient service, creating value for the State, as the sole shareholder, and ensuring high levels of professional qualification and motivation of its employees.

According to the latest financial statement, for the 2016 fiscal year, NAV had a turnover of 175,8 million euros, a 7,1% increase when comparing to 2015. This represented a profit of 15,3 million euros [47].

4.4 Foreign Object Debris

For years, Foreign Object Debris (FO) has represented a safety hazard for the aviation industry and it has contributed to a number of incidents and accidents, notably Air France Flight 4590. This flight, is an example of how a relatively small debris started a sequence of events that ultimately lead to a total loss of the aircraft [48]. Studies indicate that FO is the most potential ground based cause that contributes to catastrophic aviation failure [49].

The proportion of serious incidents is approximately 4 per 10 000 takeoffs or landings. Furthermore, a conservative approach made by Insight SRI estimates the direct costs of FOD at 1,1 billion USD per year, rising to a total of 12,4 billion USD if indirect costs are accounted for [50].

A FO is basically a foreign object, a substance, debris or article alien to the aircraft equipment that if ingested into the engine or lodged in a mechanism can potentially cause damage which may render the system unsafe for operation.

4.4.1 Flight BLF639

On 12 June 2010 a serious incident took place at Helsinki-Vantaa airport involving an AVRO 146-RJ85, registration OH-SAR and operated by Blue1 [51].

Flight BLF639, suffered severe damage to the outer left engine during the take-off run which led to a Rejected Take-off (RTO) at 100 knots. The flight was operating out of Helsinki, bound to Copenhagen with 93 passengers and 4 crew members on board.

After the aircraft vacated the runway, at Air Traffic Control (ATC) request, a runway inspection was performed. This inspection found the runway to be clear of obstacles and thus, safe to operate. As such, 2 transport aircraft were cleared to take-off from that runway. Minutes later, the Pilot in Command (PIC) of BLF639 called ATC and recommended the runway to be reinspected. This second inspection disclosed a significant amount of engine pieces on the runway and they were removed.

Neither of the aircraft which used the runway prior to debris removal were subsequently found to have suffered any damage but both were advised of the situation en route.

4.4.2 Relevant events

A number of actions took place or failed to in the different organizations.

Operations, the pilot called ATC 10 minutes after noticing significant engine damage and parts missing.

ATC asked for a runway inspection which was performed but failed to find any FO. Nonetheless, and despite, the pilot's call, the runway was deemed safe for operations even though no debris had been found. This arises a series of questions

- about the methods by which the runway was inspected;
- if the pilot's communication had been transmitted by ATC to the team performing the runway inspection;
- the lack of an approximate location of where the debris could be in the pilot's communication;
- how was the runway deemed safe for operations despite the engine parts that were missing weren't found.

Figure 4.2: Pieces of engine found by the airport maintenance unit on runway 22R [51]

4.4.3 Report conclusions

The events of this day were classified as a serious incident since two aircraft were cleared for take-off while there were debris on the active the runway, which could have damaged the aircraft during take-off run.

A number of findings were released in the Air Accidents Investigation Branch (AAIB) report: [51]

- The aircraft certificates of airworthiness and registration were valid.
- The flight crew and air traffic controller's licenses and ratings were valid.
- The airport maintenance unit staff members involved in the incident were experienced workers at Helsinki-Vantaa airport.
- The effect of weather factors on the sequence of events was limited to damp conditions on the runway, which made the engine pieces difficult to detect.
- The flight was a scheduled passenger flight.
- The take-off was aborted without delay because of severe damage to engine no. 1.
- The first runway inspection was requested and carried out in accordance with normal routine procedures. The objects on the runway were not detected, and the runway was incorrectly reported to be free of obstacles.
- Two transport aircraft were cleared for take-off from the runway, which had been reported to be free of obstacles.
- The runway was inspected again after the immediate findings from an engine inspection on the apron had been reported to the ATC.
- The airport maintenance shift supervisor joined the second inspection on his own initiative, and the controller specified the area and objects to be inspected according to the new information he had received. Several engine pieces were found on the runway.
- The pilots-in-command of the transport aircraft which had taken off between the runway inspections were informed of the findings on the runway.
- The air airline's instructions on pilot actions in the event of aborted take-off were found to be appropriate.
- In a later inspection, it was concluded that the engine damage had resulted from a fracture in the root of a second-stage turbine rotor blade.
- The rotor blade fracture was probably caused by overheat in the engine although other causes could not be excluded. The fracture could not be predicted on the basis of current engine condition monitoring procedures, which showed no difference between the damaged engine and the other engines.

- Engine maintenance actions had been signed as having been performed properly and on time, without exceeding any service life limitations.
- The pilots, ATC and airport maintenance unit filed reports on the incident in accordance with applicable regulations.
- The investigation commission classified the incident as a serious incident, because two transport aircraft took-off while there were engine pieces on the runway, which could have damaged the aircraft during take-off run.

A number of safety recommendations were also issued. Namely, increasing the cooperation between different units. Specifically, precise instructions concerning runway inspections should be issued, so that the inspecting staff has all the available information about the situation at their disposal during the inspection.

Furthermore, it was revealed that technical staff of air carriers usually have no instructions for when aircraft parts might remain on the runway and that ATC should be informed about it without any delay. According to the Finish Safety Agency this situation should be further examined and any deficiencies rectified.

Finally an assessment should be made to evaluate the need for acquiring foreign object debris detection equipment since this represents a significant flight safety threat to normal operations.

4.4.4 The notion of risk

As mentioned in section 4.4, the existence of FOD is indeed a hazard for the aviation industry leading to a number of safety risks.

In this case, the hazard can be classified as in table 4.1.

Table 4.1: FOD hazard classification

System	Subsystem	Activity	Hazard description	How was it identified
Air side	Movement area	Runway operations	FOD	Subsequent runway inspection

Going a step further, adding to the definition of risk presented in section 2.3.2, risk can be defined mathematically as a set of three elements. [52]

$$R = \{\langle s_i, p_i, x_i \rangle\}, i = 1, 2, ..., N + 1 \tag{4.1}$$

Where:

- R: risk
- s_i: a scenario identification or description

- p_i: the likelihood of that scenario
- x_i: is the consequence or evaluation measure of that scenario, i.e., the measure of damage.

N + 1 is the sum of the scenarios nobody has thought of. It is obvious that the variables p_i, x_i, themselves are uncertain. This fact is taken care of by having p_i and x_i described by probability density functions.

Furthermore, the following objective function for the expected risk for a given operation is defined: [53]

$$\bar{R} = \sum_{i=1}^{N+1} p_i \cdot x_i \tag{4.2}$$

Given the number of occurrences, this product allows an organization to decide, whether the risks taken are acceptable and commensurate with the ones expected or planned for a certain operation. The function also supports the statement on quantitative risk assessment above. $\bar{R}$ has to be distinguished from the total risk taken. The total risk taken is expressed in a risk curve which is based on the cumulative likelihood of all the scenarios.

For each risk, a hazard can also be written as:

$$H = \{\langle s_i, x_i \rangle\} \tag{4.3}$$

Each hazard H_i is evaluated according to a scenario and a consequence, s_i and x_i respectively. It can result in damage or loss and is a major hazard to the aircraft in flight.

4.4.5 Scenarios

The scenario identification process starts with a detailed and meticulous analysis of the organization's operative context. A choice was made consisting on the division of the airport field in two main sectors: air side and land side. The type of hazards traceable in each area is of very different nature. First of all, land side is a public soil. On the other hand, air side is considered a sterile area (i.e. areas of an airport defined in the airport security program where security regulated measures must be carried for anyone accessing this area). Furthermore the equipments used in both sectors are very different. For example aircraft vs private cars. Finally, the operating procedures put in place have completely different purposes, needs and complexity.

In our case, the area of major interest is the air side which is still a large and complex region, composed by many parts. Therefore, it was divided as below to seek for particular hazards.

- Aircraft stand;
- Taxiway;

- Runway;
- Terminal.

For each risk scenario there may be different levels of consequences, even the least credible consequence should be listed.

A number possible scenarios:

- FOD during parking;
- FOD during taxiing;
- FOD during takeoff;
- FOD during landing.

For a more preventive analysis, it is considered to that adverse meteorological conditions are present (poor visibility and wind). A possible foreign object debris occurrence could result in:

- Accident, where sever to fatal injuries can occur to people;
- Major incident, which would have led to a near collision between aircraft with a foreign object, significantly reducing the operation's safety;
- Significant incident, an accident or a major incident could have occurred if the risk had not be managed within safety risks. It represents a minor safety reduction.

4.4.6 Consequences

In order to make a distinction between different consequences arising from an hazard, ICAO Annex 14 [38] has defined a four classes event classification.

ICAO categorizes these safety occurrences in:

- Accidents and serious incidents;
- Incidents;
- Other safety occurrences.

An accident is an event that is unintended causing damage to persons, objects or the environment, and affects the normal functioning of the system. Aircraft accidents, for the most part, are thoroughly analyzed and documented. The consequences and losses incurred for a given type of operation are accessible.

An incident is an occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation. The distinction between an accident and a serious incident resides on the fact that the latter has such involving circumstances indicating that there is a high probability of an accident.

Finally a safety occurrence is an event that does not meet the reporting requirements. This could be e.g. the result of downgrading the incident after review.

Between a triggered hazard and an occurrence, a series of events have to occur. They compose the incident-accident sequence, that is the development of the potential damage of the hazard until its worst consequence. Once a sequence is defined, all steps are tightly connected. However, starting from the very same hazard, an equivalent consequence can be reached through a different path.

A number of incident-accident sequences have been envisioned:

- An aircraft, during its taxing, notices an object and rejects the takeoff;
- An aircraft during taxi, take-off or landing ingests or suffers an impact from a foreign object with-/without having knowledge of the event being affected immediately/in another flight phase.

4.4.7 Operational context

In order to properly determine hazards, to be able to imagine possible consequences and to adequately project mitigation boundaries, it is important to fully depict in which operational context an hazard can be trigged, a consequence can determine a loss and a protection be effective. The depth of this portrait is based upon the quality of the visits that the analyst conducts during an observation phase and the often informal information given to him during interviews/meetings and on the analyst own perception of his surroundings.

In this case corresponds with the all the apron, runway, taxiways and even the surrounding area, where foreign objects can be present during aircraft operation.

4.4.8 Initial Event

Through extensive research done across the industry, it is known that many types of debris that can be found. None of them is beneficial since they cause difficulties in maintaining the safety of operations. The different types of debris vary in materials, colors and sizes. In general, there are four basic classes of debris: metal, stone, miscellaneous and birds [50].

Another factor that is a recurrent FO source are construction activities. The combination of winter conditions with an aging pavement is also a known source of FO as the pavement can become frozen and began to crack into pieces. Wind can also propel FO such as sand, papers and plastic bags from

Table 4.2: Types and sources of FOD [50]

Types of FOD	Sources
Personnel	It is normally caused by poor working behavior and inappropriate housekeeping
Airport infrastructures	Sign, pavements and lights
Environment	Wildlife, snow and ice
The equipment operating on the airfield	Aircraft airport operations vehicles, maintenance equipment, fueling and construction equipment.
Aircraft and engine fasteners	Nuts, bolts and washers
Aircraft parts	Fuel cap, oil stick, trapdoors and tire fragments
Flight line items	Nails, personnel badges, luggage tags, soda can, etc.
Runway and taxiway materials	Concrete and asphalt chunks, rubber joint materials and paint chips

non-critical areas. The knowledge of all these effects indirectly creates awareness among organizations about the unpleasant effects of weather conditions and gives them ideas on how to solve this problem.

Awareness about FO can be incorporated and understood through positive safety culture. Therefore, personnel should have assertive attitudes and be aware of their duties regarding FO hazards and how to eliminate them. Most organizations recognize the importance of FO prevention programs. These are supported by a deep commitment from the top organization leadership management for its success. Different sources estimate different probabilities for the occurrence of foreign objects on the runway in a global way.

In the end, since the hazard distinguishes itself from the initial event, one can indicate as triggering event, the non detection of debris on the runway while conducting a runway inspection.

4.4.9 Barriers

In order to prevent the incident sequence from taking place and to reduce the likelihood of the hazard developing its damage potential to the fullest, it is important to look for casual barriers which may already be in place. Some of these barriers can prevent the consequences from happening while others can delay the activation of the initial event. The responsibility for a safety break down can not be attributed only to the front line. It is essential to design mitigation actions that involve all personnel.

In this case, there are causal barriers intrinsic in the air side areas against FO and in the training backgrounds of airport staff and crews. The operators training and the air side infrastructure characteristics preventing FO will affect the choice of the K3 and K5 parameters respectively.

Finally, given that the vehicle driver has missed debris during the first runway inspection, two causal barriers were identified:

- The vehicle driver, knowing that parts are missing from the airplane, conducts a second inspection;

- Aircraft pilot notices that the runway is contaminated and rejects the take off.

Once reasonable causal barriers are found for the hazard, this methodology suggest to build a “classical” event tree: starting from the initiating event, coinciding with the tree root, each barrier represents a tree branch; specifically, the bottom one stands for the probability of failure of the barrier, while upper ramification stands for the probability of success, equals to one minus the probability of failure, considering one the optimum. The tree ends expresses the various consequences linked to the same hazard.

4.4.10 Quantitative analysis

In this subsection an event tree for the hazard under examination is presented. All the probabilities estimate the failure probability of an event or of a barrier. Moreover a number of assumptions were made:

- No Liveware-Hardware unsafe interaction has been considered since all the equipment in the vehicle and aircraft was in perfect working condition. It would be, in fact, very hard to compute the probability of machine failure as it could arise from many different factors;

- Contrary to the initial event, in the first causal barrier there is a Liveware-Liveware interaction since the vehicle was manned by two people during the second inspection;

- For the first casual barrier the universal human factor of complacency has been involved. Starting from the point that a runway inspection had already been performed, the driver might assume that he would have noticed any debris if they were on the runway. He might be so self confident to overlook the inspection, loosing even more the awareness of danger;

- For the second causal barrier no Liveware-Software interaction is examined. In fact, not necessary the conducting crew is familiar with the airport’s layout. Furthermore, they are in constant radio contact with ATC;

- For the second causal barrier, human factor as lack of communication can be present in both communication between crew members or communication between pilots and AMS operators;

- For the second causal barrier, human factor as distraction can be very important, since both pilot not flying and pilot flying have other several tasks to perform in the while taxiing and preparing the aircraft for the take off configuration.

- No consequential barriers are currently in place to limit the harmfulness of the outcomes.

Table 4.3: Non detection of the reported debris

Interaction type	Human factor	K1	K2	K3	K4	K5	Failure probability
L	Distractions	0.01	0.5	1	1	1	0.005
L-E	Pressure (to open the runway)	0.01	0.5	1	1	1	0.005
L-S	Norms (established procedures)	0.01	0.5	1	1	1	0.005
L-L	Lack communication (pilot - airport services)	0.01	0.5	3	2	3	0.09
Subtotal							0.105

Table 4.4: Conduction of a second runway inspection without finding debris

Interaction type	Human factor	K1	K2	K3	K4	K5	Failure probability
Universal	Complacency (a first inspection had already been conducted)	0.1	0.1	1	1	1	0.01
L-E	Pressure (to open the runway)	0.1	0.1	1	1	1	0.01
L-S	Norms (established procedures)	0.1	0.1	0.5	1	1	0.005
L-L	Lack communication (between airport staff)	0.1	0.1	1	2	1	0.02
Subtotal							0.045

Table 4.5: Pilots do not notice that the runway is contaminated

Interaction type	Human factor	K1	K2	K3	K4	K5	Failure probability
L	Distractions	0.01	10	0.5	2	1	0.05
L-E	Fatigue	0.01	10	0.5	1	1	0.1
L-S	Norms (established procedures)	0.01	10	0.5	1	1	0.05
L-L	Lack communication (between PF and PNF)	0.01	10	0.5	1	1	0.05
Subtotal							0.25

Table 4.6: Event tree

Initial Event	First Barrier	Second Barrier	Consequence	Probability
	0.75		Review	0.07875
0.105				
		0.955	Unacceptable	0.02506875
	0.025			
		0.045	Unacceptable	0.00118125

4.4.11 Managing risk

As mentioned in Chapter 2, there is a wide consensus that in managing risk, it should be reduced to an acceptable level. Clearly, the operation of flying an aircraft from A to B is hazardous.

Therefore, in order to manage risks, the operator of the system, people with explicit control responsibility, must be able to influence the scenario, probability and consequences of an event.

In the case of foreign object debris, the interaction between the operator, air traffic control and the aerodrome is crucial.

The effectiveness of co-operation between ATC and the airport is paramount. This largely depends on communication practices and these should be continuously performed across all levels and not only between senior staff and supervisors. The likelihood that a certain scenario takes place is, in this case, governed by the flight deck, air traffic control and aerodrome operator decisions.

The aircraft operator is the one facing the harshest consequences. It has not only to endure the damage to the airplane but also the possible loss of human lives. The ANSP and aerodrome have less exposure to consequences, the damage to its assets is limited. In the case of a heavier aircraft, the magnitude of losses is greater as the kinetic and potential energy of an aircraft is positively correlated with the damage it can inflict. It is however possible that an aircraft, after ingesting foreign object debris, could damage the airport tower and terminal.

According to the event tree in section 4.4.10, we have 3 possible incident sequences.

Table 4.7: Incident sequence risk index

Incident sequence	Probability	Probability level	Severity	Risk index
1	0.100275	Occasional	Minor	8 - Review
2	0.00354375	Occasional	Major	12 - Unacceptable
3	0.00118125	Remote	Catastrophic	15 - Unacceptable

Obviously, the incident chain ending into an accident, thus combining the failure of both boundaries, is not acceptable. Indeed, it is mandatory to further analyze it and put in place all necessary boundaries in order to move its risk index into the yellow area, or, even better, into the green one. In this case, all sequences seek mitigation actions that will bring them to the green zone, the one of full tolerability.

4.4.12 Mitigation action

In order to try the incident sequences to the green, safe zone, there are foreign object debris prevention programs issued by the aviation authorities which provide standards and guidelines eliminating and reducing consequences of this hazard.

They are usually composed by 3 elements [55]:

- FO designation / sensitive area;
- Awareness;
- FOD air side activities preventive measure.

FO designation / sensitive area

FO designation area is essential to prevent FOD. It consists on identifying areas that are particularly sensitive to FOD. However, it is possible that debris are not controlled or found in this area. FOD sensitive areas should be designed by combining two risk factors: probability and consequences as shown in Figure 4.3.

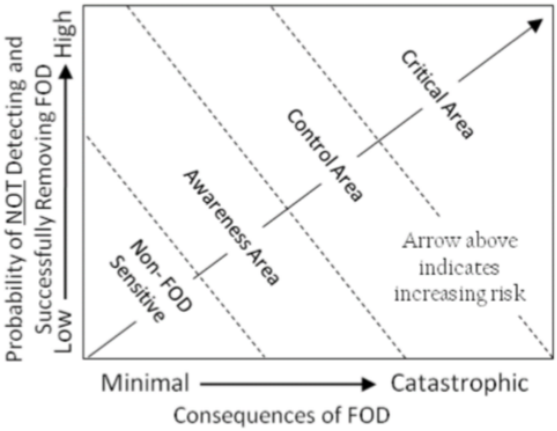

Figure 4.3: FOD sensitive areas by the combination of probability and consequences [55]

Good practices include delineating the FOD-sensitive areas and adopting a clean-as-you-go policy. This can be done with painted lines or with physical structures segregating these areas. This simple marking, on its own, will remind employees to make FOD prevention a priority when inside these areas.

Awareness

FOD prevention programs depend on the employees' awareness level regarding the issue and the program's existence. It is important that the program is properly disseminated throughout the organization with proper communication methods such as advertisement and visual tools, which are used to remind all employees about the foreign object debris hazard.

However, the methods have to be updated from time to time to ensure that all employees are aware about the program. Moreover, design of visual tool is giving major impact in FOD prevention program visibility: it must be able to deliver a clear message that is applicable, easy to read and understand.

Besides visual tools that deliver an easy to read and understand message, FOD awareness can be increased by organizational communication via seminars, case studies, electronic reporting and sharing information with other operators to minimize all FO potential hazards.

FO air side activities preventive measure

The procedures to eliminate FO hazard must consider all air side activities.

Most FO are found in airport apron, service roads, baggage area and areas near the aircraft galley usually come from aircraft servicing activities. In order to avoid any unwanted incidents due to these objects, these areas should be monitored and cleaned. Additionally, it is important to set up procedures to check ground servicing equipment for any signs of wear and tear that have tendency to create FO hazard.

Another common sources of FO in airports are from the asphalt and concrete pavements. A good supervision of FO on airfield pavement is vital in promoting safety of aircraft operations. Pavement Condition Index (PCI) is developed to identify the FO potential caused by deterioration and is incorporated in airport pavement management system [56]. The PCI is able to address any maintenance act required to reduce FO hazards.

5

Conclusion

Contents

This chapter summarizes considerations gathered during the internship at AeroEx and the collaboration with the interviewed organizations. First of all, similarities between the two SMS activities and approaches will be compared, presenting similarities and differences. Finally, future related works will be proposed.

5.1 Parallels between SMS

Since aviation organizations' primary goal is delivering a service, its timely and efficient delivery may, at times, be in conflict with operational safety considerations. If there were no service delivery efficiency considerations (for example the need meet a schedule), operational safety would cease to be a factor. The operation would be conducted only when there were no constraints. This, however, is impractical, as it would make the aviation industry inviable.

Therefore, aviation safety issues are neither inherent to, nor a condition of aviation operations, but a byproduct of the need for the delivery of a service. This further reinforces the need for safety management as a core business function that ensures an analysis of an organization's resources and allocates resources in a way which supports the overall service delivery needs of the organization.

Considering the Portuguese Safety Management System scenario, it is immediately clear how advanced these organization's SMS are. They have well organized structures, planned activities in order to reach their safety goals and a built-up approach for developing tasks.

Confirmation of what just said comes from the attention that ANAC directs toward all the organizations. Portuguese regulations on this topic are mainly dependent on international statements from both EASA and ICAO.

In the aim of continuous innovation, airlines frequently attend safety meetings, in which they present researches' results encouraging other operators organizations, still lagging behind in SMS implementation. Similarly NAV participates in safety meetings at an European level. On the other hand, because of its necessary tight link to the surrounding territory, Lisbon Airport prefers to collaborate and exchange of information with the national Authority. Nonetheless, it does participate in international undertakings.

Another similarity lies on their focus towards Safety Culture. These organizations, draw up safety bulletins, released in a paper or digital format. One of their cornerstone values is to spread Safety Culture as much as possible and to inform all personnel of the importance of safety reports and of their not-punishing purposes.

A common ground that is shared between these organizations is the difficulty that Safety Managers have in speaking to senior management about safety. Senior management is often reluctant to fully understand the need of allocating more resources to SMS. This falls short since safety indications are not yet clearly translated in cost benefits terms. It is however clear that SMS is not only reactive but

also proactive and predictive. It can explain what might occur and how to prevent it, suggesting the implementation of mitigations before any outcome. This only adds to the need for safety management as a core business function that ensures an analysis of an organization's resources and goals and allows for a balanced and realistic allocation of resources between protection and production goals, which supports the overall service delivery needs of the organization.

In order to have a simpler and a more precise explanation of the risk index calculated in retrospective/proactive risk assessments, each organization designed risk matrices tailored upon their organizational characteristics and operational constraints. Taking the ICAO risk matrix as a model, airport and ANSP analysts customize probability ranges, considering as reference the average annual aircrafts' movements. On the other hand, airlines tend to developed a more complex risk matrix, with both an increased number of severity and probability levels. In particular, each severity rank is fully characterized in technical and economic terms.

5.2 Differences between SMS

Firstly, the core business of these organizations are different. The most relevant dissimilarity resides in the structuring of the different offices which are composed by different numbers of people with specific and technical skills, adapted to the organization. This characteristic clearly affects the amount of activities that can be performed and limits the research and development capabilities.

From a technical point of view, a slightly different interpretation of the term hazard can be detected. Airport authorities tend to strictly read it as a threat, present, but not yet triggered. On the other hand operators and ANSP analysts tend to portray it as an undesirable condition, a threat already on show.

Furthermore, the technical and educational background of an airline and ATC personnel and is on average higher than handling agents and airport operators. This means that airline and ATC personnel are, at a first glance, more used to reporting forms, more trained on the topic and thus prone in detecting unsafe elements.

All this leads to different responses to changes. The introduction of mitigation actions is also different across organizations both in feedback and time needed for them to be implemented.

5.3 Future Work

Taking into account the current situation and future developments, a single assessment methodology meeting both the ANSP Performance Scheme and the EASA requirements would be essential to ensure a harmonized and consistent assessment of SMS within the wider EASA regulatory structure. It would be interesting to study a harmonized base which further supports the SSP. The absence of common management system/SMS requirements creates a number of issues both for competent authorities and organizations:

- Compliance demonstration with the different rules is time and resource intensive, creates unnecessary bureaucracy and does not support the systems approach.
- It creates additional burden for the authorities having to oversee such organizations to ensure that all different requirements are met.
- It does not support harmonization and streamlining of competent authority policies and procedures for the benefit of all regulated entities.
- It does not support the management of risks at the interfaces between organizations due to the differences in the applicable requirements, including differences in terminology and concepts.

Therefore, a common approach to assessing SMS effectiveness is expected to have a positive safety impact through:

- promoting SMS within the different domains;
- supporting competent authorities to evolve from traditional, compliance based oversight to performance-based oversight;
- providing a common baseline for SMS effectiveness assessment;
- creating a sound basis for mutual acceptance of SMS under bilateral agreements.

Bibliography

[1] *Statistical Summary of Commercial Jet Airplane Accidents*. Seattle: Boeing Commercial Airplanes, 2016. *Boeing*. Web. 8 April 2017. http://www.boeing.com/resources/boeingdotcom/company/about_bca/pdf/statsum.pdf

[2] *Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008*. Web. 8 April 2017.

[3] *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008*. Web. 8 April 2017.

[4] *Annex 19 Safety Management*. Quebec: International Civil Aviation Organization, 2013. *Skybrary*. Web. 18 May 2017. http://www.skybrary.aero/bookshelf/books/2422.pdf

[5] Wretstrand, A. et al. *"Safety as a key performance indicator: Creating a safety culture for enhanced passenger safety, comfort, and accessibility."*. Research in Transportation Economics 48 (2014): 109-115. Print.

[6] Hollnagel, E. *Safety-I and Safety-II: The Past and Future of Safety Management*. Farnham: Ashgate, 2014. Print.

[7] Waterson, P. *Patient Safety Culture: Theory, Methods and Application*. Farnham: Ashgate, 2014. Web. 14 April 2017.

[8] Hollnagel, E. et al. *From Safety-I to Safety-II: A White Paper. The Resilient Health Care Net*. Florida: University of Florida, 2015. *Resilient Healthcare*. Web 10 May 2017.

[9] Burin, J. "Being Predictive in a Reactive World." *ISASI Forum* Jan. 2013: 23-24. Print

[10] *The Senior Manager's Role in Safety Management System* Safety management international collaboration club, 2011. Print

[11] Reason, J. *Managing the Risks of Organizational Accidents*. Burlington: Ashgate, 2006. Print.

[12] Price, J. Forrest, J.*Practical Airport Operations, Safety, and Emergency Management: Protocols for Today and the Future* Cambridge: Elsevier, 2016. 74-75. Web. 14 April 2017.

[13] *Doc 9859, Safety Management Manual (SMM)*. Quebec: International Civil Aviation Organization, 2013. *Skybrary*. Web. 8 May 2017.

[14] *Safety Management Systems Course*. Quebec: International Civil Aviation Organization, 2008. Web. 8 May 2017. https://www.icao.int/safety/afiplan/Documents/Safety20Management/2008/SMSWorkshop/Modules/ICAOSMSModule5Risks08-1120(E).pdf

[15] Savage, A. *"Applying Risk Management in a University Environment to Manage the Risk of Fraud and Corruption"*. Australian Public Sector Anti-Corruption Conference (2007). Web. 2 April 2017.

[16] *Safety Management Systems (SMS) guidance for organisations*. London: UK CAA, 2010.*UK CAA*. Web. 2 June 2017. https://www.trafi.fi/filebank/a/1363863041/cc46c619411d88c3f5e4e8ac4c6609b9/11830-SMS_Guidance_Material_UKCAA.pdf

[17] Giemulla, E. Weber, L. *International and EU Aviation Law. Selected Issues*. :Kluwer Law Intl, 2011. 622.*Google Books*. Web. 22 May 2017.

[18] Walls, L. Revie, M. Bedford, T. *Risk, Reliability and Safety: Innovating Theory and Practice*. : CRC Press, 2016. 67-81.*Google Books*. Web. 31 July 2017.

[19] *Bow Tie Risk Management Methodology*. *Skybrary*. Web. 28 July 2017. https://www.skybrary.aero/index.php/Bow_Tie_Risk_Management_Methodology

[20] Maurino, D. *Threat and error management*. 2005. 67-81.*Flightsafety*. Web. 31 July 2017.

[21] G.C. Bello, V. Colombari *The Human Factors in Risk Analyses of Process Plants: The Control Room Operator Model (TESEO)*. Reliability Engineering, 1980. Print.

[22] *Quality Is Everywhere - Finding quality tools in your daily life*. *ASQ*. Web. 28 July 2017. http://asq.org/quality-progress/2017/01/quality-in-the-first-person/quality-is-everywhere.html

[23] Dumas, R. *Safety and quality: The human dimension. Professional Safety*. Professional Safety, 1987. Print

[24] Manzella, J.C. *Achieving safety performance excellence through total quality management.*. Professional Safety, 1997. Print

[25] *Annex 6 to the Convention on International Civil Aviation* . Quebec: International Civil Aviation Organization, 2016. Web. 8 May 2017.

[26] *Safety Management Systems for Commercial Air Transport Operations* . London: UKCAA, 2001. Web. 24 May 2017. http://atcvantage.com/docs/UK_Cap712_SMS_Commercial_Air_Transport_Operations.pdf

[27] *Doc 9734 AN/959*. Quebec: International Civil Aviation Organization, 2006. Web. 8 May 2017

[28] *Regulation (EC) No 290/2012 of the European Parliament and of the Council of 30 March 2012*. Web. 9 October 2017.

[29] *Regulation (EC) No 965/2012 of the European Parliament and of the Council of 5 October 2012*. Web. 14 October 2017.

[30] *Regulation (EC) No 139/2014 of the European Parliament and of the Council of 12 February 2014*. Web. 28 September 2017.

[31] *Regulation (EC) No 340/2015 of the European Parliament and of the Council of 20 February 2015*. Web. 9 October 2017.

[32] *Regulation (EC) No 965/2012 of the European Parliament and of the Council of 19 January 2016*. Web. 20 November 2017.

[33] *Regulation (EC) No 1216/2011 of the European Parliament and of the Council of 24 November 2011*. Web. 12 October 2017.

[34] *Regulation (EC) No 390/2013 of the European Parliament and of the Council of 3 May 2013*. Web. 12 October 2017.

[35] *Regulation (EC) No 452/2014 of the European Parliament and of the Council of 29 April 2014*. Web. 12 October 2017.

[36] *Annex 11 to the Convention on International Civil Aviation* . Quebec: International Civil Aviation Organization, 2001. Web. 8 May 2017.

[37] *Regulation (EC) No 965/2012 of the European Parliament and of the Council of 7 July 2011*. Web. 9 October 2017.

[38] *Annex 14 to the Convention on International Civil Aviation* . Quebec: International Civil Aviation Organization, 2016. Web. 8 May 2017.

[39] *Annex 8 to the Convention on International Civil Aviation* . Quebec: International Civil Aviation Organization, 2015. Web. 8 May 2017.

[40] *Regulation (EC) No 748/2012 of the European Parliament and of the Council of 3 August 2012*. Web. 10 October 2017.

[41] *Part-21 EASA*. Web. 10 December 2017. https://www.easa.europa.eu/document-library/acceptable-means-of-compliance-and-guidance-materials/part-21-amc-gm

[42] *Embodiment of level of involvement requirements into Part-21*. Web. 12 September 2017. https://www.easa.europa.eu/sites/default/files/dfu/CRD20to20NPA202015-03.pdf

[43] *Regulation (EC) No 321/2014 of the European Parliament and of the Council of 7 March 2014*. Web. 8 October 2017.

[44] *White fleet*. Web. 12 September 2017. http://www.flywhite.com/fleet/141.htm

[45] *White website* Web. 12 September 2017. http://www.flywhite.com

[46] *ANA website* Web. 1 October 2017. https://www.ana.pt/en/corporate/ana/about-ana

[47] *NAV website* Web. 1 October 2017. https://www.nav.pt

[48] *Accident on 25 July 2000 at La Patte d'Oie in Gonesse (95) to the Concorde registered F-BTSC operated by Air France*. BEA, 2000. Web. 5 May 2017. https://www.bea.aero/uploads/tx_elydbrapports/f-sc000725a.pdf

[49] Kraus, C. Watson, J*Guidelines for the prevention and elimination of foreign object damage/debris (FOD) in the aviation maintenance environment through improved human performance* . 2001. Web. 8 May 2017. https://www.faa.gov/about/initiatives/maintenance_hf/library/documents/media/human_factors_maintenance/maint_product781.pdf

[50] *The economic cost of FOD*. 2009. Web. 5 May 2017. http://fod-detection.com/wp-content/uploads/2009/12/the-economic-cost-of-fod.pdf

[51] *Serious incident at Helsinki-Vantaa Airport on 12 June 2010*. AAIB, 2010. Web. 30 April 2017.

[52] Kaplan, A. Garrick, B. *On The Quantitative Definition of Risk*. Risk Analysis, vol.1 1981. Web. 15 August 2017.

[53] Haimes, Y. *On the Definition of Resilience in Systems*. Risk Analysis, vol.29 1981. Print.

[54] *ADREP Taxonomy*. Quebec: International Civil Aviation Organization, 2010. *Skybrary*. Web. 31 August 2017.

[55] Lin, H. 2005 *Foreign object detection (FOD) using multi-class classifier with single camera vs. distance map with stereo configuration*. Iowa State University, 2015. Web. 25 August 2017.

[56] *Pavement Evaluation and Rating*. The Louis Berger Group, 2012. Web. 18 January 2018.