Doc 9859

# Safety Management Manual (SMM)

***Notice to Users***

*This document is an unedited advance version of an ICAO publication as approved, in principle, by the Secretary General, which is rendered available to the public for convenience. The final edited version may still undergo alterations in the process of editing. Consequently, ICAO accepts no responsibility or liability of any kind should the final text of this publication be at variance from that appearing here.*

**Second Edition – 2008** *(Advance edition – unedited)*

International Civil Aviation Organization

# TABLE OF CONTENTS

**Attachments to the SMM**



- - - - - - - - - - - - - - -

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ACARS | Aircraft Communications Addressing and Reporting System |
| ACI | Airports Council International |
| ADREP | Accident/Incident Data Reporting (ICAO) |
| AEP | Aerodrome Emergency Plan |
| AIRS | Aircrew Incident Reporting System |
| ALA | Approach and landing accidents |
| ALARP | As Low As Reasonably Practicable |
| AME | Aircraft Maintenance Engineer |
| | *Note. — For the purposes of this manual, AME will be used to represent Aircraft Maintenance Engineer/Mechanic/Technician* |
| AMJ | Advisory Material Joint |
| AMO | Approved Maintenance Organization |
| ASDE | Airport Surface Detection Equipment |
| ASR | Air Safety Report |
| ATC | Air Traffic Control |
| ATCO | Air Traffic Controller |
| ATM | Air Traffic Management |
| ATS | Air Traffic Service(s) |
| CAP | Civil Air Publication (U.K.) |
| CD | Compact Disc |
| CFIT | Controlled flight into terrain |
| CEO | Chief Executive Officer |
| Cir | Circular |
| CMC | Crisis Management Centre |
| CNS | Communications, Navigation and Surveillance |
| CRM | Crew Resource Management |
| CVR | Cockpit Voice Recorder |
| DME | Distance Measuring Equipment |
| Doc | Document |
| EGPWS | Enhanced Ground Proximity Warning System |
| ERP | Emergency Response Plan |
| FDA | Flight Data Analysis |
| FDM | Flight Data Monitoring |
| FDR | Flight Data Recorder |
| FIR | Flight Information Region |
| FMS | Flight Management System |
| FOD | Foreign Object (Debris) Damage |
| FOQA | Flight Operations Quality Assurance |

| | |
|---|---|
| FPD | FDA Programme Database |
| ft | Feet |
| GPS | Global Positioning System |
| GPWS | Ground Proximity Warning System |
| ILS | Instrument Landing System |
| IMC | Instrument Meteorological Conditions |
| ISO | International Organization for Standardization |
| kg | Kilogram(s) |
| LOSA | Line Operations Safety Audit |
| LOFT | Line-Oriented Flight Training |
| LAHSO | Landing and Hold Short Operations |
| m | Metre(s) |
| MEL | Minimum Equipment List |
| MNPS | Minimum Navigation Performance Specifications |
| MRM | Maintenance Resource Management |
| MSAW | Minimum Safe Altitude Warning |
| NM | Nautical Mile(s) |
| NOSS | Normal Operations Safety Survey |
| OJT | On-the-job Training |
| OSH | Occupational Safety and Health |
| PANS | Procedures for Air Navigation Services |
| PANS-ATM | Procedures for Air Navigation Services — Air Traffic Management |
| PANS-OPS | Procedures for Air Navigation Services — Aircraft Operations |
| PAPI | Precision Approach Path Indicator |
| PC | Personal Computer |
| QAR | Quick Access Recorder |
| QA | Quality Assurance |
| QC | Quality Control |
| QMS | Quality Management System |
| RA | Resolution Advisory |
| RNP | Required Navigation Performance |
| R/T | Radiotelephony |
| RVSM | Reduced Vertical Separation Minimum |
| SAG | Safety Action Group |
| SARPs | Standards and Recommended Practices (ICAO) |
| SDCPS | Safety Data Collection and Processing Systems |
| SDR | Safety Data Request |
| SDR | Service Difficulty Reporting |
| SHEL | Software/Hardware/Environment/Liveware |
| SID | Standard Instrument Departure |

| | |
|---|---|
| SIRO | Simultaneous Intersecting Runways Operation |
| SM | Safety Manager |
| SMM | Safety Management Manual |
| SMS | Safety Management System(s) |
| SMSM | Safety Management System Manual |
| SOPs | Standard Operating Procedures |
| SRB | Safety Review Board |
| SSP | State Safety Programme |
| STAR | Standard Instrument Arrival |
| STCA | Short-term Conflict Alert |
| TCAS | Traffic Alert and Collision Avoidance System |
| TEM | Threat and Error Management |
| TOR | Tolerability of Risk |
| TRM | Team Resource Management |
| USOAP | Universal Safety Oversight Audit Programme (ICAO) |
| VASIS | Visual Approach Slope Indicator Systems |
| VMC | Visual Meteorological Conditions |
| VOR | Very High Frequency Omni-directional Range |

- - - - - - - - - - - - - - -

# Chapter 1

# OVERVIEW

## 1.1 GENERAL

1.1.1 This Manual is intended to provide States with guidance to develop the regulatory framework and the supporting guidance material for the implementation of Safety Management Systems (SMS) by service providers. It also provides guidance for the development of a State Safety Programme (SSP), in accordance with International Standards and Recommended Practices (SARPs) contained in Annexes 1 – *Personnel licensing*, 6 – *Operation of aircraft*, 8 – Airworthiness of aircraft, 11 – *Air Traffic Services*, 13 – *Aircraft accident and incident investigation* and 14 – *Aerodromes*.

## 1.2 OBJECTIVES

1.2.1 The objectives of this Manual are:

- to provide States knowledge of safety management concepts and ICAO Standards and Recommended Practices (SARPs) on safety management contained in Annexes 1, 6, 8, 11, 13 and 14, and related guidance material;
- to provide States knowledge to certify and oversee the implementation of the key components of an SMS in compliance with relevant ICAO SARPs; and
- to provide States knowledge to develop and implement an SSP in compliance with relevant ICAO SARPs.

## 1.3 MANUAL CONCEPT

1.3.1 The concept underlying this Manual reflects a continuous loop concept. The Manual initially presents basic safety concepts, as the foundation upon which to understand and build the justification and need for both SMS and SSP. The Manual then proceeds to the discussion of how the safety concepts and tools discussed in the first part are embodied in the ICAO SARPs contained in Annexes 1, 6, 8, 11, 13 and 14. The Manual thereafter proposes a principled approach to the implementation of SMS by service providers. Lastly, the Manual introduces a proposal for the progressive implementation and maintenance of a SSP, with an emphasis in the role civil aviation authorities play in supporting SMS implementation by service providers. Figure 1-1 illustrates the Manual concept.

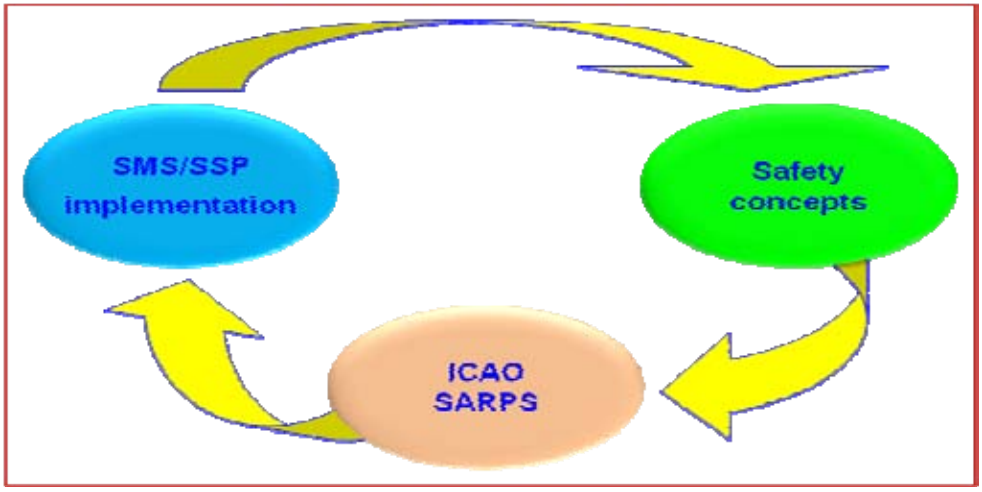



Figure 1-1 – The manual concept

## 1.4 CONTENTS OF THE MANUAL

1.4.1 The contents of the Manual include 11 chapters, as follows:

- Chapter 1 – Overview
- Chapter 2 – Basic safety concepts
- Chapter 3 – Introduction to safety management
- Chapter 4 – Hazards
- Chapter 5 – Safety risks
- Chapter 6 – ICAO safety management requirements
- Chapter 7 – Introduction to safety management systems
- Chapter 8 – SMS planning
- Chapter 9 – SMS operation
- Chapter 10 – Phased approach to SMS implementation
- Chapter 11 – State Safety Programme (SSP)

1.4.2 The Manual also includes appendices to several chapters introducing practical examples of materials necessary for the implementation and maintenance of SMS and SSP. These appendices are directly linked to SMS or SSP implementation, and/or to information in different chapters of the Manual. Therefore, the appendices are included immediately following the chapter discussing the activity they support, and should be considered as “must know”.

1.4.3 The Manual also includes attachments introducing useful information, but that is not directly linked to SMS or SSP implementation. These attachments are included at the end of the Manual, and should be considered as “nice to know”.

## 1.5 STRUCTURE OF THE MANUAL

1.5.1 The Manual follows a building block approach. Chapter 2 sets the foundations, by discussing contemporary safety concepts. Chapter 3 introduces the basics of the management of safety, with an emphasis on why safety must be managed. Chapters 4 and 5 introduce the dogmatic framework that underlies safety risk management and explain its two basic concepts: hazards and safety risks. Lastly, Chapters 6 though 11 present a principled approach to the design, implementation and maintenance of processes to manage safety, thus proposing the SSP and SMS as management systems to manage safety within States and organizations respectively, and the notion of the management of safety as a systematic activity.

1.5.2 Chapter 11 on the State safety programme is introduced in this Manual as interim guidance material, while experience is accrued by ICAO and States on the development and implementation of the SSP, at which point a dedicated Manual on the State safety programme will be developed. Further and detailed guidance material on the development and

implementation of the SSP can be obtained from the ICAO SSP Training Course, which can be downloaded from www.icao.int/fsix or www.icao.int/anb/safetymanagement.

1.5.3 The 2nd Edition of the ICAO Safety Management Manual (Doc 9859) supersedes the 1st Edition, published in 2006, in its entirety. It also supersedes the ICAO Accident Prevention Manual (Doc 9422), published in 1984, now discontinued.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Chapter 2

# BASIC SAFETY CONCEPTS

## 2.1 OBJECTIVE AND CONTENTS

2.1.1 This chapter reviews the strengths and weaknesses of long-established approaches to safety, and proposes new perspectives and concepts underlying a contemporary approach to safety.

2.1.2 The chapter includes the following:

- The concept of safety
- The evolution of safety thinking
- A concept of accident causation – The Reason model
- The organizational accident
- People, operational contexts and safety – The SHEL(L) model
- Errors and violations
- Organizational culture
- The safety investigation

## 2.2 THE CONCEPT OF SAFETY

2.2.1 Depending on the perspective, the concept of safety in aviation may have different connotations, such as:

a) Zero accidents or serious incidents, a view widely held by the travelling public;

b) Freedom from hazards, i.e. those factors which cause or are likely to cause harm;

c) Attitudes towards unsafe acts and conditions by employees of aviation organizations;

d) Error avoidance;

e) Regulatory compliance;

f) Etc.

2.2.2 Whatever the connotation one might choose, they have one underlying commonality: they all convey the possibility of absolute control. Zero accidents, freedom from hazards, and so forth, convey the idea that it would be possible – by design or by intervention – to bring under control in aviation operational contexts all variables that can precipitate bad or damaging outcomes. However, while the elimination of accidents and/or serious incidents and the achievement of similar absolutes of control would certainly be desirable, such absolutes of control are unachievable goals in open and dynamic operational contexts. Hazards are integral components of aviation operational contexts. Failures and operational errors will occur in aviation, in spite of the best and most accomplished efforts to prevent them. No human activity or human-made system can be guaranteed to be absolutely free from hazards and operational errors.

2.2.3 Safety is therefore a concept that must encompass relatives rather than absolutes, whereby safety risks arising from the consequences of hazards in operational contexts must be acceptable in an inherently safe system. The key issue still resides in control, but in relative rather than absolute control. As long as safety risks and operational errors are kept under a *reasonable degree* of control, a system – open and dynamic, such as commercial civil aviation – is considered to be safe. In other words, safety risks and operational errors that are controlled to a reasonable degree are acceptable in an inherently safe system.

2.2.4 Safety is increasingly viewed as the outcome of the management of certain organizational processes, which have the objective of keeping the safety risks of the consequences of hazards in operational contexts under organizational control. Thus, for the purposes of this manual, safety is considered to have the following meaning:

*Safety is the state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.*

## 2.3 THE EVOLUTION OF SAFETY THINKING

2.3.1 During its early years, commercial aviation was a scantily regulated activity. Brittle technology, scarce infrastructure, limited oversight and less than complete understanding of the hazards underlying aviation operations combined with production demands incommensurate to the means and resources actually available, in contrast to those that would have been necessary to meet such demands.

2.3.2 It is a given in systems safety theory that production systems that set themselves ambitious production objectives without deploying the necessary means and resources to deliver such objectives develop the potential for frequent breakdowns. Therefore, it should be hardly surprising that the early days of commercial aviation were characterised by a high frequency of accidents. It should also be hardly surprising that the early safety process focussed on the need to prevent frequent accidents as overriding priority, and resorted to the investigation of accidents as the principal means of prevention. In those early days, the investigation of accidents, hampered by the absence of other than basic technological support, was an admirable combination of art and craft.

2.3.3 Technological improvements – due in no small measure to the investigation of accidents – and the development of appropriate infrastructure allowed aviation to emerge from infant years and limited activities, and initiate a transition towards maturity and a multiple-fold expansion of activities. The introduction of technology and development of infrastructure were accompanied by a gradual but steady decline in frequency of accidents, as well as steady and ever-increasing regulatory drive. By the Fifties, aviation was en-route to becoming (in terms of accidents) one the safest industries, but also one of the most heavily regulated.

2.3.4 Ever since, a deeply ingrained belief in regulatory compliance as a guarantee of safety installed itself in aviation. The notion that safety can be guaranteed as long as rules are followed, and that deviation from rules necessarily leads to safety breakdowns, remains a pervasive one. Without denying the importance of regulatory compliance as one of the bedrocks of aviation safety, the limitations of regulatory compliance as the mainstay of safety have increasingly been recognised, particularly as complexity of aviation operations increased. It is simply impossible to write in advance regulations that provide guidance for all conceivable operational scenarios in an open and dynamic system such as aviation; it is impossible to entirely pre-specify, in advance, the spectrum of variables in the operation of the aviation system.

2.3.5 Processes are driven by beliefs. Therefore, under the belief of regulatory compliance as the key to aviation safety, the early safety process based upon accident investigation that mainly focussed in the discovery of flaws and shortcomings in technology, was broadened to encompass regulatory compliance and oversight. The safety process thus became a vigil for outcomes (accidents and/or incidents of magnitude). Once an outcome occurred, the accident investigation would put into motion a protocol to find the cause. The search for cause would look into the possibility of failures in technology (which in spite of considerable improvement was far from levels of superlative reliability). If technology failures were not evident, attention was turned to the possibility of rule-breaking by operational personnel involved.

2.3.6 Accident investigations would then backtrack the breakdown under consideration, looking for a point or points in the chain of events where people directly involved in the breakdown would not have done what they would have been expected to do, would have done something they would not have been expected to do, or for a combination of both. In the absence of technological failures, investigations would look for unsafe acts by operational personnel: actions and/or inactions that could be directly linked to the outcome under investigation. Once such actions/inactions were identified and linked – with the benefit of hindsight – to the breakdown, blame in different degrees and under different guises was the inevitable consequence, and more often than not punishment would be meted out, for failing to "perform safely".

2.3.7 Typical of this approach was to generate safety recommendations aimed at the specific, immediate safety concern identified as causing the breakdown, almost exclusively. Not too much emphasis was placed in the hazardous conditions that, although present but not "causal" to the occurrence under investigation, held nevertheless damaging potential to aviation operations under different sets of circumstances to the ones under consideration.

2.3.8 While this perspective was quite effective in identifying "what" happened, "who" did it, and "when" it happened, it was considerable less clear in disclosing "why" and "how" it happened (Figure 2-1). While at one time it was important to understand the "what", "who" and "when", more and more became necessary to understand the "why" and the "how" in order to fully understand safety breakdowns. In recent years, significant strides have been made in achieving this understanding. In retrospect, it is clear that aviation safety thinking has experienced a significant evolution over the last fifty years, evolving through eras, each with their accompanying shifts in underlying paradigms.

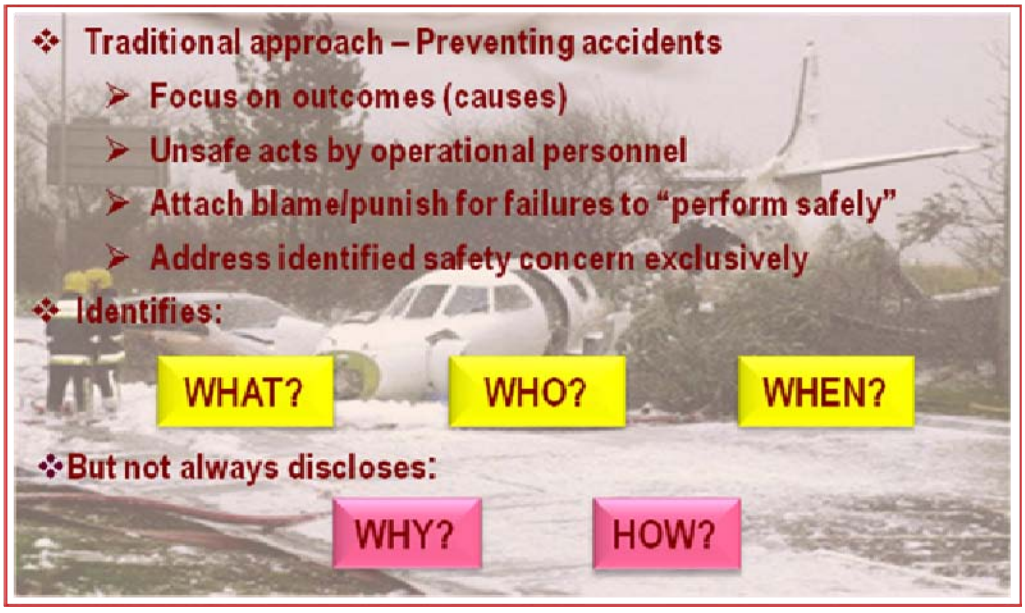



Figure 2-1 – Traditional approach – Preventing accidents

2.3.9 The early days of aviation and those before and immediately following the Second World War until the Seventies can be characterised as the "technical era": safety concerns were related mostly to technical factors. Aviation was emerging as a massive transportation industry, yet the technology supporting its operations was brittle, and technological failures were the recurring factor in safety breakdowns. The focus of safety endeavours was rightly placed at the time, as already discussed, in the investigation and improvement of technical factors.

2.3.10 By the early Seventies, progress in technology, through the introduction of jet engines, radars (both airborne and ground-based), autopilots, flight directors, improved navigation and communications capabilities and similar performance-enhancing technologies, both in the air and in the ground, shifted the concern towards human error, thus heralding the beginning of the "human era". The focus of safety endeavours then shifted to human performance and Human Factors, with the emergency of Crew Resource Management (CRM), Line-Oriented Flight Training (LOFT), human-centred automation and similar human performance supporting interventions. The period between the mid-Seventies to the mid-Nineties has been dubbed the "Golden Era" of aviation Human Factors, in reference to the huge investment by aviation to bring under control the elusive and ubiquitous human error. Nevertheless, and in spite of massive investment of resources in error-mitigation interventions, by the mid-Nineties allocation of causes of safety breakdowns continued to single out human performance as recurring factor (Figure 2-2).

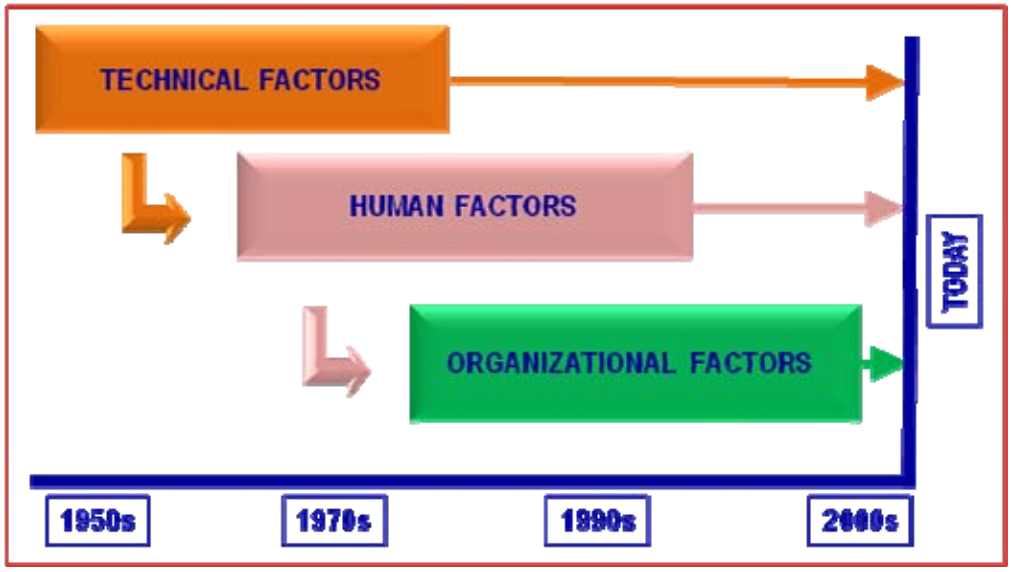



Figure 2-2 – The evolution of safety thinking

2.3.11 With the benefit of hindsight, the downside of Human Factors endeavours during a significant portion of the "Golden Era" was that – in line with prevailing aviation thinking – they tended to focus on the individual, with scant attention to the operational context in which individuals accomplished their missions. It was not until the early Nineties that it was first acknowledged that individuals do not operate in a vacuum, but within defined operational contexts. Although scientific literature regarding how features of a context can influence human performance and become determinant in shaping events and outcomes was available, it was not until then, the Nineties, that aviation acknowledged that features of operational contexts that can profoundly influence human performance, hindering or supporting it. Such acknowledgement signalled the beginning of the "organizational Era". At that point, safety endeavours broadened to a systemic perspective, to encompass organizational, human and technical factors. It was also at this time that the notion of the organizational accident was embraced by aviation.

## 2.4 A CONCEPT OF ACCIDENT CAUSATION – REASON MODEL

2.4.1 Industry-wide acceptance of the concept of the organizational accident was made possible by a simple, yet graphically powerful model developed by Professor James Reason. This model provides a means for understanding how aviation (or any other production system) operates successfully or drifts into failure. According to this model, accidents require the coming together of a number of enabling factors — each one necessary, but in itself not sufficient to breach system defences. Because complex systems such as aviation are extremely well-defended by layers of defences in-depth, single point failures are rarely consequential. Equipment failures or operational errors are never the cause of breaches in safety defences, but rather the triggers. These breaches are a delayed consequence of decisions made at the highest levels of the system, which remain dormant until their effects or damaging potential is activated by specific sets of operational circumstances. Under such specific circumstances, human failures or *active failures* at the operational level act as triggers of *latent conditions* conducive to facilitating a breach of the system's inherent safety defences. In the concept advanced by the Reason Model, all accidents include a combination of both active and latent conditions.

2.4.2 *Active failures* are actions or inactions, including errors and violations which have an immediate adverse effect. They are generally viewed – with the benefit of hindsight – as *unsafe acts*. Active failures are generally associated with front-line personnel (pilots, air traffic controllers, aircraft mechanical engineers, etc. and may result in a damaging outcome. They hold the potential to penetrate the defences put in place to protect the aviation system by the organization, the regulatory authorities, etc. Active failures may be the result of normal errors, or they may result from deviations from prescribed procedures and practices. The Reason model recognizes that there are many error–producing and violation–producing conditions in any operational context that may affect individual or team behaviour.

2.4.3 Active failures by operational personnel take place in an operational context which includes *latent conditions*. *Latent conditions* are *conditions present in the system well before a damaging outcome is experienced, and made*

*evident by local triggering factors*. The consequences of latent conditions may remain dormant for a long time. Individually, these latent conditions are usually not perceived as harmful, since they are not perceived as being failures in the first place.

2.4.4 Latent conditions become evident once the system's defences have been breached. These conditions are generally created by people far removed in time and space from the event. Front-line operational personnel inherit latent conditions in the system, such as those created by poor equipment or task design; conflicting goals (e.g. service that is on time *versus* safety); defective organizations (e.g. poor internal communications); or management decisions (e.g. deferral of a maintenance item). The perspective underlying the organizational accident aims to identify and mitigate these latent conditions on a system-wide basis, rather than by localized efforts to minimize active failures by individuals. Active failures are only symptoms of safety problems, not causes.

2.4.5 Even in the best-run organizations, most latent conditions start with the decision-makers. These decision-makers are subject to normal human biases and limitations, as well as to real constraints such as time, budget, politics, etc. Since downsides in managerial decisions cannot be always prevented, steps must be taken to detect them and to reduce their adverse consequences.

2.4.6 Decisions by line management may transform into inadequate training, poor scheduling or neglect of workplace precautions. They may lead to inadequate knowledge and skills or inappropriate operating procedures. How well line management and the organization as a whole perform their functions sets the scene for error – or violation – producing conditions. For example: How effective is management with respect to setting attainable work goals, organizing tasks and resources, managing day-to-day affairs, and communicating internally and externally? The decisions made by company management and regulatory authorities are too often the consequence of inadequate resources. However, avoiding the costs of strengthening the safety of the system can facilitate the pathway to the organizational accident.

2.4.7 Figure 2-3 portrays the Reason Model in a way that assists in understanding the interplay of organizational and management factors (i.e. system factors) in accident causation. Various *defences* are built deep into the aviation system to protect against fluctuations in human performance or decisions with a downside at all levels of the system (i.e. the front-line workplace, the supervisory levels and senior management). Defences are *resources provided by the system to protect against the safety risks that organizations involved in production activities generate and must control*. This model shows that while organizational factors, including management decisions, can create latent conditions that could lead to breaches in the systems defences, they also contribute to the robustness of the system's defences

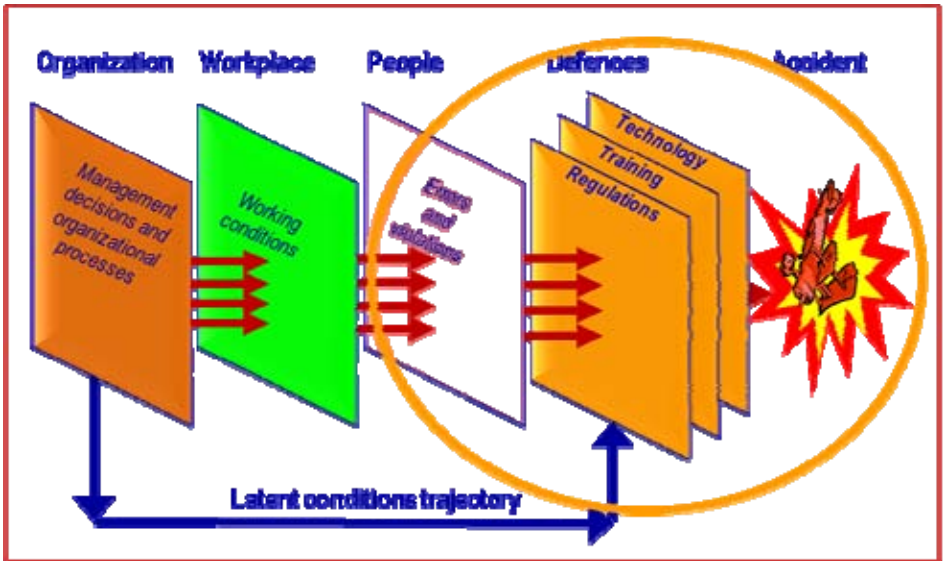



Figure 2-3 – A concept of accident causation

## 2.5 THE ORGANIZATIONAL ACCIDENT

2.5.1 The notion of the organizational accident underlying the Reason Model can be best understood through a building block approach, consisting of five blocks (Figure 2-4).

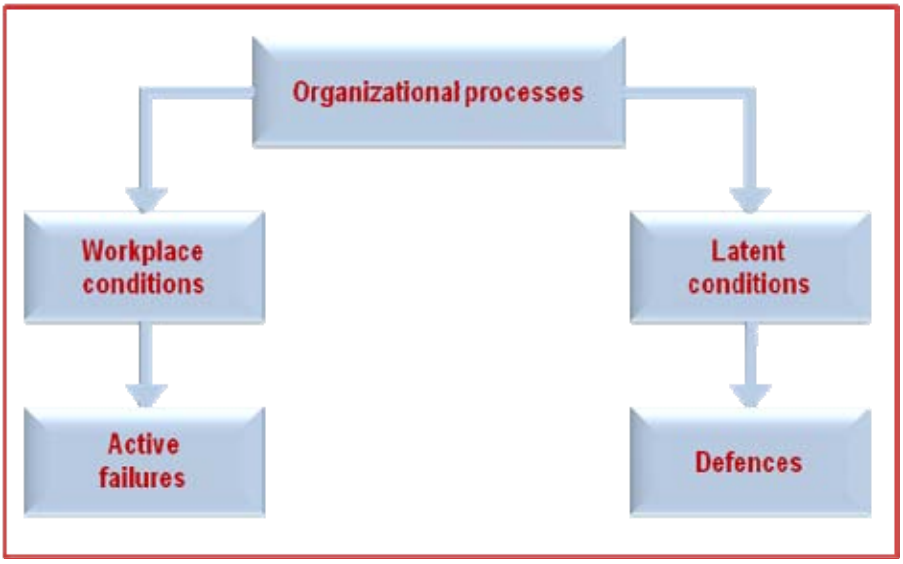



Figure 2-4 – The organizational accident

2.5.2 The top block represents the *organizational process*. These are *activities over which any organization has a reasonable degree of direct control*. Typical examples of such organizational processes include: policy making, planning, communication, allocation of resources, supervision and so forth. Unquestionably, the two fundamental organizational processes as far as safety is concerned are allocation of resources and communication. Downsides or deficiencies in these organizational processes are the breeding grounds for a dual pathway towards failure.

2.5.3 One pathway is the latent conditions pathway. Examples of latent conditions may include: deficiencies in equipment design, incomplete/incorrect standard operating procedures, training deficiencies and so forth. In generic terms, latent conditions can be grouped into two large clusters. One cluster is *inadequate hazard identification and safety risk management*, whereby the safety risks of the consequences of hazards are not kept under control, but roam freely along the system to eventually become active through operational triggers.

2.5.4 The second cluster is known as *normalization of deviance*, a notion that, simply put, is indicative of operational contexts where the exception becomes the rule. The allocation of resources in this case is flawed to the extreme. As a consequence of the lack of resources, the only way that operational personnel, who are directly responsible for the actual performance of the production activities, can successfully achieve these activities is by adopting shortcuts that involve constant violation of the rules and procedures.

2.5.5 Latent conditions have all the potential to breach aviation system *defences*. Typically, defences in aviation can be grouped under three large headings: technology, training and regulations. Defences are usually the last safety net to contain latent conditions, as well as the consequences of lapses in human performance. Most, if not all, mitigation strategies against the safety risks of the consequences of hazards are based upon the strengthening of existing defences or the development of new ones.

2.5.6 The other pathway originating from organizational processes is the *workplace conditions* pathway. *Workplace conditions* are *factors that directly influence the efficiency of people in aviation workplaces*. Workplace conditions are largely intuitive, in that all those with operational experience have experienced them to varying degrees, and include conditions such as: workforce stability, qualifications and experience, morale, management credibility, traditional ergonomics factors such as lighting, heating, cooling, and so forth.

2.5.7 Less than optimum workplace conditions foster *active failures* by operational personnel. Active failures can be considered as either errors or violations. The difference between errors and violations is the motivational component: a person trying to do the best possible to accomplish a task, following the rules and procedures as per the training received, but failing to meet the objective of the task at hand commits an *error*. A person who *willingly* deviates from rules, procedures

or training received while accomplishing a task commits a *violation*. Thus, the basic difference between errors and violation is *intent*.

2.5.8 From the perspective of the organizational accident, safety endeavours should *monitor* organizational process in order to *identify* latent conditions and thus *reinforce* defences. Safety endeavours should also *improve* workplace conditions to *contain* active failures, because it is the concatenation of all these factors that produces safety breakdowns (Figure 2-5).

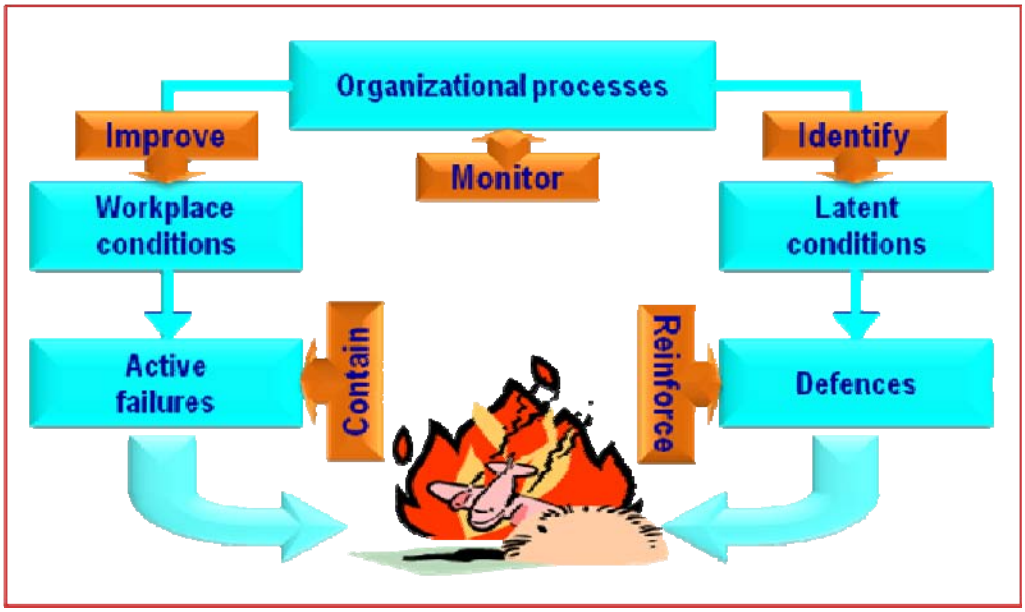



Figure 2-5 – The perspective of the organizational accident

## 2.6 PEOPLE, CONTEXT AND SAFETY – SHEL (L) MODEL

2.6.1 Aviation workplaces are multi-component, multi-feature, complex operational contexts. Their functions and performance involve complex relationships among their many components in order for the system to achieve its production goals.

2.6.2 To understand the human contribution to safety and to support human operational performance necessary to achieve the system's production goals, it is necessary to understand how human operational performance may be affected by the various components and features of the operational context and the interrelationships between components, features and people.

2.6.3 A very simple example is presented in Figure 2-6. The caveman is representative of operational personnel, and the mission (or production goal of the system) is to deliver packages to the other side of the mountains. The different components and features of the operational context and their interaction with the caveman and among themselves will impact the safety and efficiency of the delivery of packages. Thus, the interaction of the caveman with the lions may have detrimental effects in such delivery, unless the caveman is properly equipped to deal with the lions.

2.6.4 Transiting though the mountains on a probably circuitous and unpaved road without footgear will detract from efficient performance (delays in delivering the packages), and may lead to injuries, thereby raising safety concerns. Braving the possible weather without raingear is also a source for potential deficiencies in safety and efficiency.

2.6.5 It is thus evident that proper consideration and analysis of the operational context is a source of valuable information in order to understand operational performance, to support it and to enhance it.


Figure 2-6 – People and safety

2.6.6 The need to understand operational performance within the operational context it takes places in is further illustrated through another example in Figure 2-7A.

2.6.7 In this case, the system's production objective is the delivery of packages by runners between points A and B. It is a basic assumption in the design of the system that runners will follow the shortest route, which is represented by the straight dotted line.

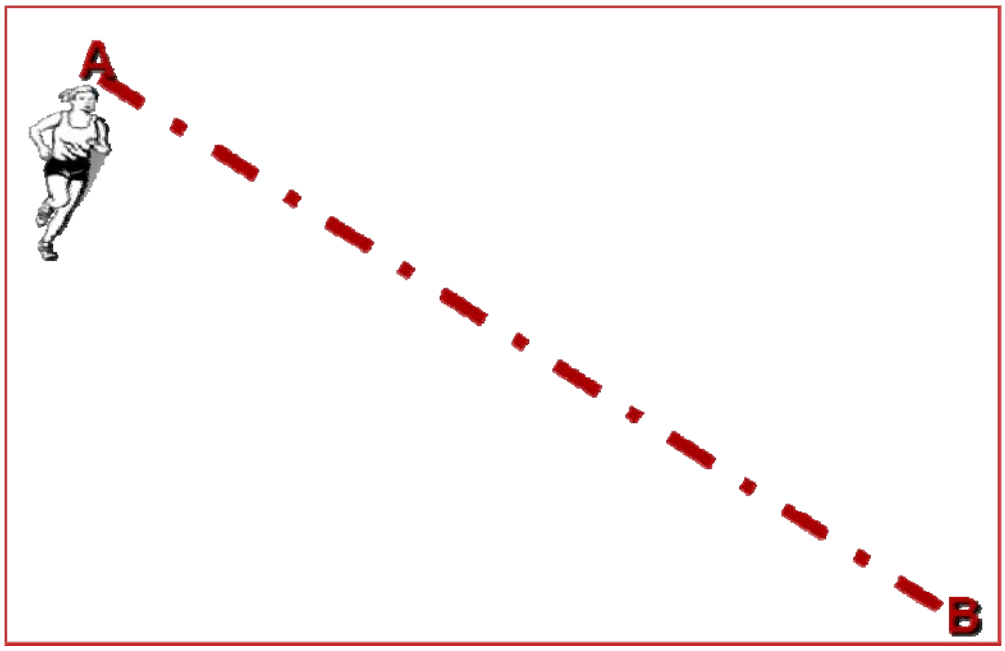


Figure 2-7A – Understanding human performance

2.6.8 No investment is spared to optimally resource the system. The best available human resources, in this case the runners, are selected, trained, indoctrinated and equipped with the best available running gear (technology). As part of the system design, monitoring of operations in real time is included. Once design steps have been completed, operations begin. Shortly after system operational deployment, monitoring of operations in real time begins. Much to the dismay of system managers, real time monitoring discloses that most runners do not follow the intended path, along the dotted straight line, but rather a zigzagging path. As a consequence, delays in delivery take place, and also incidents occur. (Figure 2-7B)

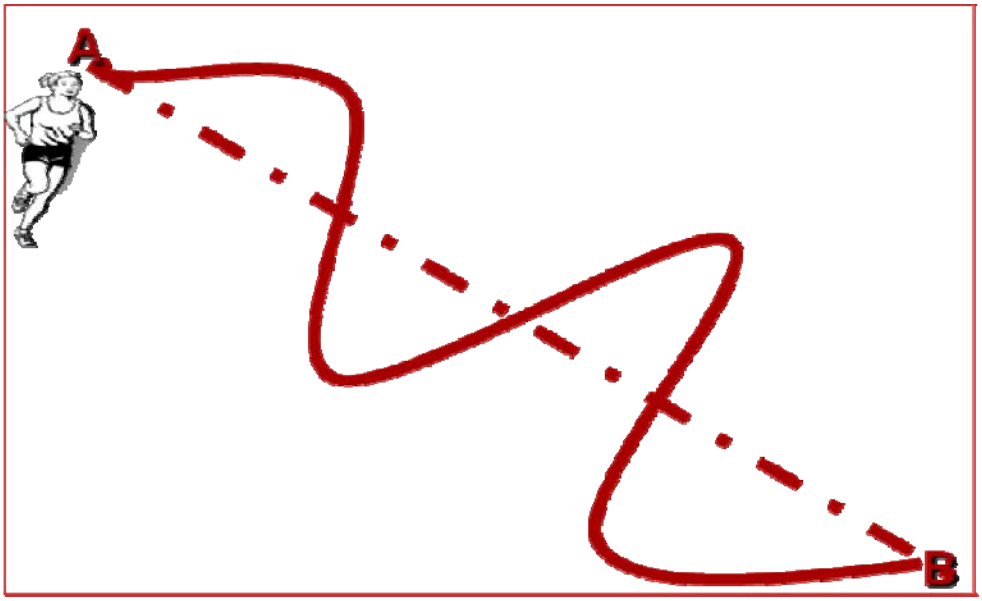



Figure 2-7B – Understanding human performance

2.6.9 At this point, system managers have two options. One option is to follow the traditional perspective discussed in paragraph 2.3.6, and allocate blame and punish the runners for failing to perform as expected. The other option is to analyse the operational context to see if there are components and features of the context that might be the source of adverse interactions with the runners. In following the second option, valuable information about certain components and features within the context will be acquired (Figure 2-7C), which will allow for the readjustment of design assumptions and the development of mitigation strategies for the safety risks of the consequences of unforeseen components and features of the context. In other words, by acquiring information on hazards (discussed in Chapter 4) in the operational context and understanding their interactions with people, system managers can bring the system back under organizational control.

2.6.10 It is thus proposed that proper understanding of operational performance and operational errors cannot be achieved without a proper understanding of the operational context in which operational performance and errors take place. This understanding cannot be achieved unless clear differentiation is made between processes and outcomes. There is a tendency to allocate a symmetry to causes and consequences of operational errors which in real practice does not exist: the very same error can have significantly different consequences, depending upon the context in which the operational error takes place. The consequences of operational errors are not person-dependent but context dependent (Figure 2-8). This concept has a significant impact in mitigation strategies: efficient and effective error-mitigation strategies aim at changing those features and components of the operational context that magnify the consequences of errors, rather than changing people.

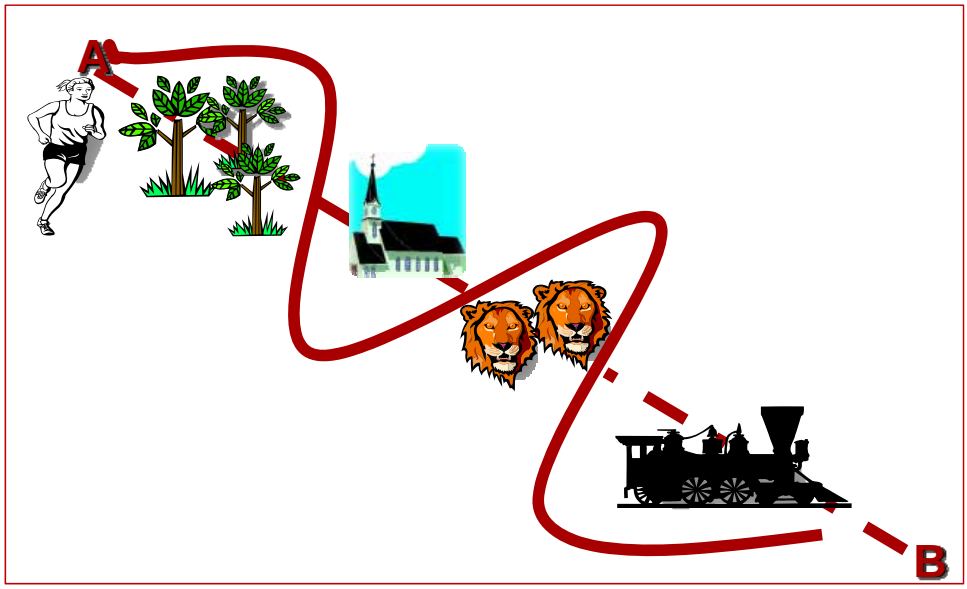



Figure 2-7C – Understanding human performance

2.6.11 The right portion in the example of Figure 2-8 also illustrates a scenario where the two managerial options discussed in paragraph 2.3.6 might apply. Following the traditional approach would lead to reminders about being careful when leaning (or not to lean) on windowsills; about the dangers in pushing flowerpots out of the window, to re-writing of procedures to the previous effects, or to punishment for pushing flowerpots out of the window (failure to perform as expected, or to perform safely). On the other hand, the organizational approach would lead to installing a contention net under the window, the windowsill would be broadened, flowerpots could be made of the frangible type, traffic under the window may be re-routed or, in extreme circumstances, the window would be fenced. The bottom line is that by removing or modifying the error-inducing features in the context, an exponential reduction in the probability and severity of the consequences of operational errors is achieved.

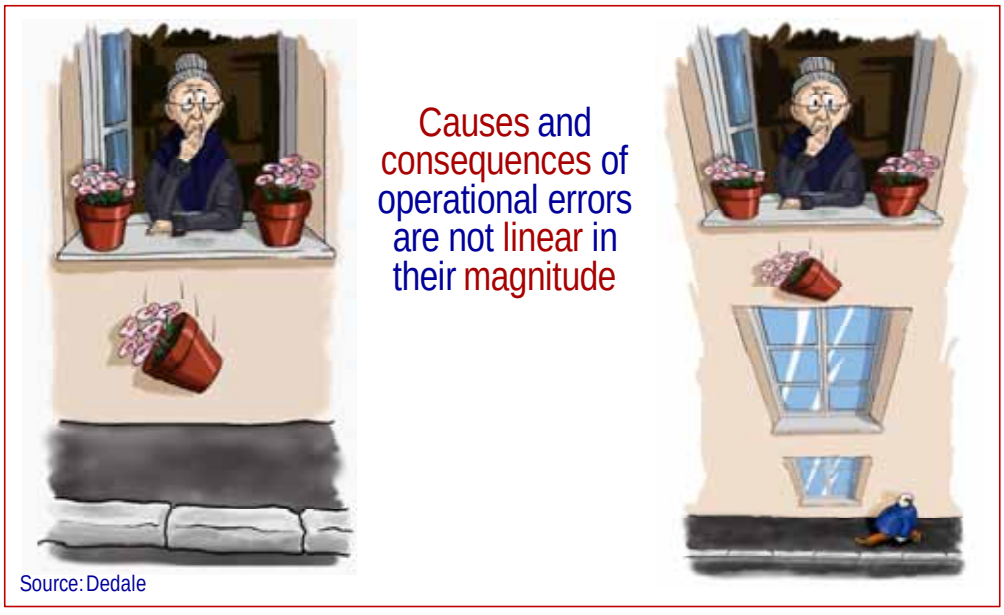



Figure 2-8 – Processes and outcomes

2.6.12 A simple yet visually powerful conceptual tool for the analysis of the components, the features of operational contexts and the possible interactions with people is the SHEL Model. The SHEL model (sometimes referred to as

the SHEL(L) model) can be used to help visualize the interrelationships among the various components and features of the aviation system. This model places emphasis on the individual and the human's interfaces with the other components and features of the aviation system. The SHEL model's name is derived from the initial letters of its four components:

a) ***Software (S)*** (procedures, training, support, etc.);

b) ***Hardware (H)*** (machines and equipment);

c) ***Environment (E)*** (the operating circumstances in which the rest of the L-H-S system must function); and

d) ***Liveware (L)*** (humans in the workplace).

2.6.13 Figure 2-9 depicts the SHEL model. This building block diagram is intended to provide a basic understanding of the relationship of individuals to components and features in the workplace.

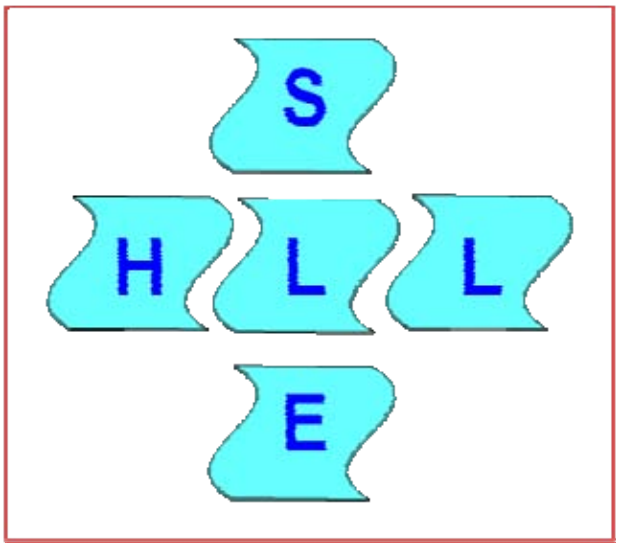



Figure 2-9 – The SHEL(L) model

2.6.14 *Liveware*. In the centre of the SHEL model are the humans at the front line of operations. Although humans are remarkably adaptable, they are subject to considerable variations in performance. Humans are not standardized to the same degree as hardware, so the edges of this block are not simple and straight. Humans do not interface perfectly with the various components of the world in which they work. To avoid tensions that may compromise human performance, the effects of irregularities at the interfaces between the various SHEL blocks and the central *Liveware* block must be understood. The other components of the system must be carefully matched to humans if stresses in the system are to be avoided.

2.6.15 Several different factors put the rough edges on the *Liveware* block. Some of the more important factors affecting individual performance are listed below:

a) *Physical factors:* These include the human's physical capabilities to perform the required tasks, e.g. strength, height, reach, vision and hearing.

b) *Physiological factors:* These include those factors which affect the human's internal physical processes, which can compromise physical and cognitive performance, e.g. oxygen availability, general health and fitness, disease or illness, tobacco, drug or alcohol use, personal stress, fatigue and pregnancy.

c) *Psychological factors:* These include those factors affecting the psychological preparedness of the human to meet all the circumstances that might occur, e.g. adequacy of training, knowledge and experience, and workload.

d) *Psycho-social factors:* These include all those external factors in the social system of humans that bring pressure to bear on them in their work and non-work environments, e.g. an argument with a supervisor, labour-management disputes, a death in the family, personal financial problems or other domestic tension.

2.6.16 The SHEL model is particularly useful in visualizing the interfaces between the various components of the aviation system. These include:

- *Liveware-Hardware (L-H*). The interface between the human and technology is the one most commonly considered when speaking of human performance. It determines how the human interfaces with the physical work environment, e.g. the design of seats to fit the sitting characteristics of the human body, displays to match the sensory and information processing characteristics of the user, and proper movement, coding and location of controls for the user. However, there is a natural human tendency to adapt to L-H mismatches. This tendency may mask serious deficiencies, which may only become evident after an occurrence.

- *Liveware-Software (L-S)*. The L-S interface is the relationship between the human and the supporting systems found in the workplace, e.g. the regulations, manuals, checklists, publications, standard operating procedures (SOPs) and computer software. It includes such *"user friendliness"* issues as currency, accuracy, format and presentation, vocabulary, clarity and symbology.

- *Liveware-Liveware (L-L)*. The L-L interface is the relationship between the human and other persons in the workplace. Flight crews, air traffic controllers, aircraft maintenance engineers and other operational personnel function as groups, and group influences play a role in determining human performance. The advent of crew resource management (CRM) has resulted in considerable focus on this interface. CRM training and its extension to air traffic services (ATS) (team resource management (TRM)) and maintenance (maintenance resource management (MRM)) focus on the management of operational errors. Staff/management relationships are also within the scope of this interface, as are corporate culture, corporate climate and company operating pressures, which can all significantly affect human performance.

- *Liveware-Environment (L-E)*. This interface involves the relationship between the human and both the internal and external environments. The internal workplace environment includes such physical considerations as temperature, ambient light, noise, vibration and air quality. The external environment includes such things as visibility, turbulence and terrain. The 24/7 aviation work environment includes disturbances to normal biological rhythms, e.g. sleep patterns. In addition, the aviation system operates within a context of broad political and economic constraints, which in turn affect the overall corporate environment. Included here are such factors as the adequacy of physical facilities and supporting infrastructure, the local financial situation, and regulatory effectiveness. Just as the immediate work environment may create pressures to take short cuts, inadequate infrastructure support may also compromise the quality of decision-making.

2.6.17 Care needs to be taken in order that operational errors do not "filter through the cracks" at the interfaces. For the most part, the rough edges of these interfaces can be managed, for example:

- The designer can ensure the performance reliability of the equipment under specified operating conditions.

- During the certification process, the regulatory authority can define the conditions under which the equipment may be used.

- The organization's management can develop Standard Operations Procedures (SOPs) and provide initial and recurrent training for the safe use of the equipment.

- Individual equipment operators can ensure their familiarity and confidence in using the equipment safely under all required operating conditions.

## 2.7 ERRORS AND VIOLATIONS

### Operational errors

2.7.1 The growth the aviation industry has experienced over the last two decades would have been impossible had advanced technology not been available to support the increase in demands for the delivery of services. In production-intensive industries like modern aviation, technology is essential to satisfy requirements regarding the delivery of services. This is a fundamental point often overlooked in safety analyses. The introduction of technology does not primarily aim at improving safety; the introduction of technology primarily aims at satisfying the demands in the increase in the delivery of services, *while maintaining* existing margins of safety.

2.7.2 Technology is thus introduced in a massive manner as an effort to satisfy production demands. One result of this massive introduction of technology aimed at improved service delivery is that the Liveware-Hardware interface of the SHEL(L) Model is overlooked, or not always considered to the extent that it should. As a consequence, brittle technology may be introduced, leading to unexpected failures.

2.7.3 While the introduction of brittle technology is an inevitable consequence of the needs of any massive production industry, its relevance to the management of safety cannot be disregarded. People at the "tip of the arrow", such as operational personnel, need to interact daily with technology while performing their operational tasks in order to achieve the delivery of services. If the Hardware-Liveware interface is not properly considered during technology design, and if the operational consequences of the interactions between people and technology are overlooked, the result of such overlook is obvious: operational errors.

2.7.4 The perspective of operational errors as an emerging property of human/technology systems brings a significantly different perspective to the management of safety when compared with the traditional, psychology-based perspective on operational errors. According to the psychology- based perspective, the source of error "resides" within the person, and is a consequence of specific psycho-social mechanisms explored and explained by the different branches of research and applied psychology.

2.7.5 Attempting to anticipate and mitigate operational errors effectively following a psychology-based perspective is extremely difficult if not altogether impossible. Selection may filter out individuals without the basic traits needed for the job at hand, and behaviours can be influenced by training and regulation. Nevertheless, the flaw of this perspective, from a strictly operational viewpoint, is clear: it is impossible to anticipate in a systematic manner typical human frailties such as distraction, tiredness, forgetfulness and so forth, and how then can interact with components and features of an operational context under specific operational conditions. Individual-based mitigation strategies are considered "soft" mitigations, because deficiencies in human performance will pop up when least expected, not necessarily in demanding situations, and unleash their damaging potential.

2.7.6 The perspective of safety as an emerging property of human/technology systems removes the source of the operational error from the human and places it squarely in the physical world, in the L/H interface. A mismatch in the interface is the source of the operational error. As part of the physical world, the source of the operational error thus becomes visible and it can be articulated in operational terms (a switch is partially hidden by a lever making it difficult to observe its correct position during night time operations) as opposed to scientific terms (perceptual limitations). The source of the operational error can therefore be anticipated and mitigated through operational interventions. There in not much that safety management can achieve regarding human perceptual limitations, but there is an array of options available through safety management to counteract the consequences of a design that includes a partially hidden switch.

2.7.7 It is part and parcel of aviation safety tradition to consider operational error as contributing factor in most aviation occurrences. This view, based on the psychology-based perspective discussed above, portrays operational errors as a form of behaviour in which operational personnel willingly engage in, as if operational personnel had a clear option between electing to commit an operational error or not and willingly engage in the first option. Furthermore, an operational error is considered as indicative of sub-standard performance, flaws in character, lack of professionalism, absence of discipline and similar attributions that years of partial understanding of human performance have developed. While convenient to describe events and expedient to blame people, these attributions stop short of understanding and explanation of operational errors.

2.7.8 Following the alternative perspective on operational error discussed, by considering operational errors as an emerging property of human/technology systems, and in placing the source of errors in the mismatch in the L/H interface, it becomes obvious that even the most competent personnel can commit operational errors. Operational errors are then accepted as a normal component of any system where humans and technology interact, and not considered as some type of aberrant behaviour. Errors can be viewed rather as a natural by-product of human-technology interactions during operational activities aimed at the delivery of services of any production system. Operational errors are accepted as a normal component of any system where humans and technology interact, and operational safety strategies are put into practice to control operational errors.

2.7.9 Given the inevitability of mismatches in the interfaces of the SHEL(L) in aviation operations, the scope for operational errors in aviation is enormous. Understanding how these mismatches can affect normal humans at work is fundamental to safety management. Only then can effective measures be implemented to control the effects of operational errors on safety.

2.7.10 It is a common misperception to establish a linear relationship between operational errors and both the immediacy and magnitude of their consequences. This misperception is discussed in paragraphs 2.6.10 and 2.6.11 in terms of operational errors and the magnitude of their consequences. The discussion argues that there is no symmetry between operational errors and the magnitude of their potential consequences. It further argues that the magnitude of the consequences of operational errors is a function of the operational context in which errors take place, rather than a consequence of the errors themselves. The discussion is furthered hereunder in terms of operational errors and the immediacy of their consequences.

2.7.11 It is a statistical fact that in aviation millions of operational errors are made, on a daily basis before a major safety breakdown occurs (Figure 2-10). Minor yearly fluctuations aside, industry statistics consistently propose an accident rate of less than one fatal accident per million departures for the last decade. To put it in different terms, in commercial airline operations worldwide, once every million production cycles an operational error is committed that develops damaging potential strong enough to penetrate system defences and generate a major safety breakdown.

Nevertheless, mismatches in the interfaces of the SHEL(L) Model generate tens of thousands of operational errors on a daily basis during the course of normal aviation operations. These operational errors, however, are trapped by the defences in-depth of the aviation system, and their damaging potential is mitigated, thus preventing negative consequences. In other words, control of operational error takes place on a daily basis through the effective performance of the aviation system defences.


Figure 2-10 – Operational errors and safety – A non linear relationship

2.7.12 A simple operational scenario is presented to explain the asymmetry between operational errors and the immediacy of their consequences (Figure 2-11A). Following engine start up, a flight crew omits to select the flaps to the appropriate take off setting during the after engines start scan flow, as indicated in the standard operating procedures. An operational error has therefore been made, but there are no immediate consequences. The operational error has penetrated the first layer of defence (SOPs, flight crew scan flow sequence following engine start), but its damaging potential is still dormant. There are no immediate consequences; the operational error just remains in the system, in latency.

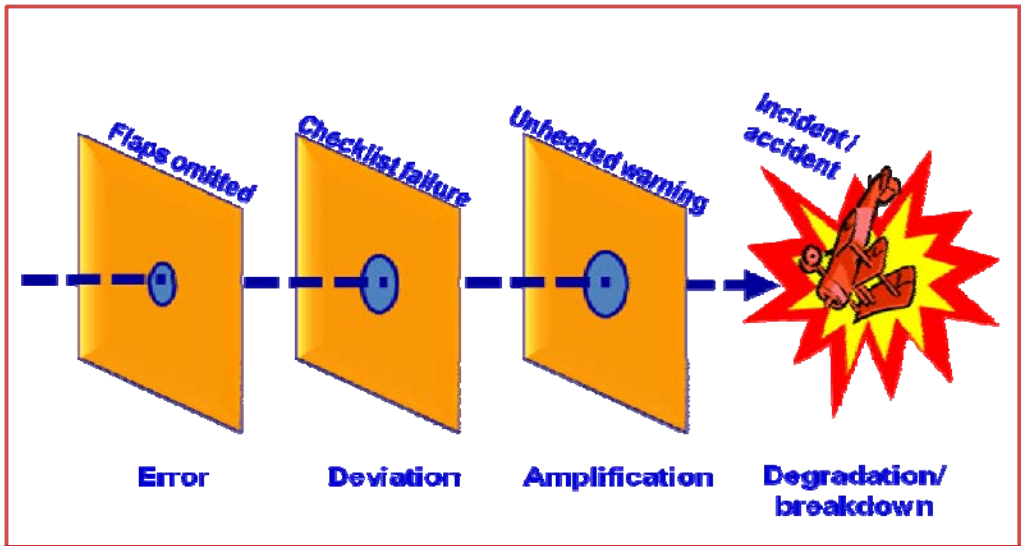



Figure 2-11A – Investigation of major breakdowns – Once in a million flights

2.7.13 The flight crew performs the after engines start checklist, but do not detect the incorrect flap setting and the aircraft initiates taxing for departure. A second opportunity is thus missed to recover from the consequences of the operational error, which continues to remain into the system, still harmless. Nevertheless, the system is now in a state of deviation or undesired state (i.e. aircraft taxing for departure with an incorrect flap setting). The flight crew performs the taxing checklist and the before takeoff checklist. On both occasions, the incorrect flap setting is missed. Further opportunities

to recover from the consequences of the operational error are missed. The operational error remains inconsequential, but the status of deviation, of the undesired state of the system magnifies.

2.7.14 The flight crew starts the take off roll, and the take off warning configuration sounds. The flight crew does not identify the reason for the warning, and continues the take off roll. The operational error still remains inconsequential, but the system undesired state has now progressed to a state of amplification. The aircraft lifts off in an incorrect flaps configuration. The system has now progressed to a state of degradation, but the undesired state can still be conceivably recovered by the flight crew. The aircraft cannot sustain flight because of the incorrect flap setting, and crashes. It is only at that point, after breaching a considerable number of defences in-depth, that the operational error develops its full damaging potential, and becomes consequential. The system experiences a catastrophic breakdown.

2.7.15 Notice the relatively considerable time span between the commission of the operational error by the flight crew and the materialization of its unrecoverable damaging potential. Notice also the number of opportunities to recover from the consequences of the operational error through defences built into the system. This time span is the time that a system affords to control the consequences of operational errors, and it is commensurate with the depth and efficiency of system defences. This is the time span throughout which the management of safety operates with considerable potential for success.

2.7.16 The more in-depth the defences, the more layers of contention the system includes, the more efficient their performance, the greater the possibilities are of controlling the consequences of operational errors. The reverse is true.

2.7.17 From the point of view of this discussion, one conclusion is apparent: the scenario discussed in paragraphs 2.7.2 through 2.7.14 is – unavoidably – what most accident investigations would capture: unmanaged operational errors that lead to catastrophic system breakdowns. This is valuable information about human and systemic failures; information that portrays what failed, what did not work, what defences did not perform as intended. While valuable baseline, this information is not enough to fully understand safety breakdowns and should be complemented by information from alternative sources.

2.7.18 Consider a modified version of the scenario depicted in paragraphs 2.7.12 through 2.7.14 (Figure 2-11B).

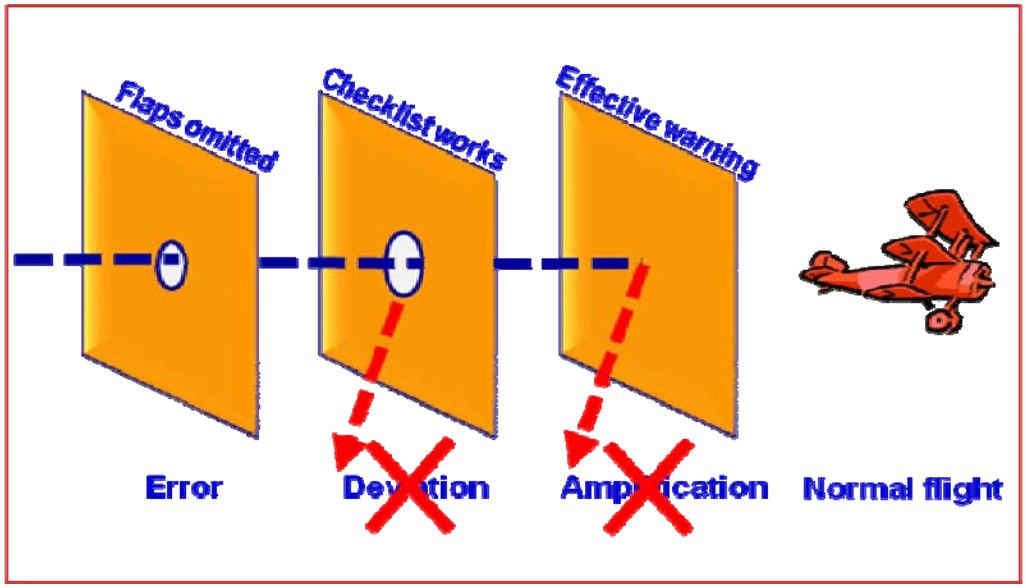



Figure 2-11B – Safety management – On almost every flight

Notice that there are at least four obvious instances where defences could have been triggered to contain the damaging potential of the initial operational error (omission to select take off flaps in the after engines start flight crew scan flow):

- The after start checklist;
- The taxing checklist;
- The before takeoff checklist; and
- The take off configuration warning

2.7.19 There are other instances, not as obvious nonetheless possible, where defences could have been triggered: warnings by ramp personnel, warnings by flight crews in similar aircraft, warnings by ATC personnel, etc. Effective performance of the defences in any of these instances could have controlled the consequences of the initial operational error and restored the system to normal status. The damaging potential of the operational error would have been eliminated at each instance thus making, for practical purposes, the operational error disappear.

2.7.20 The argument advanced here is that scenarios of operational errors inducing catastrophic breakdowns are rare, while scenarios of operational errors inducing system undesired states (deviation/degradation) are frequent. These scenarios capture information on what *initially did not work*, but mostly about *what thereafter worked*, including defences that performed as designed. This is the type of information that the sources of safety information alternative and complementary to the investigation of accidents capture. The information from an accident investigation would certainly identify the four instances in which defences would have been triggered, but it can in all likelihood only explain why they were not.

2.7.21 The additional sources of information under discussion would identify the instances in which defences should have been triggered, and describe why they were. These sources characterise *successes;* and thus, integrating the information from accidents with the information from these alternative sources provides for a more complete picture about specific safety concerns. Furthermore, because scenarios as the one described in this paragraph are frequent, these alternative sources of safety information – if deployed – provide considerable volume of constant information, to complement the more sporadic information provided by accidents, thus allowing for a fuller understanding about the potential for safety breakdowns. The conclusion than can be drawn from this second scenario is that safety resiliency is not so much a question of operational error-free performance, but rather a question of effective operational error management.

### Three strategies for the control of operational error

2.7.22 The three basic strategies to control operational errors are based upon the three basic defences of the aviation system: technology, training and regulations (including procedures).

2.7.23 R*eduction strategies* intervene directly at the source of the operational error by reducing or eliminating the contributing factors to the operational error. Examples of reduction strategies include improving the access to aircraft components for maintenance, improving the lighting in which the task is to be performed, reducing environmental distractions and so forth:

- Human-centred design
- Ergonomic factors
- Training
- …

2.7.24 *Capturing strategies* assume the operational error has already been made. The intent is to "capture" the operational error before any adverse consequences of the operational error are felt. Capturing strategies are different from reduction strategies in that they does not directly serve to eliminate the error:

- Checklists
- Task cards
- Flight strips
- …

2.7.25 *Tolerance strategies* refer to the ability of a system to accept an operational error without serious consequence. Example of a measure to increase system tolerance to operational errors is the incorporation of multiple hydraulic or electrical systems on an aircraft to provide redundancy, or a structural inspection programme that provides multiple opportunities to detect a fatigue crack - before it reaches critical length:

- System redundancies
- Structural inspections
- …

2.7.26 Operational error management must not limited to front-line personnel. The performance of front-line personnel is, as depicted by the SHEL(L) Model, influenced by organizational, regulatory, and environmental factors. For example, organizational processes, such as inadequate communication, ambiguous procedures, unreasonable scheduling,

insufficient resources, unrealistic budgeting, etc., constitute the breeding grounds for operational errors. As already discussed, all these are processes over which an organization must have a reasonable degree of direct control.

### Errors *vs.* violations

2.7.27 Thus far, the discussion in this section has focussed on operational errors, which have been characterised as a normal component of any system where people and technology interact to achieve system production goals. The discussion will now focus on violations, which are quite different from operational errors. Both can lead to failure of the system, and can result in high-consequence situations. A clear differentiation and understanding between operational errors and violations is essential for the purpose of the management of safety.

2.7.28 The fundamental difference between operational errors and violations lies in *intent*. While an error is unintentional, a violation is a deliberate act. People committing operational errors are trying to do the right thing, but for the many reasons discussed in previous paragraphs on operational error, they fail to achieve their expectations. People committing violations, on the other hand, know that they are engaging in behaviours that involve a deviation from established procedures, protocols, norms or practices, yet, they persevere in the intent.

2.7.29 For example, a controller allows an aircraft to descend through the level of a cruising aircraft when the DME distance between them is 18 NM, and this occurs in circumstances where the correct separation minimum is 20 NM. If the controller miscalculated the difference in the DME distances advised by the pilots, this would be an operational error. If the controller calculated the distance correctly, and allowed the descending aircraft to continue through the level of the cruising aircraft knowing that the required separation minimum did not exist, this would be a violation.

2.7.30 In aviation, most violations are the result of deficient or unrealistic procedures where people have developed "work arounds" to accomplish the task. Most stem from a genuine desire to do a good job. Seldom are they acts of negligence. There are two general types of violations: situational violations and routine violations.

2.7.31 *Situational violations* occur due to the particular factors that exist at the time, such as time pressure or high workload. In spite of the knowledge that a violation is being incurred, goal-orientation and mission achievement lead people to deviate from norms, in the belief that the deviation does not bear adverse consequences.

2.7.32 *Routine violations* are violations which have become 'the normal way of doing businesses" within a work group. They occur when the work group has difficulty in following procedures in order to get the job done, because of practicality/workability issues, deficiencies in human-technology interface design and so forth, and informally devise and adopt "better" procedures, which eventually become routine. This is the notion of normalization of deviance discussed in paragraph 2.5.4. Routine violations are seldom considered as such by a work group, because their objective is to get the job done. They are considered as "optimising" devices, since they aim at saving time and effort by simplifying a task (even if it involves cutting corners).

2.7.33 A third, and less often considered, type of violation which is often overlooked are *organization-induced violations,* which to can be viewed as an extension of the routine violations. The full potential of the safety message that violations can convey can only be understood when considered against the demands imposed by the organization regarding the delivery of the services for which the organization was created in the first place. Figure 2-12 depicts the relationship between the two basic considerations an organization must weigh and balance in relation to the delivery of its services and when defining its organizational processes: system output and related safety risk.

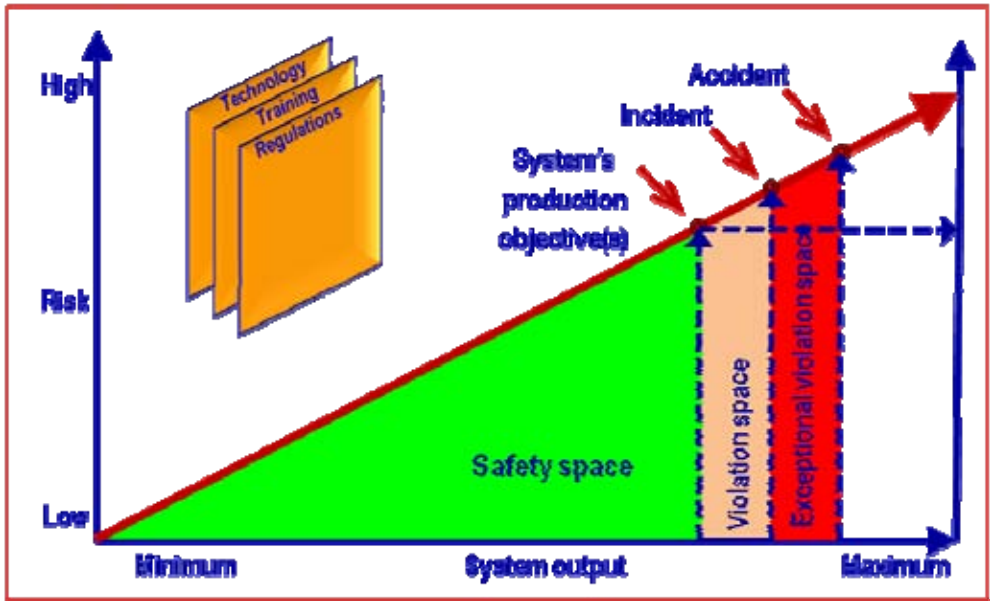



Figure 2-12 – Understanding violations

2.7.34 In any organization engaged in the delivery of services, system output and safety risks are intertwined. As demands for system output (i.e. delivery of services) increase, the safety risks associated with the delivery of services also increase, because of the increase in exposure. Therefore, as Figure 2-12 illustrates, minimum system output correlates with the lowest safety risk, while maximum system output correlates with the highest safety risk. Continuous operation exposed to highest safety risks is undesirable, not only from a safety standpoint but also from a financial standpoint. Thus, organizations interpolate between desirable output and tolerable safety risk, and define a system output that is less than the maximum possible, but which correlates with a tolerable level of safety risk. In so doing, the organization has defined its *production objectives*, as a function of balancing acceptable output with acceptable safety risk.

2.7.35 One fundamental decision related to the process of defining production objectives (agreed on the basis of a balance compromise between system output and safety risks) is the establishment of the *defences* that the organization needs to develop in order to protect itself from the safety risks it will generate while producing. As already discussed, the three basic defences of the aviation system are technology, training and regulations (including procedures). Therefore, when defining its production objectives, the organization also needs to define what are the tools (technology) necessary to safely and effectively achieve service delivery; how to foster the behaviours the workforce must exhibit to safely and efficiently use the tools (training), and the set of norms and procedures that dictate workforce performance (regulations).

2.7.36 Thus, system output, level of safety risk and defences converge to the point that defines the production objectives of the organization. They also depict the boundaries of what may be called the "safety space of the organization". The safety space represents a protected zone, the zone within which the defences that the organization has erected guarantee maximum resilience to the safety risks the organization will face while delivering the system output in terms of production objectives.

2.7.37 The reason for the maximum resilience that the safety space affords is that the defences erected by the organization are commensurate to the planned system output, which in turn is commensurate to the tolerable safety risk. In other words, the resources allocated by the organization to protect are appropriate and commensurate to the activities related to the delivery of services. This does not mean that the organization cannot experience an accident, since accidents are random events resulting from the concatenation of unforeseeable circumstances. It means that the organization has arrangements for the management of safety that guarantee an acceptable control of safety risks during the delivery of services, *under foreseeable circumstances*. Simply put, the organization has done the best it possibly can, safety-wise.

2.7.38 Given the dynamic nature of aviation, organizations may occasionally face transient, short-term demands for increased output (i.e. increased delivery of services) during brief periods of time, for example, seasonal variations in seat demands, specific circumstances such a worldwide sporting event, and so forth. In order to maintain intact the safety zone, the organization should review and re-arrange or modify its existing allocation of resources, and strengthen existing defences to counteract the increased output and the ensuing increased level of safety risk.

2.7.39 Aviation history, sadly, suggests otherwise. Quite too often, as the aftermath of safety breakdowns show, aviations organizations try to cope with short periods of increased system output by "stretching" defences: resorting to overtime instead of hiring additional personnel, thus leading to increased workload and fatigue; using technology in "more efficient" ways instead of incorporating additional technology; "optimising" procedures and resources without revising standard operating procedures and norms, and so forth.

2.7.40 What this stretching of defences effectively does is it places the organization outside the safety space, first into the violation space, and ultimately into the exceptional violation space. In other words, in order to deliver the increased output with same resources, operational personnel must deviate from established processes by resorting to shortcuts or workarounds *sanctioned* by the organization. The operational personnel did not elect to engage in such shortcuts or workarounds, the organization did. The colloquial expression "giving a leg up to the company" eloquently describes the situation in which people are forced to engage in organization-sanctioned deviations to deliver a system output incommensurate with the resources allocated to such an end.

2.7.41 Hard evidence that the organization has drifted into the violation space is generally provided by incidents. A learning organization will then reassess its allocation of resources to expand its safety space in order to maintain the harmony between system output, tolerable safety risk and defences or, if unable to expand its safety space, it will retract into the established safety space by reducing the system output. Some organizations will ignore the warnings provided by incidents, persist in their course of action, and thus inevitably drift into the exceptional violation space. An accident is then a likely outcome.

## 2.8 ORGANIZATIONAL CULTURE

2.8.1 Culture can be described in the simplest terms as a "collective programming of the mind". One of the most graphic descriptions of culture portrays it as the "software of the mind". Culture influences the values, beliefs and behaviours that we share with the other members of our various social groups. Culture binds us together as members of groups and provides clues and cues as to how to behave in both normal and unusual situations. Culture sets the rules of the game, or the framework for all our interpersonal interactions. It is the sum total of the way people conducts their affairs in a particular social milieu, and provides a context in which things happen. In terms of the management of safety, understanding culture is as important as understanding context, since culture is an important determinant of human performance.

2.8.2 It is a common pitfall when studying culture and, in particular, cross-cultural issues as they may affect aviation safety, to unwillingly engage in judgement, and portray one particular culture as perhaps "better" or "more suited" than another, or propose one particular culture as "bad" or "unsuitable" for specific safety proposals. This is inappropriate and fruitless, because the study of cross-cultural issues is – in terms of safety or else – about *differences*, not *judgment*. Cultures are indeed different, and each and every culture has significant strengths as well as identifiable weaknesses. The purpose of serious cross-cultural endeavours, when applied to the management of safety, is to build upon combined cultural strengths, as they relate to safety practices, while minimising the downside of combined cultural weaknesses.

2.8.3 Organizations, being groups of people, are not immune to cultural considerations. Organizational performance is subject to cultural influences at every level. The following three levels of culture (Figure 2-13) have relevance to safety management initiatives, since the three levels are determinants of organizational performance:

a) *National culture* differentiates the national characteristics and value systems of particular nations. People of different nationalities differ, for example, in their response to authority, how they deal with uncertainty and ambiguity, and how they express their individuality. People are not all attuned to the collective needs of the group (team or organization) in the same way. In collectivist cultures, for example, there is acceptance of unequal status and deference to leaders. This may affect the possibility of questioning decisions or actions by elders — an important consideration in teamwork for example. Work assignments that mix national cultures may thus affect team performance by creating misunderstandings.

b) *Professional culture* differentiates the characteristics and value systems of particular professional groups (the typical behaviour of pilots *vis à vis* that of air traffic controllers, or maintenance engineers). Through personnel selection, education and training, on-the-job experience, peer pressure, etc., professionals (physicians, lawyers, pilots, controllers) tend to adopt the value system and develop behaviour patterns consistent with their peers; they learn to "walk and talk" alike. They generally share a pride in their profession and are motivated to excel in it. On the other hand, they may adopt value systems that lead to developing sense of personal invulnerability, a feeling that performance is not affected by personal problems, or that errors will not be made in situations of high stress.


Figure 2-13 – Three distinct cultures

c) *Professional culture* differentiates the characteristics and value systems of particular professional groups (the typical behaviour of pilots *vis à vis* that of air traffic controllers, or maintenance engineers). Through personnel selection, education and training, on-the-job experience, etc., professionals (physicians, lawyers, pilots, controllers) tend to adopt the value system and develop behaviour patterns consistent with their peers; they learn to "walk and talk" alike. They generally share a pride in their profession and are motivated to excel in it. On the other hand, they may adopt value systems that lead to developing sense of personal invulnerability, a feeling that performance is not affected by personal problems, or that errors will not be made in situations of high stress.

d) *Organizational culture* differentiates the characteristics and value systems of particular organizations (the behaviour of members of one company *vs.* that of another company, or government *vs.* private sector behaviour). Organizations provide a shell for national and professional cultures. For example, in an airline, pilots may come from different professional backgrounds (military *vs.* civilian experience, bush or commuter operations *vs.* development within a large carrier). They may also come from different organizational cultures due to corporate mergers or lay-offs.

2.8.4 The three cultural sets described above interact in operational contexts. These interactions determine for example how:

a) juniors will relate to their seniors;

b) information is shared;

c) personnel will react under demanding operational conditions;

d) particular technologies will be embraced;

e) authority will be acted upon and how organizations react to operational errors (punish offenders or learn from experience);

f) automation is used;

g) procedures (SOPs) are developed;

h) documentation is prepared, presented, and received;

i) training is developed and delivered;

j) work assignments are made;

k) different work groups (pilots, ATC, maintenance personnel, cabin crew) will relate; and

l) management and unions will relate.

In other words, culture impacts on virtually every type of interpersonal and inter-organizational interaction. In addition, cultural considerations creep into the design of equipment and tools. Technology may appear to be culture-neutral,

but it reflects the biases of the manufacturer (consider the English language bias implicit in much of the world's computer software). Yet, for all the above discussion, there is no right and no wrong culture; they are what they are and they each possess a blend of strengths and weaknesses.

2.8.5 The greatest scope for creating and nourishing an effective, generative culture for the management of safety is at the organizational level. Operational personnel in aviation are influenced in their day-to-day behaviour by the value system of their organization. Does the organization recognize safety merit? Promote individual initiative? Discourage or encourage risk taking? Enforce strict SOP compliance or tolerate breeches of SOPs? Promote open two-way communications? Thus, the organization is a major determinant of the behaviours employees will engage in while performing operational activities that support the delivery of services for which the organization is in business. Organizational culture sets the boundaries for accepted operational performance in the workplace by establishing the norms and limits. Thus, organizational culture provides a cornerstone for managerial and employee decision-making: **"This is how we do things here, and this is the way we talk about the way we do things here."**

2.8.6 Organizational culture then consists of shared beliefs, practices and attitudes. The tone for an effective, generative organizational culture is set and nurtured by the words and actions of senior management. Organizational culture is the atmosphere created by senior management which shapes workers' attitudes towards, among others, safety practices. Organizational culture is affected by such factors as:

a) policies and procedures;

b) supervisory practices;

c) safety planning and goals;

d) actions in response to unsafe behaviours;

e) employee training and motivation; and

f) employee involvement or "buy in".

2.8.7 The ultimate responsibility for the establishment and adherence to sound safety practices rests with the directors and management of the organization – whether it is an airline, an aerodrome, an ATS or an AMO. The safety ethos of an organization is established from the outset by the extent to which senior management accepts accountability for safe operations, and for dealing with emerging safety concerns.

2.8.8 How line management deals with day-to-day activities is fundamental to an organizational culture which is generative for the management of safety. Are the correct lessons being drawn from actual line experiences and appropriate actions taken? Is the affected staff constructively involved in this process, or do they feel they are the victims of management's unilateral action?

2.8.9 The relationship that line management has with the representatives of the regulatory authority is also indicative of a generative organizational culture. This relationship should be marked by professional courtesy but with enough distance so as not to compromise accountability. Openness will lead to better safety communications rather than strict enforcement of regulations. The former approach encourages constructive dialogue, while the latter encourages concealing or ignoring the real safety problems.

2.8.10 Although compliance with safety regulations is fundamental to the development of sound safety practices, contemporary thinking is that much more is required. Organizations that simply comply with the minimum standards set by the regulations are not well situated to identify emerging safety problems.

2.8.11 An effective way to promote safe operations is to ensure that an operator has developed an operational environment where all staff feels responsible for and considers the impact of safety on everything they do. This way of thinking must be so deep-rooted in their activities that it truly becomes 'the way we do business around here'. All decisions, either by the Board of Directors, by a driver on the ramp, or by an engineer, need to consider the implications on safety.

2.8.12 Such an operational environment must be generated from the 'top down' and relies on a high degree of trust and respect between workers and management. Workers must believe that they will be supported in any decisions made in the interest of safety. They must also understand that intentional breaches of safety that jeopardize the operation will not be tolerated.

### Effective safety reporting

2.8.13 One of the most influential aspects of an organizational culture in terms of the management of safety is that it shapes safety reporting procedures and practices by operational personnel. Identification of hazards is a fundamental activity underlying the management of safety. Nobody is in a better position to report the existence of hazards, of what works

the way it is supposed to work and of what does not, than operational personnel, who have to live with and face hazards on an everyday basis. Effective safety reporting of hazards by operational personnel is therefore a cornerstone of the management of safety. Therefore, an operational environment in which operational personnel have been trained and are constantly encouraged to report hazards is the prerequisite for effective safety reporting.

2.8.14 Effective safety reporting builds upon certain basic attributes, such as:

a) senior management place strong emphasis on hazard identification as part of the strategy for the management of safety, and as a consequence there is an awareness of the importance of communicating hazard information at all levels of the organization;

b) senior management and operational personnel hold a realistic view of the hazards faced by the organization's service delivery activities and, as a consequence, there are realistic rules relating to hazards and to potential sources of damage;

c) senior management define the operational requirements needed to support active hazard reporting, ensure that key safety data is properly registered, demonstrate a receptive attitude to the reporting of hazards by operational personnel and implement measures to address the consequences of hazards;

d) senior management ensure that key safety data is properly safeguarded and promote a system of checks and balances so that reporters of hazards feel confident that hazard reporting will not be put to uses others than for which it was implemented (the management of safety);

e) personnel are formally trained to recognise and report hazards and understand the incidence and consequences of hazards in the activities supporting delivery of services; and

f) there is a low incidence of risk-taking behaviour, and a safety ethic which discourages such behaviour.

**Effective safety reporting – Five basic traits**

2.8.15 There are five basic traits that are universally associated with effective safety reporting systems. (Figure 2-14) These five basic traits are related to the basic attributes of effective safety reporting discussed in paragraph 2.8.14:

a) *Willingness*. As a consequence of deliberate efforts by senior management to define the operational requirements needed to support active hazard reporting and to ensure that key safety data is properly registered, operational personnel are willing to report hazards, operational errors that might arise from exposure to hazards, as well as their personal experiences as appropriate.

b) *Information*. As a consequence of the formal training to recognise and report hazards and to understand the incidence and consequences of hazards in the activities supporting delivery of services, operational personnel are knowledgeable about the human, technical and organizational factors that determine the safety of the system as a whole.

c) *Flexibility*. As a consequence of holding realistic views of the hazards underlying the organization's service delivery activities and the development of realistic rules relating to hazards and to potential sources of damage, operational personnel can adapt hazard reporting when facing unusual circumstances, shifting from the established mode to a direct mode thus allowing information to quickly reach the appropriate decision-making level.

d) *Learning*. As a consequence of the awareness of the importance of communicating hazard information at all levels of the organization, operational personnel have the competence to draw conclusions from safety information systems and the organization has the will to implement major reforms.

e) *Accountability*. As a consequence that key safety data is properly safeguarded, and the promotion of a system of checks and balances that ensures that reporters of hazards feel confident that hazard reporting will not be put to uses others than for which it was implemented, operational personnel are encouraged (and rewarded) for providing essential safety information related to hazards. However, there is a clear line that differentiates between acceptable and unacceptable operational performance.

2.8.16 Effective safety reporting is a cornerstone of the management of safety. Once reported, information on hazards is turned into safety data. Effective safety reporting is therefore the gate for safety data acquisition. Once acquired, safety data must be managed. Safety data management builds upon three clearly defined steps. The first two steps in safety data management are the collection of safety data on hazards and analysis of safety data, to turn data into information. The third, and often overlooked step, is the mitigation or response activities to hazards by the organization as a consequence of

the safety information developed. An organization's response to safety information on hazards may vary from active mitigation to blatant disregard.

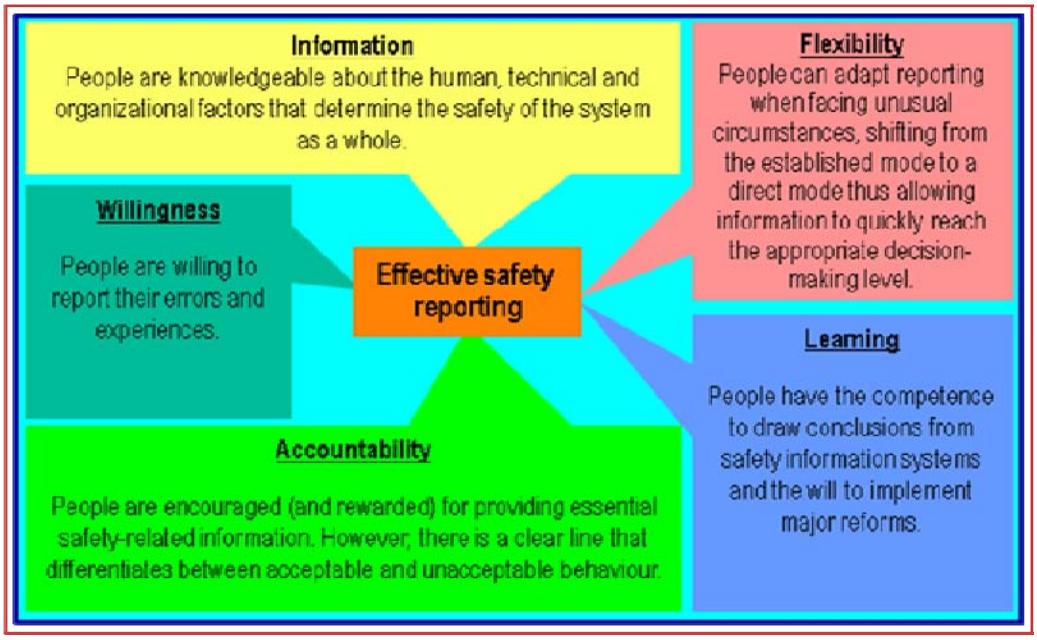



Figure 2-14 – Effective safety reporting – Five basic traits

2.8.17 Organizational literature proposes three characterizations of organizations, depending on how they respond to information on hazards and safety information management:

a) *Pathological* – Hide the information

b) *Bureaucratic* – Restrain the information

c) *Generative* – Value the information

2.8.18 Table 2-1 below presents a matrix that summarizes, in a self-explanatory manner, key aspects of the management of safety information compared to the three organizational characterizations discussed in paragraph 2.8.17.

| | Pathological | Bureaucratic | Generative |
|---|---|---|---|
| Information | Hidden | Ignored | Sought |
| Messengers | Shouted | Tolerated | Trained |
| Responsibilities | Shirked | Boxed | Shared |
| Reports | Discouraged | Allowed | Rewarded |
| Failures | Covered up | Merciful | Scrutinized |
| New ideas | Crushed | Problematic | Welcomed |
| Resulting organization | Conflicted organization | "Red tape" organization | Reliable organization |

Table 2-1 – Three possible organizational cultures

### Culture, blame and punishment

2.8.19 Effective safety reporting, safety data management and the management of safety rely to a large degree on the voluntary reporting of events, hazards and personal experiences by the people who "operate the system". These are the operational personnel who deliver, through their daily activities, the services for which the organization is in business. During activities related to the delivery of services, operational personnel must co-exist with hazards on a daily basis. For this reason hazard reporting by operational personnel is a rich source of safety information for organizations.

2.8.20 Voluntary reporting systems were conceived during the late Seventies and early Eighties. They were developed as error reporting systems rather than hazard reporting systems, coinciding with the deployment of Human Factors in aviation as discussed in Section 2.3 under the evolution of safety thinking. Error reporting systems have multiplied in the intervening years.

2.8.21 Since the inception of voluntary reporting systems, a growing understanding of operational errors has led errors to be viewed as the results of some existing condition or circumstance, as discussed in Section 2.7. As a result, safety management seeks out existing conditions or circumstances that are the genesis of operational errors. The systematic identification of safety deficiencies pays a much higher dividend for safety management than simple error collecting and counting. In terms of voluntary reporting systems, this has led to a shift from *error reporting* systems to *hazard reporting* systems.

2.8.22 Nevertheless, the notion of voluntary reporting systems as error reporting systems instead of hazard reporting systems is pervasive in aviation. Many organizations have not yet transitioned to the realization that safety management action can most effectively take place when aimed at material and identifiable components of the operational context (hazards) rather than to the vagaries associated with human performance. In other words, that it is more practical, easier and to a large extent more effective, to fix contexts than it is to fix people.

2.8.23 The difference between error reporting and hazard reporting is fundamental. Error reporting is self-incriminatory and may thus lead to blame and punishment, while hazard reporting is objective and neutral. Because of the early and pervasive emphasis on error reporting as opposed to hazard reporting, the protection of reporters has been a hot topic since the inception of reporting systems, while at the same time a source of polemic and debate. Inevitably, the debate has drifted into the wrong direction, on most fronts.

2.8.24 Various terms such as responsibility, accountability and liability have been used to refer to different aspects of the same concept; systemic failures have been used to dilute personal accountabilities within the impersonal dimensions of organizations; individual failures have been used to excuse the absence of a clear definition of responsibilities that should define the boundaries of operational performance and duty; punishment has been used to shield the fact that professionals are oftentimes deprived of the means to perform operationally according to duty statements, and so forth. Beyond these considerations, the protection of sources of safety information remains a contentious issue, and one with the potential to turn into a significant obstacle for the progress of safety management.

2.8.25 Probably the most significant aspect of the debate, and certainly its most polemic, is linking the protection of voluntary hazard reporting systems with the blanket, unqualified protection of accident investigation records. In the enthusiasm to realise the full safety potential of the collection of safety information, the need to protect records from voluntary hazard reporting systems and the need to protect records from accidents and serious incidents, *without properly qualifying exactly what accident and serious incident records should be protected*, has been confused. Clearly, two significantly different safety information systems have been thrown into the same bag.

2.8.26 A judicial investigation, and subsequent retribution in some form, should not be unexpected following an aviation accident or serious incident, because deficiencies in the system or deviations from system baseline performance have realised their full damaging potential. As a consequence, lives have probably been lost and property damaged, even if no negligence or ill-intent existed. This is not the case with information from a voluntary hazard reporting system. Voluntary hazard reporting systems generate information on deficiencies in the system or deviations from baseline system performance that have not released their damaging potential; no lives have been lost nor property damaged.

2.8.27 The unclear message from aviation professionals intent on protecting safety information has therefore been frequently misunderstood, because it has too often challenged the legitimacy of the judicial investigation itself. Opposing judicial investigations arguing that safety benefits outweigh judicial interests, while understandable within safety circles and the aviation industry at large, has only strengthened the determination of judicial authorities who believe the argument equals a demand for undue immunity.

2.8.28 Culture has not escaped this drift into the wrong direction and its underlying polemic debate. Throughout the years, the industry has witnessed a progression in attempts to interface culture with the protection of safety information and the protection of reporters from retribution, as a means of improving safety. Early notions advocating for a "non-punishing culture" evolved into "non-blame culture" or "blame-free culture"; and eventually into "safety culture" and "just culture".

2.8.29 Safety culture and just culture have become broadly accepted labels that generally describe an organizational culture that fosters safe practices and encourages active and effective safety reporting while affording protection to reporters. Nevertheless, unless a balanced perspective is adopted, such labels – like all folk labels – hold potential for misperceptions and misunderstandings, and ultimately for aberrant endeavours.

2.8.30 Firstly, because the term *culture* is used loosely, if not liberally, to describe *context* (*safety reporting culture* as opposed to *context in which effective safety reporting takes place*).

2.8.31 Secondly, because safety culture, just culture and similar labels are constructs (abstractions). These labels portray shortcuts that describe very specific, geographically constricted values and beliefs representing what the building blocks of dedicated processes and practices regarding safety and fairness should consist of. Such dedicated processes and practices are naturally underpinned by, and biased towards, the specific, local values and beliefs of the culture that proposes them, and therefore far from universal. As biased constructs, safety culture, just culture and similar shortcuts not only are discriminatory and judgemental, but in addition they are not tangible, they are immaterial, and they do not exist in the physical world. They are a product of the human mind, and therefore impossible to act upon.

2.8.32 Thirdly, both safety culture and just culture are outcomes. They are the consequence of a series of organizational processes and practices. Organizations engage or do not engage in certain specific processes and practices, as a consequence of which they achieve or do not achieve these outcomes. As outcomes, and just like constructs, neither safety culture nor just culture can in themselves be acted upon, only the processes and practices leading to them can be.

2.8.33 Fourthly, while the notions of both safety and just culture as well as their predecessor notions are multi-block constructs, the common thread is the contention that a safety or a just culture is one in which operational personnel can report their errors without fear of reprisal, as long as negligence or wilful disregard for safety is not evident. Herein lays the most significant drawback of espousing the process of the acquisition of safety information on hazards and its supporting procedures, to constructs.

2.8.34 By linking safety culture and just culture to the protection of people, the legal argument discussed in paragraph 2.8.25 through 2.8.27 takes precedence over any technical or safety-related argument. The perception is created that the objective of a safety culture or a just culture is to preclude the possibility of the so-called "criminalization of error". This is an endeavour which, while of understandable moral and ethical relevance, is of lesser relevance, strictly speaking, for purposes related to the management of safety. While arguably abhorrent in certain circles, the so-called "criminalization of error" is legally, ethically and morally within the sovereign rights of any country, provided established international agreements are observed. Strictly speaking, for purposes related to the management of safety, the process that needs to be promoted, nurtured and defended is *effective safety reporting*. But then , the achievement of this process can be materialised in many different ways and following many different strategies.

2.8.35 Therefore, *how* effective safety reporting is achieved should be left to the preferences, possibilities and constraints of specific contexts, local values and beliefs, rather than proposing off-the-shelf recipes reminiscent of cultural imperialism and with the potential to clash with local values and beliefs. As long as an organization develops and nurtures the process of effective safety reporting to support the management safety, *how* it does is irrelevant, provided effective safety reporting *is* indeed achieved.

2.8.36 A fifth and last argument in favour of the process of effective safety reporting and against the constructs of safety culture and just culture should also be noted. The notion of an off-the-shelf safety culture or of a just culture underpinned by specific building blocks inevitably drifts into a classical stereotypical situation: those organizations which do not adhere to the specific building blocks proposed would by logical reasoning exhibit an *unsafe* culture or an *unjust* culture. This is a highly questionable cause-effect relationship, and a very dangerously loaded one.

2.8.37 Organizations may not adhere to the specified building blocks of the accepted constructs, yet they may arguably develop effective safety reporting processes to support the management of safety, following building blocks more attuned to local values and beliefs. As a multi-national organization, ICAO cannot adhere to the stereotypical branding of local values and beliefs, nor allocate supremacy to one set of particular values or belief over another. Therefore, discussions in this Manual distance themselves from the constructs of safety culture and just culture, and are restricted to the development of an *organizational culture that fosters safe practices and encourages the process of active and effective safety reporting*, through whichever means or building blocks it might be achieved.

## 2.9 SAFETY INVESTIGATION

2.9.1 The investigation of safety occurrences is an important component of the management of safety. Chapter 7 characterises the accident investigation process as the ultimate goalkeeper of system safety. The value of the safety investigation is, however, proportional to the approach under which the investigation is carried out.

2.9.2 The traditional approach discussed in paragraph 2.3.8 describes what is known as a safety investigation for "funereal" purposes:

- To put losses behind
- To reassert trust and faith in the system
- To resume normal activities
- To fulfil political purposes

2.9.3 The concept of occurrence causation described in Section 2.4, and the notion of the organizational accident discussed in Section 2.5, are linked to what is known as safety investigation for improved system reliability:

- To learn about system vulnerability
- To develop strategies for change
- To prioritize investment of safety resources

2.9.4 In closing this chapter, one example of each approach to safety investigation is schematically presented. Both examples relate to the investigation of accidents.

### Safety investigation for funereal purposes

2.9.5 **The facts**

- An old generation four engine turboprop freighter with a flight crew of two as sole occupants flies into severe icing conditions during a night time domestic flight;
- As a consequence of the ice accretion, engines 2 and 3 flameout, and seven minutes later engine 4 fails. The flight crew manages to re-start engine number 2;
- The aircraft is now in a condition of considerable asymmetrical power, with both engines on the left side delivering power and the two engines on the right side unserviceable. The flight crew experiences serious difficulty in controlling the aircraft;
- Because of the high demand on the aircraft's remaining sources of electrical power, electrical load shedding is not possible, and the electrical system reverts to battery power. The flight crew is left with limited emergency instrumentation to maintain control of the aircraft, limited radio communications and limited navigational capabilities;
- While attempting to conduct an emergency landing battery power is depleted, all electrical power is lost;
- All that is left to the flight crew is the self-powered standby gyro, a flashlight and the self-powered engine instruments;
- The flight crew is unable to maintain controlled flight, and the aircraft crashes out of control.

2.9.6 **Findings of the safety investigation**

- The flight crew did not use the weather radar to avoid the icing conditions;
- The flight crew did not consult the emergency check-list to resolve the power plant and electrical system malfunctions;
- The flight crew was faced with a demanding situation requiring decisive thinking and clear action;
- The aircraft was flown into icing conditions which exceeded certification conditions for the engines;
- The flight crew did not request diversion to a closer aerodrome;
- The flight crew did not use correct phraseology to declare an emergency;
- The flight crew practised poor crew resource management (CRM);
- There was mismanagement of aircraft systems;
- The presentation and visual information of the emergency checklist was poor; and

- There were issues regarding flight operations internal quality assurance procedures.

2.9.7 **Causes**

- Multiple engine failures;
- Incomplete performance of emergency drills;
- Flight crew actions in securing and re-starting engines;
- Drag from un-feathered propellers;
- Weight of ice;
- Poor CRM;
- Lack of contingency plans; and
- Loss of situational awareness.

2.9.8 **Safety recommendations**

- Authority should remind pilots to use correct phraseology.
- Authority should research into most effective form of presentation of emergency reference material.

**Safety investigation for improved system reliability**

2.9.9 **The facts**

- An old generation two engine turboprop commuter aircraft engaged in a regular passenger transport operation is conducting a non-precision approach in marginal weather conditions in an uncontrolled, non-radar, remote airfield;
- The flight crew conducts a straight-in approach, instead of following the full published approach procedure;
- Upon reaching MDA, the flight crew does not acquire visual references;
- The flight crew abandons MDA without having acquired visual references to pursue the landing; and
- The aircraft crashes into terrain short of the runway.

2.9.10 **Findings** of the safety investigation

- [The flight crew committed numerous errors and violations];

***but***

- The flight crew composition, while legal, was unfavourable in view of the demanding flight conditions;
- According to company practice, the flight crew pilot made a straight-in, direct approach, which was against regulations;
- There was a lack of standards for commuter operations in the State;
- There was a lack of supervision of air traffic facilities by the State;
- The authorities had exhibited disregard of previous safety violations by the operator;
- The State's legislation was out of date;
- There were conflicting goals within the authority regarding facilitating industry development against safety oversight needs;
- There was a lack of resources within the authority to fulfil its responsibilities;
- There was a lack of a State aviation policy to support the authority; and

- There were deficiencies in the State's training system.

2.9.11 **Causes**

- The flight crew decision to continue approach below MDA without visual contact;
- The decision was influenced by performance pressures; and
- The decision was influenced by the airline's poor culture.

2.9.12 **Safety recommendations**

- [The report includes numerous "tip-of-the-arrow" oriented recommendations, regarding flight crew performance];

***but also with regard to***

- Reviewing the process of granting AOC by the authority;
- Reviewing the State's training system;
- The definition of an aviation policy which provides support to the task of the aviation administration;
- Reforming existing aviation legislation;
- Reinforcing existing legislation as an interim measure; and
- Improving both accident investigation and aircraft and airways inspection processes.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Chapter 3

# INTRODUCTION TO SAFETY MANAGEMENT

## 3.1 OBJECTIVE AND CONTENTS

3.1.1 This chapter discusses the need for, and the strategies and key features of safety management. The chapter addresses the differences between the management of safety as an organizational process and the prevention of accidents as a remedial activity. The chapter includes the following:

3.1.2 The chapter includes the following:

- The safety stereotype
- The management dilemma
- The need for safety management
- Strategies for safety management
- The imperative of change
- Safety management – Eight building blocks
- Four responsibilities for managing safety

## 3.2 THE SAFETY STEREOTYPE

3.2.1 A misperception has been pervasive in aviation regarding where safety fits in terms of priority within the spectrum of objectives that aviation organizations pursue, regardless of the nature of the services that aviation organizations might deliver. This misperception has evolved into a universally accepted stereotype: in aviation, safety is the first priority. While socially, ethically and morally impeccable because of its inherent recognition of the supreme value of human life, the stereotype and the perspective that it conveys does not hold ground when considered from the perspective that the management of safety as an organizational process.

3.2.2 All aviation organizations, regardless of their nature, have a business component, to a greater or lesser degree. Thus, all aviations organizations can be considered business organizations. A simple question is then relevant to shed light on the truthfulness, or lack thereof, of the safety stereotype: what is the fundamental objective of a business organization? The answer to this question is obvious: to deliver the service for which the organization was created in the first place, to achieve production objectives and eventually deliver dividends to stakeholders.

3.2.3 There is no aviation organization that has been created to deliver *only* safety. Even organizations that act as guardians of aviation safety are subject to efficiency constraints, internal or external, as dictated by their stakeholders. This includes the International Civil Aviation Organization, national and supra national civil aviation authorities, international trade organizations and safety advocate international organizations.

3.2.4 Chapter 2 discusses that safety is increasingly viewed as the consequence of the management of certain organizational processes, with the final objective of keeping the safety risks of the consequences of hazards in operational contexts under organizational control. The management of specific organizational processes, most business related, is a necessary condition to enable organizations to achieve their production objectives through the delivery of services. These organizational processes, including communication, allocation of resources, planning, supervision, and so forth, were also discussed in Chapter 2. The management of these processes is delivered through core business functions and management systems, such as financial management, human resources management, legal management and similar. The perspective advanced by this Manual is that safety is not the first priority of aviation organization. Rather, the management of safety is just another organizational process that allows aviation organizations to achieve their business objectives through the delivery of their services. Safety management is therefore just another core business function that must be considered at the same level and with the same importance of other core business functions, and it is delivered through a dedicated management system (safety management system or SMS, discussed in Chapter 7).

## 3.3 THE MANAGEMENT DILEMMA

3.3.1 The perspective of the management of safety as an organizational process and of safety management as a core business function clearly places ultimate safety accountability and responsibility for such function at the highest level of aviation organizations (without denying the importance of individual safety responsibility for the delivery of services). Nowhere are such accountability and responsibility more evident than in decisions regarding allocation of resources.

3.3.2 The resources available to aviation organizations are finite. There is no aviation organization with infinite resources. Resources are essential to conduct the core business functions of an organization that directly and indirectly support delivery of services. Resource allocation therefore becomes one of the most important, if not *the* most important, of the organizational processes that senior management must account for.

3.3.3 Unless the perspective of safety management as core business function is adhered to by the organization, there is the potential for a damaging competition in the allocation of resources to conduct the core business functions that directly and indirectly support delivery of services. Such competition may lead to a management dilemma that has been dubbed the "dilemma of the two Ps".

3.3.4 Simply put, the "dilemma of the two Ps" can be characterised as the conflict that would develop at the senior management level of the organization because of the perception that resources must be allocated on an *either/or* basis to what are believed to be conflicting goals: *production* goals (delivery of services) or *protection* goals (safety).

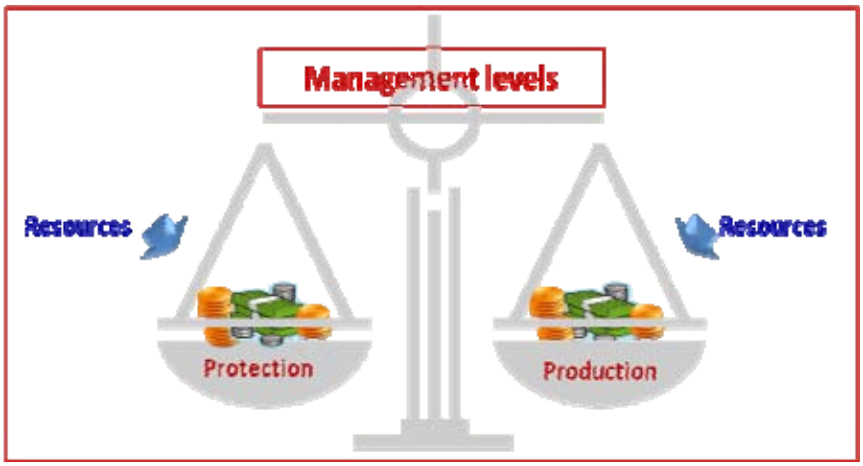



Figure 3-1A – The management dilemma

3.3.5 Figure 3-1A 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 (i.e. just another 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. In this case, the "dilemma of the two Ps" has been effectively dealt with. If fact, it can be argued that in this case the dilemma does not exist.

3.3.6 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 when such competition develops, protection is usually the loser, with organizations privileging (*albeit* introducing numerous caveats to the contrary) production objectives. Inevitably, as shown in Figure 3-1B, such partial organizational decision making leads to a catastrophe. It is simply a matter to time.

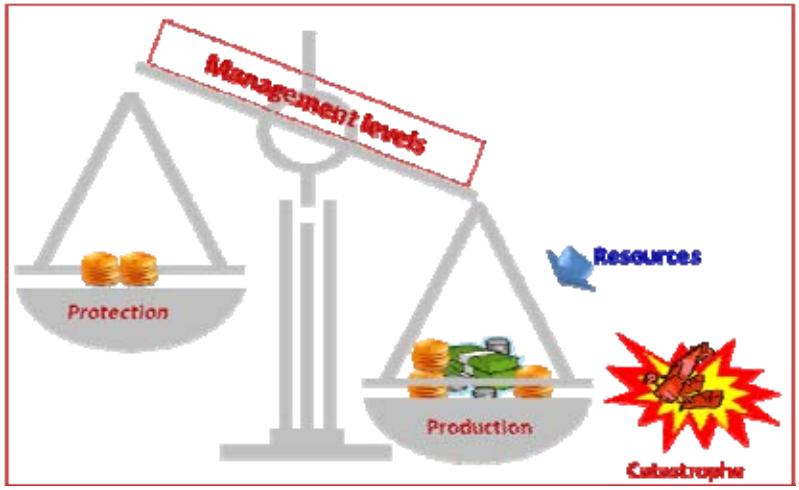



Figure 3-1B – The management dilemma

3.3.7 Figure 3.1C 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 as 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 of other core business processes. In this way, safety management becomes part of the fabric of the organization, and an allocation of resources commensurate to the overall resources available to the organization is ensured.

3.3.8 The rationale for safety management as a core business function can be extended into one final argument that bears considerable relevance to the processes underlying hazard identification and safety risk management as the operational activities and functions involved in safety management (discussed in Chapters 4 and 5).

3.3.9 Since aviation organizations have as primary objective the delivery of services, the timely and efficient delivery of the services may at times come in conflict with operational safety considerations. For example, because of the need of meeting a schedule, an airliner needs to land at a particular airport at a particular time, regardless of weather conditions, traffic volume, airport limitations and similar constraints which are absolutely related to the delivery of the service. If the service delivery efficiency considerations (the need to meet a schedule) were removed, operational safety (adverse weather conditions, high traffic volume, airport limitations) would cease to be a factor. The operation would be conducted only when the constraints disappear. This, however, is impractical, because it would destroy the viability of the aviation industry. Aviation operations must therefore be conducted under conditions that are not dictated not so much by operational safety considerations but rather by service delivery considerations.

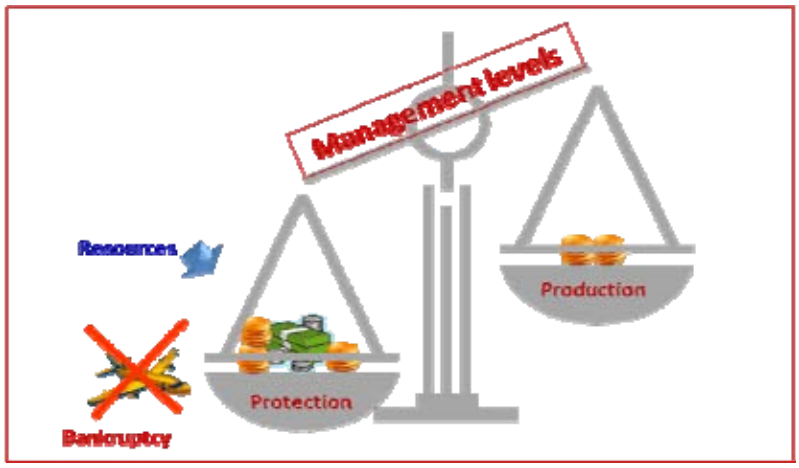



Figure 3-1C – The management dilemma

3.3.10 The corollary is clear: aviation safety issues are neither inherent to nor a natural condition of aviation operations, but a by-product of the need for, and engagement into, activities related to production or delivery of services. This reinforces the need for safety management as core business functions 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.

## 3.4 THE NEED FOR SAFETY MANAGEMENT

3.4.1 Traditionally, the need for safety management has been justified based on a predicted industry growth and the potential for increase in accidents as a consequence of such growth. While accident reduction will always remain a priority of aviation, there are more compelling reasons underlying the transition to a safety management environment in international civil aviation world-wide than statistical projections.

3.4.2 Aviation is arguably the safest mode of mass transportation, and one of the safest socio-technical production systems in the history of humankind. This achievement acquires particular relevance when considering the youth of the aviation industry, which is measured in decades, as compared to other industries the histories of which span through centuries. It is a tribute to the aviation safety community and its unrelenting endeavours that in a mere century aviation has progressed, from the safety perspective, from a fragile system to the first ultra-safe system in the history of transportation. In retrospect, the history of the progress of aviation safety reliability can be divided – just like the evolution of safety thinking discussed in Chapter 2 – in three distinct eras, each with fundamentally differing attributes.

3.4.3 In the first era, which spans from the pioneering days of the early 1900s until approximately the late Sixties (the technical era discussed in Chapter 2), aviation could be characterised as a fragile system from a safety reliability standpoint. Safety breakdowns, although certainly not daily occurrences, were not infrequent. It was then only logical that safety understanding and prevention strategies were mainly derived from accident investigation. There was really no system to speak of, rather the industry functioned because individuals literally threw it upon their shoulders and moved it forward. The safety focus was on individuals and the individual management of safety risks, which in turn built upon the foundations provided by intensive training programmes.

3.4.4 During the second era, from the early Seventies till the mid-Nineties (the human era), aviation became not only a system, but a safe system. The frequency of safety breakdowns diminished significantly, and a more all-encompassing understanding of safety, which went beyond individuals to look into the broader system, was progressively developed. This naturally led to a search for safety lessons beyond those generated by accident investigation, and thus the emphasis shifted towards the investigation of incidents. This shift to a broader perspective of safety and incident investigation was accompanied by the massive introduction of technology as the only way to achieve increased system production demands, and an ensuing, multiple-fold increase in safety regulations.

3.4.5 From the mid-Nineties onwards to the present day (the organizational era), aviation entered its third safety reliability era, becoming an ultra-safe system, (i.e. a system that experiences less than one catastrophic safety breakdown every one million production cycles). From a global perspective and notwithstanding regional spikes, accidents became infrequent to the extent of becoming exceptional events, or anomalies in the system. Serious incidents also became fewer and far apart. In concert with this reduction in occurrences, the shift towards a broad systemic safety perspective that had started to emerge during the previous era consolidated itself. Fundamental in this consolidation was the adoption of a business-like approach to the management of safety, based upon the routine collection and analysis of daily operational data. This business management-like approach to safety underlies the rationale of safety management systems (SMS), discussed in Chapter 7. In the simplest terms, SMS is the application of business management practices to the management of safety. Figure 3-2 illustrates the evolution of safety discussed here above.

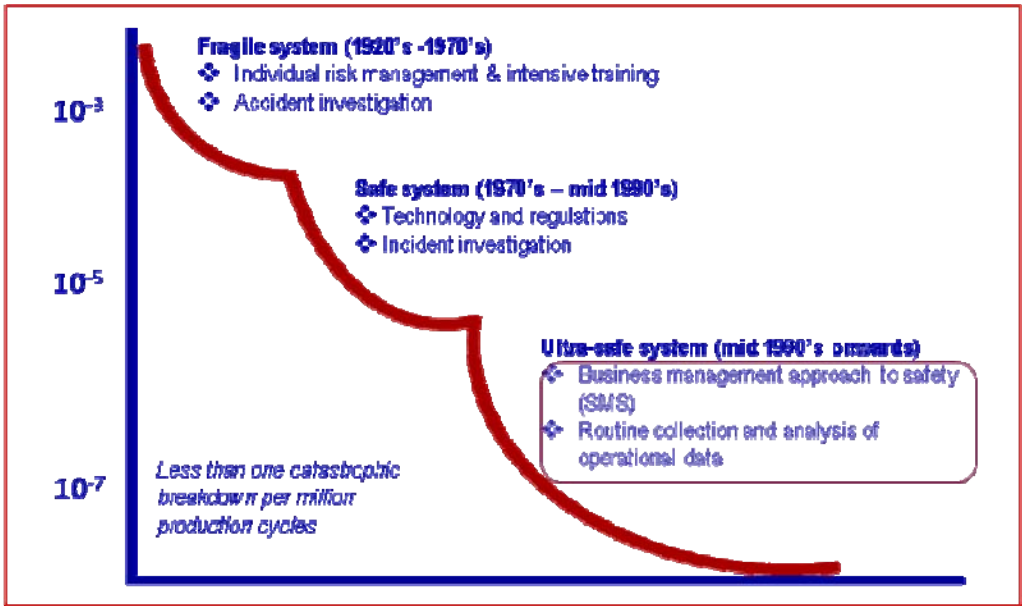



Figure 3-2 – The first ultra-safe industrial system

3.4.6 The application of business management practices to aviation safety with its underlying routine collection and analysis of operational data has as objective the development of the safety space discussed in Chapter 2. Within such safety space, the organization can freely roam while delivering its services, with the assurance that it is within a space of maximum resistance to the safety risks of the consequences of hazards which exist in the context in which it must operate to deliver its services.

3.4.7 The importance of balanced allocation of resources to pursue protection and production goals and thus deny the potential for the development of the "dilemma of the two Ps" has already been discussed. As extension of this previous discussion, the notion of production and protection is relevant to the definition of the boundaries of an organization's safety space as shown in Figure 3-3 below.

3.4.8 It will recalled that organizational decision making leading to excess allocation of resources for protection can have an impact in the financial health of the organization and, in theory at least, could ultimately lead to bankruptcy. It is therefore essential that boundaries be defined; boundaries that if approached by the organization while roaming within the safety space provides early warning that a situation of unbalanced allocation of resources is developing or exists. There are two sides to the safety space, or two boundaries: the financial boundary and the safety boundary.

3.4.9 The "financial boundary" is defined by the financial management of the organization. In order to develop an early warning that alerts that the organization is approaching the financial boundary, financial management does not take into consideration the worst possible outcome (bankruptcy). Financial management practices are based upon taking the daily pulse of specific financial indicators: market trends, changes in prices of commodities and external resources required by the organization to deliver its services, and so forth. Based on this daily collection and analysis of routine financial data, financial management not only defines the financial boundary of the safety space, but also re-adjusts its position constantly.

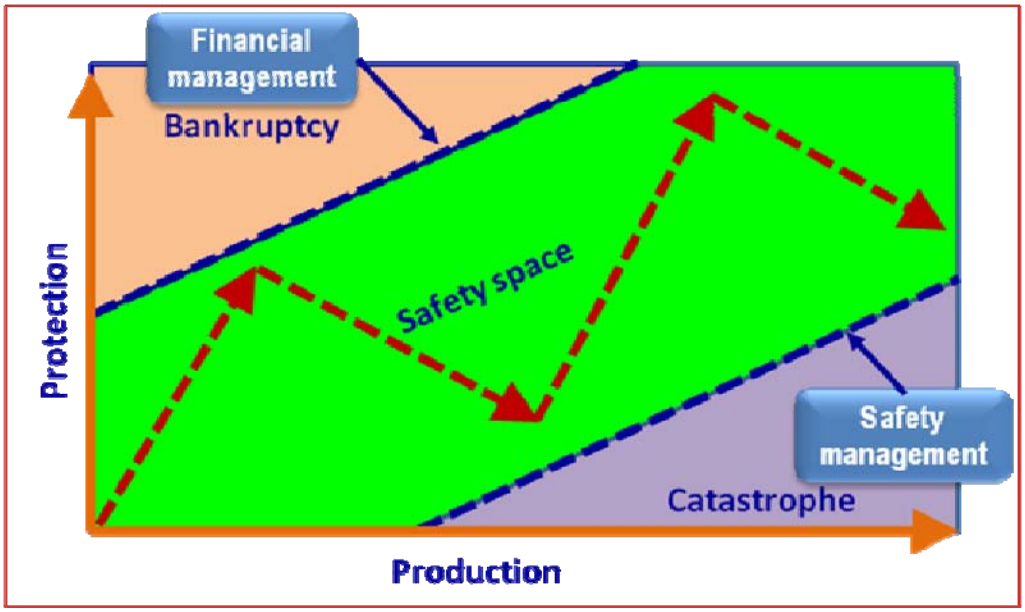



Figure 3-3 – The safety space

3.4.10 It will also be recalled that organizational decision making leading to excess allocation of resources for production can have an impact in the safety health of the organization and could ultimately lead to catastrophe. It is therefore essential that a safety boundary be defined that provides early warning that a situation of unbalanced allocation of resources is developing or exists, in this case regarding protection. The "safety boundary" of the safety space should be defined by the safety management of the organization.

3.4.11 This boundary is essential to alert the organization that an unbalanced allocation of resources that privileges production objectives is developing or exists, that can eventually lead to a catastrophe. Unfortunately, there is no parallel between the practices employed by financial management and safety management. Because of the deeply-ingrained notion of safety as the absence of accidents or serious incidents, the safety boundary of the safety space rarely exists in aviation organizations. In fact, it can be argued that few, if any, aviation organizations, have in fact developed a safety space.

3.4.12 Although early warnings and flags exist, safety-wise, they are for the most part ignored or not acknowledged, and organizations learn that they have misbalanced the allocation of resources when they experience an accident or serious incident. Thus, unlike financial management, under the perspective of safety as the absence of accidents or serious incidents the organization looks for worst case outcomes (or rather their lack thereof), as indication of successful safety management. This approach is not so much safety management as it is damage control. Aviation organizations need to transition to a safety management approach to ensure that the safety boundary is defined, in order to close the loop with the "financial boundary" and thus define the organization's safety space.

3.4.13 The evolution in safety reliability discussed in paragraphs 3.4.3 to 3.4.5 argues about the need to develop additional, alternative means of safety data collection, beyond accident and incident reports. Up to the late-Seventies, safety data collection was mostly effected through accident and incident investigations, and became increasingly scarce as improvements in safety led to a reduction in accident numbers. Furthermore, in terms of safety data acquisition, the accident and serious incident investigation process is reactive: it needs a trigger (a safety breakdown) for the safety data collection process to be launched.

3.4.14 As a consequence of the need to maintain a steady volume of safety data, safety data from accidents and serious incidents was complemented by safety data from expanded collection systems. In the expanded systems, safety data from low-severity events became available through mandatory and voluntary reporting programmes. In terms of safety data acquisition, these newer systems are proactive, since the triggering events required for launching the safety data collection process are of significant lesser consequences than those that trigger the accident and serious incident safety data capture process. The fact nevertheless remains that safety data from reporting programmes only becomes available after safety deficiencies triggers a low consequence event.

3.4.15 By the early Nineties, it became evident that in order to sustain safety in the ultra-safe system, in order to support the business-like approach to safety underlying SMS, larger volumes of safety data, acquired without the need of triggers were required. This led to the development of predictive safety data collection systems, to complement the existing proactive and reactive safety data collections systems. To that end, electronic data acquisition systems and non-jeopardy self-reporting programmes were introduced, to collect safety data from normal operations, without the need of triggering events

to launch the safety data collection process. The latest addition to predictive safety data collection systems are data acquisition systems that are based on direct observation of operational personnel during normal operations.

3.4.16 There is a solid justification for collecting safety data from normal aviation operations. In spite of its safety excellence, the aviation system, just like any other human-made system, is far from perfect. Aviation is an open system; it operates in an uncontrolled natural environment and is subject to environmental disturbances. It is simply impossible to design from scratch an open system that is perfect, if for no other reason because it is impossible to anticipate all possible operational interactions between people, technology and the context in which aviation operations take place. Monitoring normal operational on real time basis allows to iron out flaws and drawbacks that were not anticipated during system design. This argument is further advanced in paragraphs 3.4.17 to 3.4.19 hereunder.

### The practical drift

3.4.17 During the early stages of system design, two questions are topmost in the mind of system designers: bearing in mind the declared production goals of the system, what resources are necessary to achieve such production goals, and how to protect the system from hazards during the operations necessary to achieve the production goals. System designers utilise different methods to answer these questions. One such method is defining plausible scenarios (as many as possible) of operational interactions between people, technology and the operational context, to identify potential hazards in the operational interactions.

3.4.18 The end result of the process is an initial system design based upon three basic assumptions: assumptions about the technology needed to achieve the system production goals, assumptions about the training necessary for people to properly operate the technology, and assumptions about the regulations and procedures that dictate system and people behaviour. These assumptions underlie the baseline (or ideal) system performance. For the purpose of this explanation, ideal or baseline system performance (i.e., how the system *should* perform) can be graphically presented as a straight line (Figure 3-4).

3.4.19 Assumptions are tested, baseline performance validated, and eventually the system becomes operational. Once operationally deployed, the system performs as designed, following baseline performance, most of the times. Oftentimes, nevertheless, operational performance is different from baseline performance. In other words, once systems become operational, a gradual drift from the baseline performance expected according to the system's design assumptions and the system's operational performance gradually but inexorably develops, as consequence of real-life operations. Since the drift is a consequence of daily practice, it is referred to a "practical drift".

3.4.20 A practical drift from baseline performance to operational performance is as expected as unavoidable in any system, no matter how careful and well-thought out its design planning might have been. The reasons for the practical drift are multiple-fold: technology that does not always operate as predicted; procedures that cannot be executed as planned under dynamic operational conditions; regulations that are not quite mindful of contextual limitations; introduction of subtle changes to the system after its design without the corresponding reassessment of their impact in basic design assumptions; addition of new components to the system without an appropriate safety assessment of the hazards such components might introduce; the interaction with other systems; and so forth. Thus, it is a fair statement that, in any system, people deliver the activities aimed at service delivery inside the drift. The fact remains, however, that in spite of all system's shortcomings leading to the drift, people operating inside the practical drift make the system work on a daily basis. People deploy local adaptations and personal strategies (that embody the collective domain expertise of aviation operational professions), thus circumventing system shortcomings. This adaptation process is captured by the vernacular expression "the way we do business here, beyond what the book says".

3.4.21 Formally capturing what takes place within the practical drift through formal means, among others, formally capturing collective domain expertise. This holds considerable learning potential about successful safety adaptations, and therefore for the control of safety risks. The formal capture of this collective domain expertise can be turned into formal interventions for system re-design or improvements, if the learning potential is applied in a principled manner. On the minus side, the unchecked proliferation of local adaptations and personal strategies may allow the practical drift to develop far too much from the expected baseline performance, to the extent that an incident or an accident becomes a possibility. Figure 3-4 illustrates the notion of practical drift discussed in this paragraph.

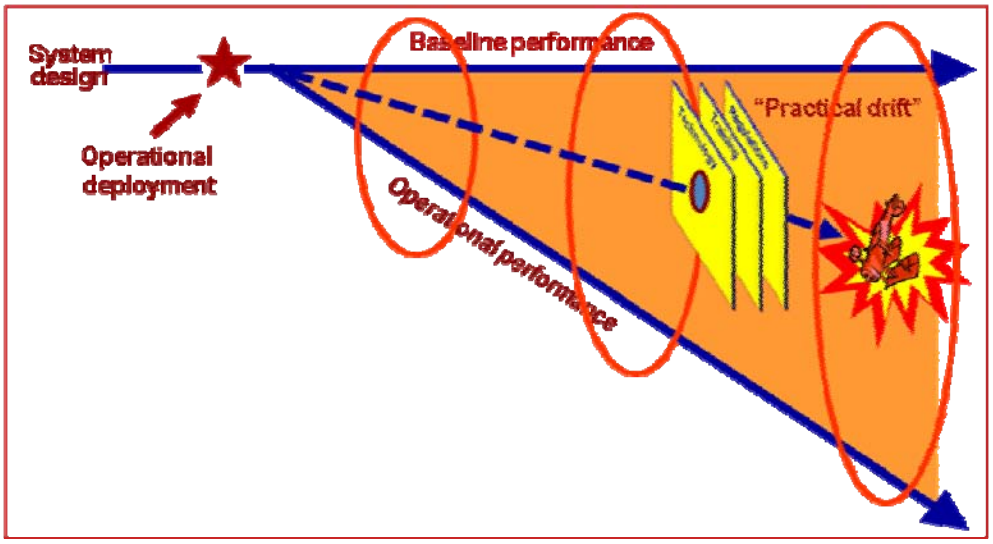



Figure 3-4 – The practical drift

## 3.5 STRATEGIES FOR SAFETY MANAGEMENT

3.5.1 The development of the practical drift is inevitable. All aviation organizations, even the healthiest, most resilient organizations, conduct their daily operations inside the practical drift. The practical drift is simply inherent to the nature of dynamic and open socio-technical production systems, of which aviation is a prime example. On an everyday basis, while pursuing delivery of services, organizations navigate the practical drift, seeking to position themselves as far away as possible from points where the drift is at its maximum, and as closely as possible to the point of inception of the practical drift. During this daily navigation, organizations must overcome potentially confronting "currents" or obstacles: these are the hazards that arise as a consequence of an unbalanced allocation of resources to support the needs of the organization, and the non-resolution of the "dilemma of the two Ps".

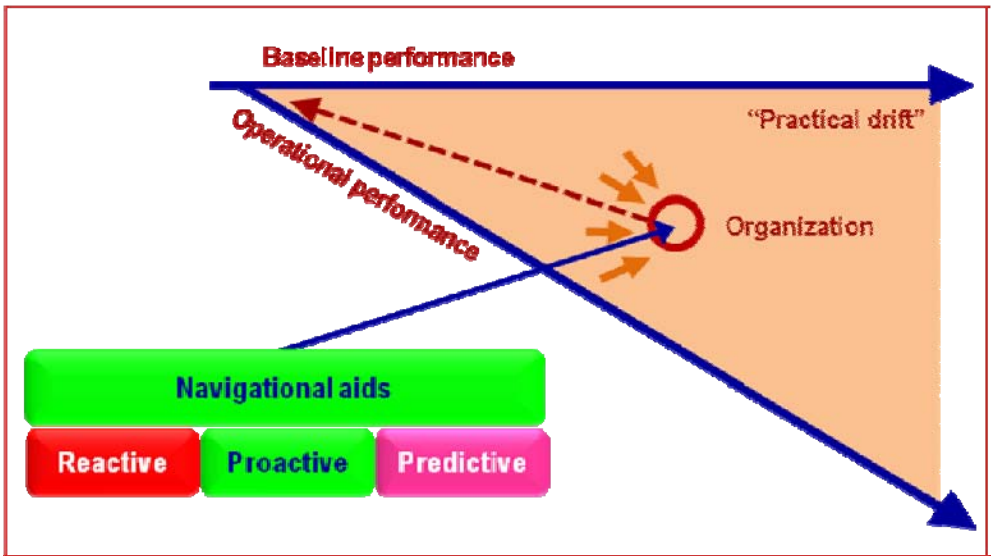



Figure 3-5 – Navigating the practical drift

3.5.2 In order to successfully navigate the practical drift, organizations need navigational aids that generate the necessary information to negotiate currents and obstacles (See Figure 3-5). These navigational aids capture operational data, that once analyzed will inform organizations of the best passages through currents and obstacles. There are a number of navigational aids available to aviation organizations. Such navigational aids can be grouped into three types, according to the seriousness of the consequences of the triggering event that launches the safety data capture process: reactive, proactive and predictive.

3.5.3 Reactive navigational aids require that a very serious triggering event, with oftentimes considerable damaging consequences, take place in order to launch the safety data capture process. Reactive navigational aids are based upon the notion of waiting until "something breaks to fix it". They are most appropriate for situations involving failures in technology and/or unusual events. Reactive navigational aids are integral part of mature safety management. The contribution of reactive navigational aids to safety management nevertheless depends on the extent to which the information they generate goes beyond the triggering cause(s) of the event, and the allocation of blame, and includes contributory factors and findings as to safety risks. The investigation of accidents and serious incidents are examples of reactive navigational aids.

3.5.4 Proactive navigational aids require that a less serious triggering event, probably with little or no damaging consequences, take place in order to launch the safety data capture process. Proactive navigational aids are based upon the notion that system failures can be minimized by identifying safety risks within the system before it fails; and taking the necessary actions to mitigate such safety risks. Mandatory and voluntary reporting systems, safety audits and safety surveys are examples of proactive navigational aids.

3.5.5 Predictive navigational aids do not require that a triggering event take place in order to launch the safety data capture process. Routine operational data is continually captured, in real time. Predictive navigational aids are based upon the notion that safety management is best accomplished by trying to find trouble, not just waiting for it to show up. Therefore, predictive safety data capture systems aggressively seek safety information which may be indicative of emerging safety risks from a variety of sources.

3.5.6 Predictive safety data collection systems are essentially statistical systems, whereby a considerable volume of operational data which, by and in itself is largely meaningless, is collected and analysed, and combined with data from reactive and proactive safety data collection systems. The aggregation of data thus leads to the development of a most complete intelligence that allows organizations to navigate their way around obstacles and currents and position themselves optimally within the drift. Confidential reporting systems, flight data analysis and normal operations monitoring are examples of predictive navigational aids.

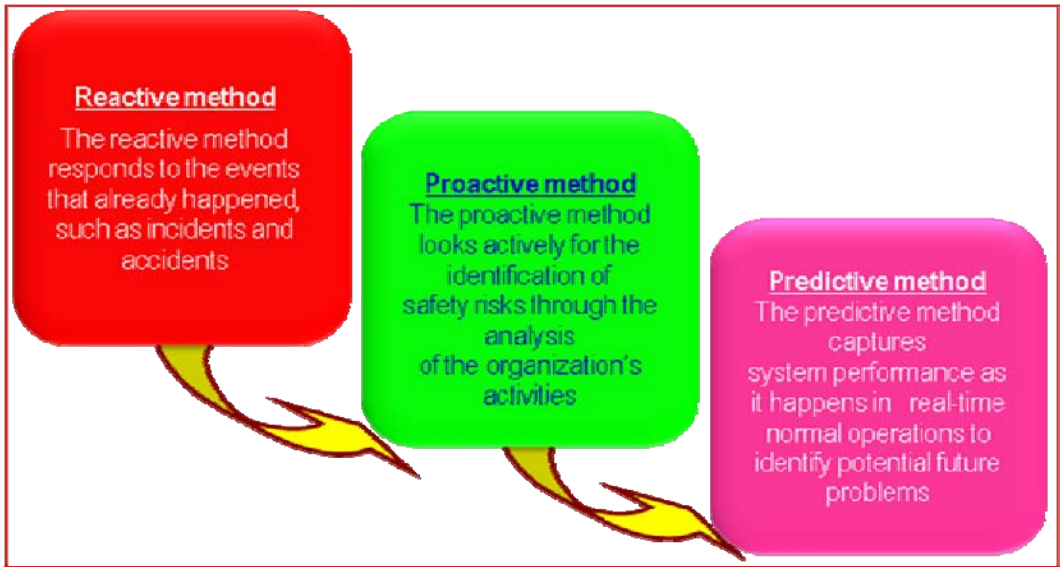



Figure 3-6 – Safety management strategies

3.5.7 Reactive, proactive and predictive safety data capture systems provide safety data for equivalent reactive, proactive and predictive safety management strategies, which in turn inform specific reactive, proactive and predictive mitigation methods. A summary of safety management strategies, as discussed in the previous paragraphs, is presented in Figure 3-6 above.

3.5.8 Mature safety management requires the integration of reactive, proactive and predictive safety data capture systems, a judicious combination of reactive, proactive and predictive mitigation strategies, and the development of reactive, proactive and predictive mitigation methods. Nevertheless, it is important to keep in mind, when developing mitigation strategies, that each of the three safety data capture systems discussed collect safety data at different levels of the operational drift. It is equally important to keep in mind that each of the three mitigation strategies and methods intervene at different levels of the practical drift.

3.5.9 In order to illustrate this, we must return to the practical drift, as pictured in Figure 3-7 hereunder. Hazards exist as a continuum along the practical drift. If uncontained, they travel down the drift, seeking during the voyage for opportunities to unleash their increasing and damaging potential. Close to the point of origin or inception of the practical

drift, hazards are relatively harmless, because they have had no opportunity to develop their damaging potential. The more hazards progress unimpeded in their journey along the practical drift, they more they gather momentum and increase their damaging potential as they track unchecked along the continuum. As hazards approach the point where the practical drift is widest, they have developed maximum potential for damage, including the potential for serious breakdowns. It is therefore essential for safety management to capture hazards as close as possible to the point of inception of the practical drift.

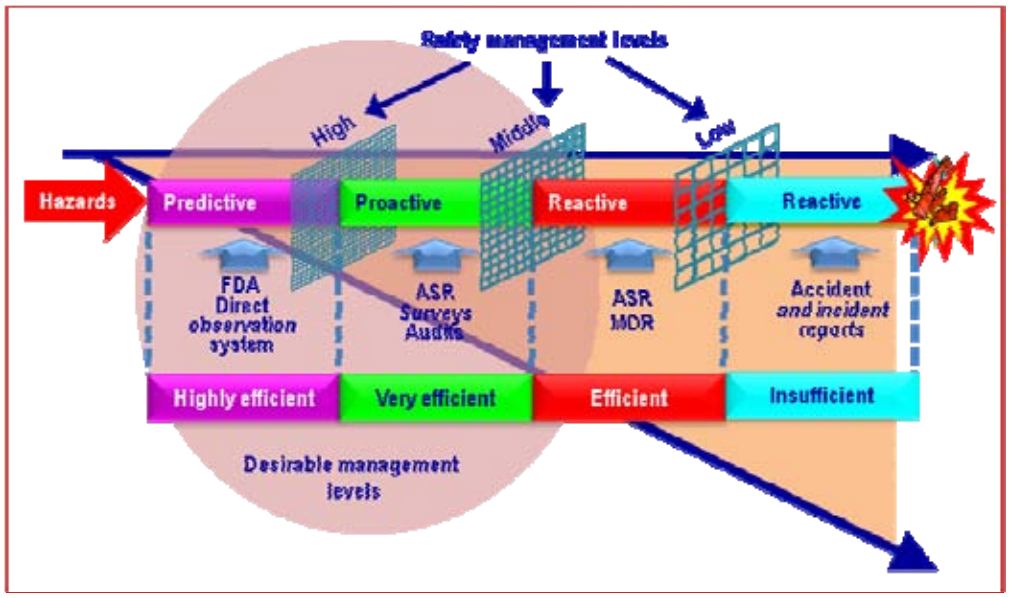



Figure 3-7 – Strategies – Levels of intervention and tools

3.5.10 Predictive safety data capture systems, strategies and methods operate quite close to the origin or point of inception of the practical drift. This is a very high level of intervention, and a highly efficient one. The reason for the high efficiency of predictive safety data capture systems, strategies and methods is two-fold: on one hand, they deal with hazards when hazards are in their infancy, when hazards have had no opportunity to start developing their damaging potential, and are therefore easier to contain. Because of this, the mitigations developed from predictive safety data turn into contention nets or filters of such tightness that almost totally block the passage of emerging hazards further down the continuum of the practical drift.

3.5.11 Proactive safety data capture systems, strategies and methods also operate upstream the practical drift and the hazard continuum, but not as close to the origin or point of inception of the practical drift as predictive safety data capture systems strategies and methods. This is also a high level of intervention, and a very efficient one. Nevertheless, hazards have had opportunity to start developing their damaging potential. Because of this, the mitigations developed from proactive safety data turn into contention nets or filters that are tight, yet they allow passage of developing hazards down the continuum.

3.5.12 Reactive safety data capture systems, strategies and methods operate at two levels of the practical drift. Some, such a mandatory occurrence reporting systems, operate at a middle level of intervention. This is an efficient level, but hazards have continued to grow in damaging potential. The mitigations developed from this first level of reactive safety data thus turn into contention nets of filters with loose texture, which can be frequently penetrated by hazards. At the lowest level of reactive safety data capture systems, strategies and methods, accident and serious incident investigation operate in a damage repair mode. The information developed from purely reactive safety data is insufficient for safety management.

## 3.6 THE IMPERATIVE OF CHANGE

3.6.1 As global aviation activity and complexity continues to grow, deeply changed operational contexts with their new challenges turn traditional methods for managing safety to an acceptable level less effective and efficient. Different, evolving methods for understanding and managing safety are necessary. There is a transition currently taking place in international civil aviation, which reflects a significant shift from the paradigm espoused by safety endeavours in the past.

3.6.2 As already discussed, the traditional safety paradigm was based in the accident/serious incident investigation process as its main safety intervention and method, and it was built upon three basic assumptions:

- The aviation system performs most of the time as per design specifications (i.e. base line performance);
- Regulatory compliance guarantees system baseline performance and therefore ensures safety (compliance based); and
- Because regulatory compliance guarantees system base line performance, minor, largely inconsequential deviations during routine operations (i.e. processes) do not matter, only major deviations leading to bad consequences (i.e. outcomes) do matter (outcome oriented).

3.6.3 A contrasting, contemporary safety paradigm is evolving. This evolving paradigm is the one favoured by this Manual. It is based on the notion of managing safety through process control, beyond the investigation of occurrences, and it builds upon three basic assumptions also:

- The aviation system does not perform most of the time as per design specifications (i.e. operational performance leads to the practical drift);
- Rather than relying in regulatory compliance exclusively, real-time performance of the system is constantly monitored (performance based); and
- Minor, inconsequential deviations during routine operations are constantly tracked and analysed (process oriented).

## 3.7 SAFETY MANAGEMENT – EIGHT BUILDING BLOCKS

3.7.1 Eight basic and generic building blocks underlie the process of managing safety, as follows.

- **Senior management's commitment to the management of safety**. Managing safety, just like any other management activity, requires allocation of resources. This allocation of resources is, in all organizations, a function of senior management, hence the need for senior management's commitment to the management of safety. In plain language: no money, no safety.
- **Effective safety reporting**. It is a known aphorism that "one cannot manage what one cannot measure". In order to manage safety, organizations need to acquire safety data on hazards that allows for measurement to take place. Most of such data will be acquired through voluntary and self-reporting by operational personnel. It is essential therefore for organizations to develop working environments where effective safety reporting by operational personnel takes place.
- **Continuous monitoring** through systems that collect safety data on hazards during normal operations. However, safety data collection is just the first step. Beyond collection, organizations must analyse and extract safety information and safety intelligence from data, because data that is collected and locked in a drawer is as good a no data at all. Furthermore, it is essential to share the safety information and intelligence gleaned with those who operate the system daily, for it is them who are in constant contact with the hazards the consequences of which effective safety reporting aims to mitigate.
- **Investigation of safety occurrences** with the objective of identifying systemic safety deficiencies rather than assigning blame. It is not as important to identify "who did it" as it is to learn "why it happened". System resilience can be much more effectively reinforced by removing systemic deficiencies than by removing supposedly "unfit" individuals.
- **Sharing safety lessons learned and best practices** through the active exchange of safety information. Another well-known aphorism eloquently illustrates the need for data sharing and exchange of safety information: "learn from the mistakes of others, you are not going to live long enough to make them all yourself". The aviation industry's excellent tradition of safety data sharing must be maintained and if at all possible reinforced.
- **Integration of safety training for operational personnel**. Seldom training curricula for operational personnel include dedicated safety training. There is an assumption that since "safety is everybody's responsibility", operational personnel are safety experts in their own right. The fallacy of this line of

reasoning is evident, and discussed in Chapter 7. There is an urgent need to include dedicated training addressing the basics of safety management at all levels of operational personnel training.

- **Effective implementation of Standard Operating Procedures (SOPs)**, including the use of checklists and briefings. SOPs, checklist and briefings, whether in a flight deck, an air traffic control room, a maintenance shop or an aerodrome apron, are amongst the most effective safety devices operational personnel has to discharge their daily responsibilities. They are a powerful mandate from the organization, regarding how senior management wants operations to be conducted. The safety value of realistic, properly written and constantly adhered to SOPs, checklist and briefings should never be underestimated.

- **Continuous improvement of the overall level of safety**. Managing safety is not a one-day affair. The war for safety management is not a conventional warfare, where the front lines are well defined, known to everybody, and one major battle will decide the outcome of the war. The war for safety management, managing safety, is akin to guerrilla warfare: the front lines are not clear, the enemy is not always visible, and gains are measured by inches. It is an on-going activity that can only be successful through continuous improvement.

3.7.2 The results of implementing these eight building blocks will be an organizational culture that fosters safe practices, encourages effective safety communication, and actively manages safety.

## 3.8 FOUR RESPONSIBILITIES FOR MANAGING SAFETY

3.8.1 The responsibilities for managing safety can be grouped into four generic and basic areas, as follows:

- **Definition of policies and procedures regarding safety**. Policies and procedures are organizational mandates reflecting how senior management wants operations to be conducted. A clear definition of policies and procedures is therefore essential to provide operational personnel clear guidance on the operational behaviours the organization expects from operational personnel in day-to-day operations.

- **Allocation of resources for safety management activities**. Managing safety requires resources. The allocation of resources is a managerial function. Management has the authority and therefore the responsibility for the allocation of resources to mitigate the safety risks of the consequences of hazards that threaten the capabilities of the organization.

- **Adoption of best industry practices**. The tradition of aviation regarding safety excellence has already been discussed. This leads to the continuous development of robust safety practices. Aviation has in addition a tradition regarding safety information exchange through both institutional and informal channels. These two positive traits of international civil aviation should be reinforced and practised to foster adoption of best industry practices.

- **Incorporating regulations governing civil aviation safety.** There might be a misperception that safety management will make prevailing regulatory frameworks redundant or unnecessary. This is a misperception that must be dispelled in the strongest terms. There will always be need of a regulatory framework as the bedrock in which safety management endeavours will find their foundation. In fact, sensible safety management can only develop from sensible regulations.

3.8.2 In summary, safety management

- Includes the entire operation;
- It focuses on processes, making a clear differentiation between processes and outcomes;
- It is data-driven;
- It involves constant monitoring;
- It is strictly documented;
- It aims at gradual improvement as opposed to dramatic change; and
- It is based in strategic planning as opposed to piecemeal initiatives.

- - - - - - - - - - - - - - -

# Chapter 4

# HAZARDS

## 4.1 OBJECTIVE AND CONTENTS

4.1.1 The chapter presents the fundamentals of hazard identification and analysis. The chapter includes the following:

- Hazards and consequences
- First fundamental – Understanding hazards
- Second fundamental – Hazard identification
- Third fundamental – Hazard analysis
- Fourth fundamental – Documentation of hazards

## 4.2 HAZARDS AND CONSEQUENCES

4.2.1 Hazard identification and safety risk management are the core processes involved in the management of safety. They are neither new, nor have they been developed as a consequence of recent interest in safety management and, in particular, Safety Management Systems (SMS). Hazard identification and safety risk management are dogmatic components that underlie the overarching concept of system safety. This is an all-encompassing, engineering-based approach that contributes to system design, and which was developed more that forty years ago. The difference between traditional system safety and present-day safety management is that, because of its engineering roots, system safety focussed mostly on the safety implications of technical aspects and components of the system under consideration, somewhat to the expense of the human component. Safety management, on the other hand, builds upon the dogma of system safety (hazard identification and safety risk management), and expands the field of perspective to include Human Factors and human performance as key safety considerations during system design and operation.

4.2.2 The differentiation between hazards and safety risks is oftentimes a source of difficulty and confusion. In order to develop safety management practices that are relevant and effective, a clear understanding what is a hazard and what is a safety risk is essential. This chapter discusses hazards exclusively, while Chapter 5 discusses safety risks. In discussing hazards, and to assist in the understanding of the difference between hazards and safety risks, the discussion splits the overall concept of hazard into two components: the hazard itself, and its consequences. The clear understanding of the difference between these two components is also paramount for the practice of safety management.

4.2.3 A **hazard** is defined as *a condition or an object with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function*. Systems in which people must actively and closely interact with technology to achieve production goals through delivery of services are known as *socio-technical systems*. All aviation organizations are thus socio-technical systems. Hazards are normal components or elements of socio-technical systems. They are integral to the contexts where delivery of services by socio-technical production systems takes place. In and by themselves, hazards are not “bad things”. Hazards are not necessarily damaging or negative components of a system. It is only when hazards interface with the operations of the system aimed at service delivery that their damaging potential may become of safety concern.

4.2.4 Consider, for example, wind, a normal component of the natural environment. Wind is a hazard: it is a *condition with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.* A fifteen-knot wind, by and in itself, does not necessarily hold potential for damage during aviation operations. In fact, a fifteen-knot wind blowing directly down the runway will contribute to improve an aircraft performance during departure. However, when a fifteen-knot wind blows in a direction ninety degrees across a runway of intended take-off or landing, it becomes a cross-wind. It is only then, when the hazard interfaces with operations in the system (take-off or landing an airplane) aimed at service delivery (the need to transport passengers or cargo to/from the particular aerodrome while meeting a schedule), that its potential for damage becomes a safety concern (a lateral runway excursion because the pilot may not be able to control the airplane as a consequence of the crosswind). This example illustrates the discussion in paragraph 4.2.3: a hazard should not necessarily be considered as a “bad thing”, or something with a negative connotation. Hazards are integral part of operational contexts and their consequences can be addressed, through various mitigation strategies that will be discussed later in this Manual, to contain the hazards’ damaging potential.

4.2.5 A **consequence** is defined as *the potential outcome (or outcomes) of a hazard*. The damaging potential of a hazard materialises through one or many consequences. In the example of the crosswind above, one consequence of the hazard "crosswind" could be "loss of lateral control". A further, more serious consequence could be "runway lateral excursion". An even more serious consequence could be "damage to landing gear". It is important, therefore, to describe all likely consequences of a hazard during hazard analysis, and not only the most obvious or immediate ones.

4.2.6 The discussion on the consequences of hazards brings two important points to bear in mind. First, hazards belong in the present. They are – in most cases – part of the operational context and therefore they are present in the workplace before operational personnel "show up to work". As physical components of the operational context or workplace, most hazards are, and should be, detectable through audits. Consequences, on the other hand, belong in the future. They do not materialise until hazards interact with certain operations of the system aimed at service delivery. It is as a consequence of this interaction that hazards may unleash their damaging potential. This brings about one essential tenet of safety management: mitigation strategies should aim at proactively containing the damaging potential of hazards and not at waiting until the consequences of hazards take place and then reactively address such consequences.

4.2.7 Second, for the purpose of safety management, the consequences of hazards should be described in *operational terms*. Many hazards hold the potential for the ultimate and most extreme consequence: loss of human life. Most hazards hold potential for loss property, ecological damage and similar high-level consequences. However, describing the consequences of hazards in extreme terms makes it difficult to design mitigation strategies, except cancellation of the operation. In order to design mitigation strategies to address the safety concerns underlying the less-than-extreme, lower level operational consequences of the hazard (for example, crosswind), such consequences must be described in operational terms (runway lateral excursion), rather than in extreme terms (loss of life).

4.2.8 Chapter 2 discusses safety as a condition of controlled safety risk. The description of the consequences of hazards that may affect a particular operation is part of the assessment of the safety risks of the consequences of the hazard (discussed in Chapter 5). The assessment of the safety risks of the consequences of hazards allows an organization to make an informed decision whether it can achieve the condition of control of the safety risks, and thus continue the operation. If the consequences of the hazard (crosswind) are described in extreme terms (loss of life) rather than operational terms (runway lateral excursion), the safety risk assessment is largely voided, since the condition of control of safety risks will be unlikely be achieved, unless formidable expenditure is incurred, and the likely mitigation will be cancellation of the operation.

## 4.3 FIRST FUNDAMENTAL – UNDERSTANDING HAZARDS

4.3.1 As already discussed, there exists a tendency to confuse hazards with their consequences. When this confusion takes place, the description of the hazard in operational terms then reflects the consequences rather than the hazard itself. In other words, it is not uncommon to see that hazards are described as their consequence(s).

4.3.2 Stating and naming a hazard as one of its consequences has the potential for not only disguising the true nature and damaging potential of the hazard in question, but it also interferes with the identification of other important consequences of the hazard.

4.3.3 On the other hand, properly stated and named hazards allow identifying the nature and damaging potential of the hazard. Properly stating and naming hazards also allow to correctly infer the sources or mechanisms of the hazard and, most important, to evaluate the loss outcome(s), other than extreme outcomes, which is one the final objectives of safety risk management as discussed in Chapter 5.

4.3.4 A further example is presented to illustrate the difference between hazards and consequences. An aerodrome operates with its signage in state of disrepair. This complicates the task of ground navigation by aerodrome users, both aircraft as ground vehicles. In this case, the correct naming of the hazard could be "unclear aerodrome signage" (i.e. condition with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function). As a result of this hazard, many possible consequences may take place. One consequence (i.e. one potential outcome) of the hazard "unclear aerodrome signage" may be "runway incursion". But there may be other consequences: ground vehicles driving into restricted areas, aircraft taxing into wrong taxiways, collision between aircraft, collision between ground vehicles, collision between aircraft and ground vehicles, and so forth. Thus, naming the hazard as "runway incursion" instead of "unclear aerodrome signage" disguises the nature of the hazard and interferes with the identification of other important consequences. This will likely lead to partial or incomplete mitigation strategies.

4.3.5 Hazards can be grouped in three generic families: natural hazards, technical hazards and economic hazards.

4.3.6 Natural hazards are a consequence of the habitat or environment within which operations related to the provision of services take place. Examples of natural hazards include:

- severe weather or climatic events (E.g.: hurricanes, winter storms, droughts, tornadoes, thunderstorms, lighting, and wind shear);

- adverse weather conditions (E.g.: icing, freezing precipitation, heavy rain, snow, winds, and restrictions to visibility);
- geophysical events (E.g.: earthquakes, volcanoes, tsunamis, floods and landslides);
- geographical conditions (E.g.: adverse terrain or large bodies of water);
- environmental events (E.g.: wildfires, wildlife activity, and insect or pest infestation); and/or
- public health events (E.g.: epidemics of influenza or other diseases).

4.3.7 Technical hazards are a result of energy sources (electricity, fuel, hydraulic pressure, pneumatic pressure and so on) or safety-critical functions (potential for hardware failures, software glitches, warnings and so on) necessary for operations related to the delivery of services. Examples of technical hazards include deficiencies regarding:

- aircraft and aircraft components, systems, subsystems and related equipment;
- an organization's facilities, tools, and related equipment; and/or
- facilities, systems, sub-systems and related equipment that are external to the organization.

4.3.8 Economic hazards are the consequence of the socio-political environment within which operations related to the provision of services take place. Examples of economic hazards include:

- growth;
- recession;
- cost of material or equipment;
- etc.

4.3.9 Safety management activities aimed at controlling safety risks will mostly – but not necessarily exclusively – address technical and natural hazards.

## 4.4 SECOND FUNDAMENTAL – HAZARD IDENTIFICATION

4.4.1 It has already been discussed that hazards are part of the fabric of any socio-technical production system. Therefore, the scope for hazards in aviation is wide. Examples of the scope of factors and processes that should be looked into when engaging in hazard identification include:

a) design factors, including equipment and task design;

b) procedures and operating practices, including their documentation and checklists, and their validation under actual operating conditions;

c) communications, including means, terminology and language;

d) personnel factors, such as company policies for recruitment, training, remuneration and allocation of resources;

e) organizational factors, such as the compatibility of production and safety goals, the allocation of resources, operating pressures and the corporate safety culture;

f) work environment factors, such as ambient noise and vibration, temperature, lighting and the availability of protective equipment and clothing;

g) regulatory oversight factors, including the applicability and enforceability of regulations; the certification of equipment, personnel and procedures; and the adequacy of oversight;

h) defences, including such factors as the provision of adequate detection and warning systems, the error tolerance of equipment and the extent to which the equipment is resilient against errors and failures; and

i) human performance, including medical conditions and physical limitations.

4.4.2 As discussed in Chapter 3, hazards may be identified in the aftermath of actual safety events (accidents or incidents), or they may be identified through proactive and predictive processes aimed at identifying hazards before they

precipitate safety events. There is a variety of sources of hazard identification. Some sources are internal to the organization while other sources are external to the organization.

4.4.3 Examples of the internal sources of hazard identification available to an organization include:

- Flight data analysis
- Company voluntary reporting system
- Safety surveys
- Safety audits
- Normal operations monitoring schemes
- Trend analysis
- Feedback from training
- Investigation and follow-up of reported hazards and incidents

4.4.4 Examples of external sources of hazard identification available to an organization include:

- Accident reports
- State mandatory occurrence reporting system
- State voluntary reporting system
- State oversight audits
- Information exchange systems

4.4.5 The fundamental point in this discussion is that no source or programme entirely replaces others, nor it makes other sources or programmes redundant or unnecessary. Hazard identification conducted under mature safety management practices resorts to a judicious combination of internal and external sources, reactive, proactive and predictive processes, and their underlying programmes.

4.4.6 All personnel within aviation organizations should receive the appropriate safety management training, at a level commensurate to their responsibilities, so that everybody in the organization is prepared and able to identify and report hazards. From this perspective, hazard identification and reporting is everybody's responsibility. However, organizations must have designated personnel with the exclusive charge of hazard identification and analysis. This would normally be the personnel assigned to the safety services office, discussed in Chapter 8. Therefore, broadening the previous perspective, in aviation organizations, hazard identification is everybody's responsibility, but accountability for hazard identification lies with dedicated safety personnel.

4.4.7 How hazards are identified will depend on the resources and constraints in each particular organization. Some organizations will deploy comprehensive, technology-intensive hazard identification programmes. Other organizations will deploy modest hazard identification programmes better suited to their size and the complexity of the operations. Nevertheless, hazard identification, regardless of implementation, complexity and size, must be a formal process, clearly described in the organization safety documentation. *Ad hoc* hazard identification is an unacceptable safety management practice.

4.4.8 Under mature safety management practices, hazard identification is a continuous, ongoing daily activity. It never stops or rests. It is an integral part of the organizational processes aimed at delivering the services that the organization is in business to deliver. Nevertheless, there are three specific conditions under which special attention to hazard identification is warranted. These three conditions should trigger a more in-depth and far-reaching hazard identification process, and include:

- Any time the organization experiences an unexplained increase in safety-related events or regulatory infractions;
- Anytime major operational changes are foreseen, including changes to key personnel or other major equipment or systems; and
- Before and during periods of significant organizational change, including rapid growth or contraction, corporate mergers, acquisitions or downsizing.

## 4.5 THIRD FUNDAMENTAL – HAZARD ANALYSIS

4.5.1 Hazard identification is a wasted exercise unless safety information is extracted from the data collected. The first step in developing safety information is hazard analysis.

4.5.2 Hazard analysis is, in essence, a three-step process:

- First step: identify the **generic hazard** (also known and top level hazard, or TLH). Generic hazard is, in the context of this Manual, used as a term that intends to provide focus and perspective on a safety issue, while also helping to simplify the tracking and classification of many individual hazards flowing from the generic hazard.
- Second step: break down the generic hazard into **specific hazards** or **components** of the generic hazard. Each specific hazard will likely have a different and unique set of causal factors, thus making each specific hazard different and unique in nature.
- Third step: link specific hazards to potentially **specific consequences**, i.e., specific events or outcomes.

4.5.3 An example is provided to illustrate the notions of generic hazard, specific hazard, and consequences. An international airport that handles 100,000 movements per year launches a construction project to extend and repave one of two crossing runways. The following three-step process hazard analysis would apply:

- **Step A** – State the generic hazard (hazard statement or TLH)
  - Airport construction
- **Step B** – Identify specific hazards or components of the generic hazard
  - Construction equipment
  - Closed taxiways
  - Etc.
- **Step C** – Link specific hazards to specific consequence(s)
  - Aircraft colliding with construction equipment (construction equipment)
  - Aircraft taking into wrong taxiway (closed taxiways)
  - Etc.

4.5.4 The runway construction example discussed in the paragraph above can be used to extend the discussion about the "dilemma of the two Ps" in Chapter 3 to hazard analysis: efficient and safe provision of service requires a constant balance between production goals and safety goals. In the case of the runway construction example, there is clearly an efficiency (production) goal: maintaining regular aerodrome operations during a runway construction project. There is an equally clear safety (protection) goal: maintaining existing margins of safety in aerodrome operations during the runway construction project. In conducting the hazard analysis, two basic premises of safety management must be at the forefront of the analyses:

- hazards are potential vulnerabilities inherent in socio-technical production systems. They are a necessary part of the system, as a result of the capabilities they provide or can potentially provide to the system to deliver its services. Aviation workplaces therefore contain hazards which may not be cost-effective to address even when operations must continue; and
- hazard identification is a wasted effort if restricted to the aftermath of rare occurrences where there is serious injury, or significant damage. This is graphically portrayed in Figure 4.1, by connecting hazard identification to the practical drift discussed in Chapter 3.

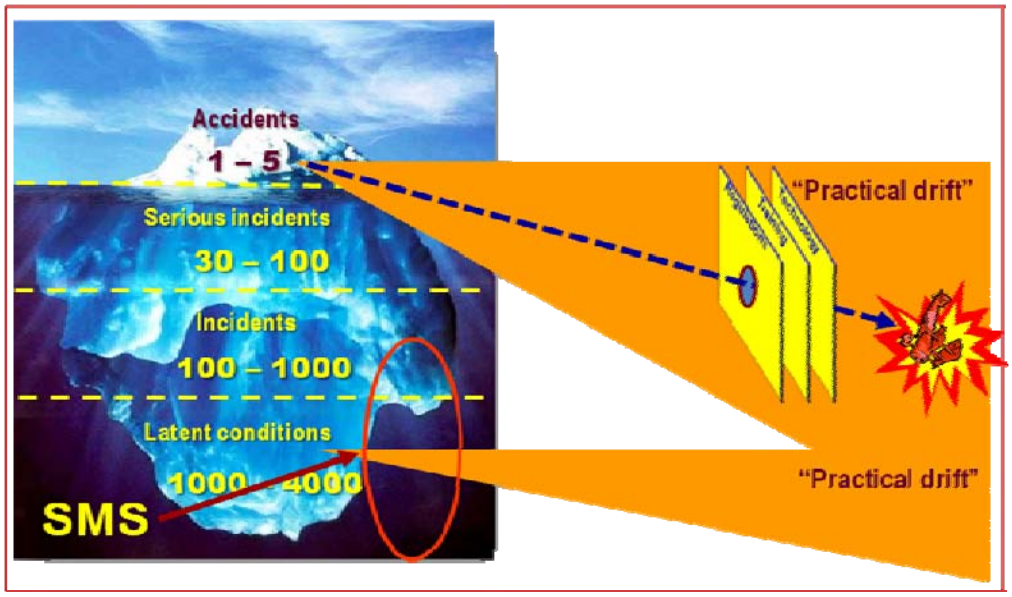



Figure 4-1 — The focus of hazard identification

## 4.6 FOURTH FUNDAMENTAL – DOCUMENTATION OF HAZARDS

4.6.1 Hazards typically perpetuate themselves in a system and deliver their damaging potential mainly because absence or ineffectiveness of hazard identification. Lack of hazard identification is often the result of:

- not thinking about operational conditions with the potential to unleash the damaging potential of hazards;
- not knowing about operational conditions with the potential to unleash the damaging potential of hazards;
- unwillingness to consider or investigate operational conditions with the potential to unleash the damaging potential of hazards; and
- unwillingness to spend money to investigate operational conditions with the potential to unleash the damaging potential of hazards.

4.6.2 Unawareness and unwillingness can only be overcome by knowledge. The formal documentation of hazards is therefore an essential requirement for hazard identification as well as a trait of mature safety management. The safety information (i.e., analysed raw data) and the safety intelligence (i.e., safety information that has been corroborated and further analysed by adding context) combine to generate safety knowledge that must formally reside in the organization, not in the heads of individual members of the organization. A formal repository of safety knowledge is a safeguard against volatility of the information. In addition, an organization that has historical safety knowledge will make safety decisions based upon facts and not opinion.

4.6.3 Appropriate documentation management regarding hazard identification is important as a formal procedure to translate raw operational safety information into hazard-related knowledge. Continuous compilation and formal management of this hazard-related knowledge becomes the "safety library" of an organization. In order to develop knowledge on hazards and thus build the "safety library", it must be remembered that tracking and analysis of hazards is facilitated by standardizing:

- definitions of terms used;
- understanding of terms used;
- validation of safety information collected;
- reporting (i.e., what the organization expects);
- measurement of safety information collected; and

- management of safety information collected.

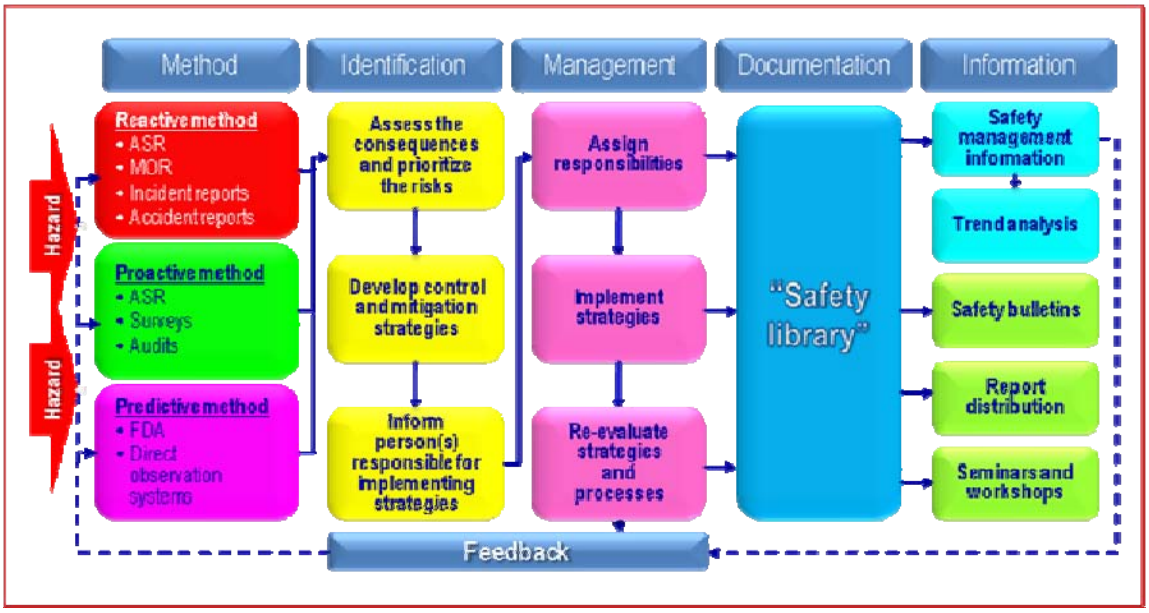



Figure 4-2 — Documentation of hazards

4.6.7 Figure 4-2 illustrates the process of hazard documentation. Hazards are constantly identified through reactive, proactive and predictive sources and underlying methods of safety information collection. Following collection and identification, hazard information is assessed in terms of consequences, and priorities and responsibilities regarding mitigation responses and strategies. All this information, including hazards, consequences, priorities, responsibilities and strategies must be collected into the "safety library" of the organization. The product of the "safety library" is not only the preservation of the corporate safety memory, but the safety library becomes a source of safety knowledge to be used as reference for organizational safety decision-making. The safety knowledge incorporated in the "safety library" provides feedback and control reference against which to measure hazard analysis and consequences management, as well as the efficiency of the sources or methods of safety information collection. It also provides material for safety trend analyses, as well as for safety education purposes (safety bulletins, reports, seminar and the like).

- - - - - - - - - - - -

# Appendix 1 to Chapter 4

# SAFETY INFORMATION ANALYSIS

4.1 After collecting and recording safety information through various sources of hazard identification, meaningful conclusions can only be reached through analysis of the information. Reduction to simple statistics serves little useful purpose without evaluation of the practical significance of the statistics in order to define a problem that can be resolved.

4.2 Having established safety databases and reporting systems, organizations should analyse the information contained in their reports and their databases to determine any safety actions required.

## Safety information analysis — what is it?

4.3 Analysis is the process of organizing facts using specific methods, tools or techniques. Among other purposes, it may be used to:

a) assist in deciding what additional facts are needed;

b) ascertain factors underlying safety deficiencies; and

c) assist in reaching valid conclusions.

4.4 Safety analysis is based on factual information, originating from several sources. Relevant data must be collected, sorted and stored. Analytical methods and tools suitable to the analysis are then selected and applied. Safety analysis is often iterative, requiring multiple cycles. It may be quantitative or qualitative. The absence of quantitative baseline data may force a reliance on more qualitative methods of analysis.

## Objectivity and bias

4.5 Consideration needs to be given to all relevant information; however, not all safety information is reliable. Time constraints do not always permit the collection and evaluation of sufficient information to ensure objectivity. Intuitive conclusions may sometimes be reached which are not consistent with the objectivity required for credible safety analysis.

4.6 Humans are subject to some level of bias in judgement. Past experience will often influence judgement, as well as creativity, in establishing hypotheses. One of the most frequent forms of judgement error is known as “confirmation bias”. This is the tendency to seek and retain information that confirms what we already believe to be true.

## Analytical methods and tools

4.7 There are different methods used in safety analysis; some are automated, some are not. In addition, several software-based tools (requiring different levels of expertise for effective application) exist. Listed below are some analytical methods and tools that are available:

- ***Statistical analysis***. Many of the analytical methods and tools used in safety analysis are based on statistical procedures and concepts, for example, risk analysis utilizes concepts of statistical probability. Statistics play a major role in safety analysis by helping to quantify situations, thereby providing insight through numbers. This generates more credible results for a convincing safety argument.

  The type of safety analysis conducted at the level of an organization safety management activity requires basic skills for analysing numeric data, for identifying trends and for making basic statistical computations such as arithmetic means, percentiles and medians. Statistical methods are also useful for graphical presentations of analyses.

  Computers can handle the manipulation of large volumes of data. Most statistical analysis procedures are available in commercial software packages (E.g. Microsoft Excel). Using such applications, data can be entered directly into a pre-programmed procedure. While a detailed understanding of the statistical theory behind the technique is not necessary, the analyst should understand what the procedure does and what the results are intended to convey.

  While statistics are a powerful tool for safety analysis, they can also be misused and, consequently, can lead to erroneous conclusions. Care must be taken in the selection and use of data in statistical analysis. To ensure appropriate application of the more complex methods, the assistance of specialists in statistical analysis may be required.

- ***Trend analysis***: By monitoring trends in safety data, predictions may be made about future events. Emerging trends may be indicative of embryonic hazards. Statistical methods can be used to assess the significance of perceived trends. The upper and lower limits of acceptable performance against which to compare current performance may be defined. Trend analysis can be used to trigger "alarms" when performance is about to depart from accepted limits.

- ***Normative comparisons***: Sufficient data may not be available to provide a factual basis against which to compare the circumstances of the event or situation under examination with everyday experience. The absence of credible normative data often compromises the utility of safety analyses. In such cases, it may be necessary to sample real world experience under similar operating conditions. Normal operations monitoring programmes provide useful normative data for the analysis of aviation operations.

- ***Simulation and testing***: In some cases, hazards may become evident through testing, for example, laboratory testing may be required for analysing material defects. For suspect operational procedures, simulation in the field under actual operating conditions or in a simulator may be warranted.

- ***Expert panel***: Given the diverse nature of hazards, and the different perspectives possible in evaluating any particular unsafe condition, the views of others, including peers and specialists, should be sought. A multidisciplinary team formed to evaluate evidence of an unsafe condition can also assist in identifying and evaluating the best course for corrective action.

- ***Cost-benefit analysis***: The acceptance of recommended safety risk control measures may be dependent on credible cost-benefit analyses. The costs of implementing the proposed measures are weighed against the expected benefits over time. Sometimes, cost-benefit analysis may suggest that accepting the consequences of the safety risk is preferable to the time, effort and cost necessary to implement corrective action.

- - - - - - - - - - - - - - -

# Appendix 2 to Chapter 4

# MANAGEMENT OF SAFETY INFORMATION

## 4.1 General

4.1.1 Safety data of quality are the lifeblood of safety management. Effective safety management is "data driven". Information collected from operational and maintenance reports, safety reports, audits, evaluations of work practices, etc. generate a lot of data — although not all of it is relevant for safety management. So much safety-related information is collected and stored that there is a risk of overwhelming responsible managers, thereby compromising the utility of the data. Sound management of the organization's databases is fundamental to effective safety management functions (such as trend monitoring, risk assessment, cost-benefit analyses, and occurrence investigations).

4.1.2 The argument necessary for safety change must be based on the analysis of consolidated and safety data. The establishment and maintenance of a safety database provide an essential tool for corporate managers, safety managers and regulatory authorities monitoring system safety issues. Unfortunately, many databases lack the data quality necessary to provide a reliable basis for adjusting safety priorities, evaluating the effectiveness of risk mitigation measures and initiating safety-related research. An understanding of data, databases and the use of appropriate tools is required to reach timely and valid decisions.

4.1.3 Increasingly, computer software is being used to facilitate the recording, storage, analysis and presentation of safety information. It is now possible to easily conduct sophisticated analysis on information in the databases. A wide range of relatively inexpensive electronic databases, capable of supporting the organization's data management requirements, are commercially available for desktop computers. These stand-alone systems have the advantage of not using the organization's main computer system, thus improving the security of the data.

## 4.2 Information system needs

4.2.1 Depending on the size of their organizations, users require a system with a range of capabilities and outputs to manage their safety data. In general, users require:

a) a system with the capability of transforming large amounts of safety data into useful information that supports decision-making;

b) a system that will reduce workload for managers and safety personnel;

c) an automated system that is customizable to their own culture; and

d) a system that can operate at relatively low cost.

## 4.3 Understanding databases

4.3.1 To take advantage of the potential benefits of safety databases, a basic understanding of their operation is required.

### *What is a database?*

Any information that has been grouped together in an organized manner can be considered a database. Paper records can be maintained in a simple filing system (i.e., a manual "database"), but such a system will suffice only for the smallest of operations. Storage, recording, recall and retrieval of data are cumbersome tasks. Safety data of whatever origin should preferably be stored in an electronic database that facilitates the retrieval of this information in a variety of formats.

4.3.2 The capability to manipulate, analyse and retrieve information in a variety of ways is known as database management. Most database management software packages incorporate the following organizational elements for defining a database:

a) *Record*. A grouping of information items that go together as a unit (such as all data concerning one occurrence);

b) *Field*. Each separate information item in a record (such as the date or location of an occurrence); and

c) *File.* A group of records having the same structure and an interrelationship (such as all engine-related occurrences for a specific year).

4.3.3 Databases are considered to be "structured" when each data field has a fixed length and its format type is clearly defined by a number, date, "yes/no" answer, character or text. Often only a fixed choice of values is available to the user. These values are stored in reference files, often referred to as base tables or list value tables, for example, a selection of aircraft make and model from a predetermined list. In order to facilitate quantitative analysis and systematic searches, free-form text entry in structured databases is minimized by confining it to a fixed field length. Often such information is categorized by a system of keywords.

4.3.4 Databases are considered to be "text-based" when information holdings are primarily written documents (for example, accident and incident summaries or written correspondence). The data are indexed and stored in free-form text fields. Some databases contain large amounts of text and structured data; however, modern databases are much more than electronic filing cabinets.

## 4.4 Database limitations

There are limitations to be considered when developing, maintaining or using databases. Some of the limitations relate directly to the database system, while others relate to the usage of the data. If unsupportable conclusions and decisions are to be avoided, database users should understand these limitations. Database users should also know the purpose for which the database was assembled, and the credibility of the information entered by the organization which created and maintains it.

## 4.5 Database integrity

4.5.1 Safety databases are a strategic element of an organization's safety management activities. The data are vulnerable to corruption from many sources, and care must be taken to preserve the integrity of the data. Many employees may have access to the database for inputting data. Others will require access to the data for the performance of their safety duties. Access from multiple sites of a networked system can increase the vulnerability of the database.

4.5.2 The utility of a database will be compromised by inadequate attention to maintaining the data. Missing data, delays in inputting current data, inaccurate data entry, etc. corrupt the database. Even the application of the best analytical tools cannot compensate for bad data.

## 4.6 Database management

### *Protection of safety data*

4.6.1 Given the potential for misuse of safety data that has been compiled strictly for the purpose of advancing aviation safety, database management must begin with protection of the data. Database managers must balance the need for data protection with that of making data accessible to those who can advance aviation safety. Protection considerations include:

a) adequacy of "access to information" laws vis-à-vis safety management requirements;

b) organization policies on the protection of safety data;

c) de-identification, by removing all details that might lead a third party to infer the identity of individuals (for example, flight numbers, dates/times, locations and aircraft type);

d) security of information systems, data storage and communication networks;

e) limiting access to databases to those with a "need to know"; and

f) prohibitions on unauthorized use of data.

## 4.7 Safety database capabilities

The functional properties and attributes of different database management systems vary, and each should be considered before deciding on the most suitable system for an operator's needs. Experience has shown that air safety-related incidents are best recorded and tracked using a PC-based database. The number of features available depends on the type of system selected. Basic features should enable the user to perform such tasks as:

a) log safety events under various categories;

b) link events to related documents (e.g. reports and photographs);

c) monitor trends;

d) compile analyses, charts and reports;

e) check historical records;

f) share data with other organizations;

g) monitor event investigations; and

h) flag overdue action responses.

## 4.8 Database selection considerations

4.8.1 The selection of commercially available database systems will depend upon the user's expectations, the data required, the computer operating system and the complexity of the queries to be handled. A variety of programmes with differing capabilities and skill demands is available. The choice of which type to use requires a balance of the considerations listed below:

a) ***User-friendliness***: The system should be intuitively easy to use. Some programmes provide a wide range of features but require significant training. Unfortunately, there are often trade-offs between the user-friendliness and search power; the more user-friendly the tool, the less likely it will be able to handle complex queries.

b) ***Access***: Although access to all details stored in the database would be ideal, not all users require such access. The structure and complexity of the database will influence the choice of any particular query tools.

c) ***Performance*** is a measure of how efficiently the system operates. It depends on such considerations as:

1) how well the data are captured, maintained and monitored;

2) whether the data is stored in formats that facilitate trend or other analyses;

3) the complexity of the database structure; and

4) the design of the host computer system (or network).

d) ***Flexibility*** is dependent on the system's ability to:

1) process a variety of queries;

2) filter and sort data;

3) use binary logic (i.e., the system can deal with "AND/OR" conditions such as "all pilots who are captains and have 15 000 hours of experience", or "all pilots who are captains or have 15 000 hours of experience");

4) perform basic analysis (counts and cross-tabulations);

5) produce user-defined outputs; and

6) connect with other databases to import or export data.

4.8.2 Costs vary with individual organization requirements. The price charged by some system vendors is a flat fee, which allows multiple users on any one licence. Alternatively, with other system vendors, the rate increases depending on the number of authorized users. The purchaser should take into consideration such associated cost factors as:

a) installation costs;

b) training costs;

c) software upgrade costs;

d) maintenance and support fees; and

e) other software licence fees that may be necessary.

- - - - - - - - - - - - - - -

# Chapter 5

# SAFETY RISKS

## 5.1 OBJECTIVE AND CONTENTS

5.1.1 This chapter presents the fundamentals of safety risk management. The chapter includes the following:

- Definition of safety risk
- First fundamental – Safety risk management
- Second fundamental – Safety risk probability
- Third fundamental – Safety risk severity
- Fourth fundamental - Safety risk tolerability
- Fifth fundamental – Safety risk control/mitigation
- The five fundamentals of safety risk management – Summary

## 5.2 DEFINITION OF SAFETY RISK

5.2.1 Chapter 2 of this Manual defines safety as the outcome of the management of a number of organizational processes. The management of these organizational processes has the objective of keeping safety risks under organizational control. Key in this perspective is the notion of safety as outcome, and safety risk management as process.

5.2.2 Chapter 4 of this Manual further discusses hazard identification as one the two core activities supporting the management of safety. Hazard identification also contributes to the robustness of other organizational processes indirectly related to the management of safety. In order to provide for a proper identification and analysis of hazards, Chapter 4 establishes a clear differentiation between hazards, as sources of potential injury or damage, and their safety consequences described in operational terms.

5.2.3 Safety risk management is the other core activity that supports the management of safety and contributes to other, indirectly related organizational processes. The term safety risk management, as opposed to the more generic term risk management, is meant to convey the notion that the management of safety does not aim – directly – at the management of financial risk, legal risk, economic risk and so forth, but it restricts itself primarily to the management of safety risks.

5.2.4 It is a common pitfall that safety management activities oftentimes do not progress beyond hazard identification and analysis, or in other cases jump from hazard identification direct to mitigation deployment, bypassing the evaluation and prioritization of the safety risks of the consequences of hazards. After all, once sources of danger or harm are identified, and their consequences analysed and agreed, mitigation strategies to protect against the consequences can certainly be deployed. This view would be correct if one were to adhere to the notion of “safety as the first priority”, and focus in the prevention of bad outcomes. However, under the notion of safety management, agreeing on consequences of identified hazards and describing them in operational terms is not enough to engage in mitigation deployment. It is necessary to evaluate the seriousness of consequences, so as to define priorities for the allocation of resources when proposing mitigation strategies.

5.2.5 It has already been proposed that it is a basic management axiom that one cannot manage what one cannot measure. Therefore, it is essential to somehow measure the seriousness of the consequences of hazards. This is the essential contribution of safety risk management to the safety management process. But “putting a number” to the consequences of hazards, the safety management process provides the organization with a principled basis for safety risk decisions and the subsequent allocation of organizational resources to contain the damaging potential of hazards. In this way, safety risk management completes the basic safety management trilogy of hazards-consequences-safety risks, and directly supports the resolution of the “dilemma of the two Ps” discussed in Chapter 3.

5.2.6 Risk, in its vernacular and broadest sense, has been the subject of much discussion and literature on the topic is abundant. A potential for confusion exists, that is partly due to the vernacular use of the term, which is all too-frequent, quite broad and generally vague. The first step in addressing the confusion is narrowing down the use of the generic

term *risk* to the very specific term *safety risk.* Beyond this, it is essential from the outset to establish a clear definition of safety risk, and to link such definition to the concepts of hazard and consequence(s) expressed in operational terms.

5.2.7 Even after narrowing the using of the generic term *risk* down to the more specific term *safety risk*, confusion may still arise. This is because the notion of risk is an artificial one. Safety risks are not tangible or visible components of any physical or natural environment; it is necessary to *think* about safety risks to understand or form an image of them. Hazards and consequences, on the other hand, are tangible or visible components of a physical or natural environment, and therefore intuitive in terms of understanding and visualization. The notion of safety risk is what is known as a *construct*, i.e., it is an artificial convention created by humans. In simple words, while hazards and consequences are physical components of the natural world, safety risks do not really exist in the natural world. Safety risk is a convention product of the human mind intended to measure the seriousness, or "put a number", to the consequences of hazards.

5.2.8 Safety risk is defined as *the assessment, expressed in terms of predicted probability and severity, of the consequence(s) of a hazard taking as reference the worst foreseeable situation*. Typically, safety risks are designated through an alpha-numeric convention that allows for their measurement. Using the example of crosswind discussed in Chapter 4, it can be seen that the proposed definition of safety risk allows to link safety risks with hazards and consequences, thus closing the loop in the hazard-consequence-safety risk trilogy:

- a wind of 15 knots blowing directly across the runway is a *hazard;*
- the potential for a runway lateral excursion, because a pilot might not be able to control the aircraft during takeoff or landing, is one of the *consequences* of the hazard;
- the assessment of the consequences of a runway lateral excursion, expressed in terms of probability and severity as an alpha-numerical convention, is the *safety risk*.

## 5.3 FIRST FUNDAMENTAL – SAFETY RISK MANAGEMENT

5.3.1 Safety risk management is a generic term that encompasses the assessment and mitigation of the safety risks of the consequences of hazards that threaten the capabilities of an organization, to a level as low as reasonably practicable (ALARP). The objective of safety risk management is to provide the foundations for a balanced allocation of resources between all assessed safety risks and those safety risks the control and mitigation of which is viable. In other words, safety risk management assists in resolving the "dilemma of the two Ps". Safety risk management is a therefore key component of the safety management process. Its added value, however, lies in the fact that it is a data-driven approach to resource allocation, thus defensible and easier to explain.

5.3.2 Figure 5-1 depicts a broadly adopted generic visual representation of the safety risk management process. The triangle is presented in inverted position, suggesting that aviation (just like any other socio-technical production system) is "top heavy" from a safety risk perspective: most safety risks of the consequences of hazards will be assessed as initially falling in the intolerable region. A lesser number of safety risks of the consequences of hazards will be assessed in such a way that the assessment falls straight in the tolerable region. An even fewer number of the safety risks of the consequences of hazards will be assessed in such a way that the assessment falls straight in the acceptable region.

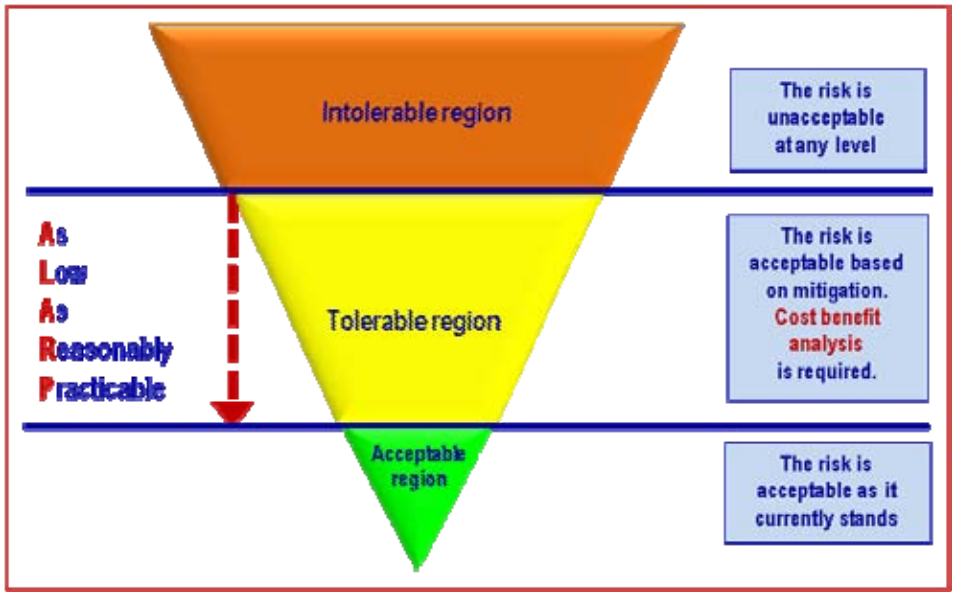



Figure 5-1 – Safety risk management

5.3.3 Safety risks assessed as initially falling in the intolerable region are unacceptable under any circumstances. The probability and/or severity of the consequence(s) of the hazard(s) are of such a magnitude, the damaging potential of the hazard poses such a threat to the viability of the organization, that immediate mitigation action is required. Generally speaking, two alternatives are available to the organization to bring the safety risks to the tolerable or acceptable regions: (1) allocate resources to reduce the exposure to, and/or the magnitude of the damaging potential of the consequence(s) of the hazard(s), or (2) if mitigation is not possible, cancel the operation(s).

5.3.4 Safety risks assessed as initially falling in the tolerable region are acceptable, provided mitigation strategies already in place guarantee that, to the foreseeable extent, the probability and/or severity of the consequence(s) of hazard(s) are kept under organizational control. The same control criteria apply to safety risks initially falling in the intolerable region and mitigated to the tolerable region. A safety risk initially assessed as intolerable that is mitigated and slides down to the tolerable region must remain "protected" by mitigation strategies that guarantee its control. In both cases, a cost-benefit analysis is required: is there a return in the investment underlying the allocation of resources to bring the probability and/or severity of the consequence(s) of hazard(s) under organizational control? Or is the allocation of resources required of such magnitude that will pose a greater threat to the viability of the organization than bringing the probability and/or severity of the consequence(s) of hazard(s) under organizational control?

5.3.5 The acronym ALARP is used to describe a safety risk that has been reduced to a level that is *as low as reasonably practicable*. In determining what is "reasonably practicable" in the context of safety risk management, consideration should be given to both the technical feasibility of further reducing the safety risk, and the cost. This must include a cost-benefit analysis. Showing that the safety risk in a system is ALARP means that any further risk reduction is either impracticable or grossly outweighed by the costs. It should, however, be borne in mind that when an organization "accepts" a safety risk, this does not mean that the safety risk is eliminated. Some residual level of safety risk remains; however, the organization has accepted that the residual safety risk is sufficiently low that it is outweighed by the benefits.

5.3.6 Safety risks assessed as initially falling in the acceptable region are acceptable as they currently stand, and require no action to bring or keep the probability and/or severity of the consequence(s) of hazard(s) under organizational control.

5.3.7 Cost-benefit analyses are at the heart of safety risk management. There are two distinct costs to be considered in cost-benefit analyses: direct costs and indirect costs.

5.3.8 Direct costs are the obvious costs and are fairly easy to determine. They mostly relate to physical damage and include rectifying, replacing or compensating for injuries, equipment aircraft/equipment and property damage. The high costs underlying the loss of organizational control of certain extreme consequences of hazards, such as an accident, can be reduced by insurance coverage. It must be borne in mind, however, that purchasing insurance does nothing to bring the probability and/or severity of the consequence(s) of hazard(s) under organizational control, it only transfers the monetary risk from the organization to the insurer. The safety risk(s) remains unaddressed. Simply buying insurance to transfer monetary risk can hardly be considered a safety management strategy.

5.3.9 Indirect costs include all those costs that are not directly covered by insurance. Indirect costs may amount to more than the direct costs resulting from loss of organizational control of certain extreme consequences of hazards. Such costs are sometimes not obvious and are often delayed. Some examples of uninsured costs that may accrue from loss of organizational control of extreme consequences of hazards include:

a) *Loss of business and damage to the reputation of the organization*. Many organizations will not allow their personnel to fly with an airline with a questionable safety record.

b) *Loss of use of equipment*. This equates to lost revenue. Replacement equipment may have to be purchased or leased. Companies operating a one-of-a-kind aircraft may find that their spares inventory and the people specially trained for such an aircraft become surplus.

c) *Loss of staff productivity*. If people are injured in an occurrence and are unable to work, labour legislation may still require that they continue to receive some form of compensation. Also, these people will need to be replaced at least for the short term, incurring the costs of wages, training, overtime, as well as imposing an increased workload on the experienced workers.

d) *Investigation and clean-up*. These are often uninsured costs. Operators may incur costs from the investigation including the costs of their staff involvement in the investigation, as well as the costs of tests and analyses, wreckage recovery, and restoring the event site.

e) *Insurance deductibles*. The policyholder's obligation to cover the first portion of the cost of any event must be paid. A claim will also put a company into a higher risk category for insurance purposes and therefore may result in increased premiums. (Conversely, the implementation of safety mitigation interventions could help a company to negotiate a lower premium).

f) *Legal action and damage claims*. Legal costs can accrue rapidly. While it is possible to insure for public liability and damages, it is virtually impossible to cover the cost of time lost handling legal action and damage claims.

g) *Fines and citations*. Government authorities may impose fines and citations, including possibly shutting down unsafe operations.

5.3.10 Cost-benefit analyses produce results that can be numerically precise and analytically exact. Nevertheless, there are less exact and numeric factors that weigh in a cost-benefit analysis. These factors include:

a) *Managerial*. Is the safety risk consistent with the organization's safety policy and objectives?

b) *Legal*. Is the safety risk in conformance with current regulatory standards and enforcement capabilities?

c) *Cultural*. How will the organization's personnel and other stakeholders view the safety risk?

d) *Market*. Will the organization's competitiveness and well-being vis-à-vis other organizations be compromised by the safety risk?

e) *Political*. Will there be a political price to pay for not addressing the safety risk?

f) *Public*. How influential will the media or special interest groups be in affecting public opinion regarding the safety risk?

## 5.4 SECOND FUNDAMENTAL – SAFETY RISK PROBABILITY

5.4.1 The process of bringing the safety risks of the consequence(s) of hazards under organizational control starts by assessing the probability that the consequence(s) of the hazard materialise during operations aimed at delivery of services. This is known as assessing the safety risk *probability*.

5.4.2 Safety risk probability is defined as *the likelihood that an unsafe event or condition might occur*. The definition of the likelihood of a probability can be aided by questions such as:

a) Is there a history of similar occurrences to the one under consideration, or is this an isolated occurrence?

b) What other equipment or components of the same type might have similar defects?

c) How many personnel are following, or are subject to, the procedures in question?

d) What percentage of the time is the suspect equipment or the questionable procedure in use?

e) To what extent are there organizational, management or regulatory implications that might reflect larger threats to public safety?

5.4.3 Any or all of the factors underlying these example questions may be valid, underlining the importance of considering multi-causality. In assessing the likelihood of the probability that an unsafe event or condition might occur, all potentially valid perspectives must be evaluated.

5.4.4 In assessing the likelihood of the probability that an unsafe event or condition might occur, reference to historical data contained in the "safety library" of the organization is paramount in order to make informed decisions. It follows that an organization which does not have a "safety library" can only make probability assessments based at best in industry trends, at worst in opinion.

5.4.5 Based on the considerations emerging from the replies to questions such as those listed in paragraph 5.4.2, the likelihood of the probability that an unsafe event or condition might occur can be established, and its significance assessed using a safety risk probability table.

5.4.6 Figure 5-2 presents a typical safety risk probability of occurrences table, in this case, a five-point table. The table includes a qualitative definition of the probability of occurrence of an unsafe event or condition, an explanation of the meaning of each qualitative definition, and an assignment of a number to each definition. It must be stressed that this is an example presented for educational purposes only. Although this table, as well as the severity table and the risk assessment and tolerability matrixes discussed in the following paragraphs are – conceptually speaking – industry standards, the level of detail and complexity of tables and matrixes must be adapted and commensurate to the particular needs and complexities of different organizations. There are organizations that include both qualitative and quantitative definitions. Likewise, some tables extend up to fifteen points. The five-point tables and five-by-five matrixes are by no means a standard. They are just considered of a complexity that is suitable for educational purposes as well as for the needs of the readership of this Manual.

| Probability of occurrence | | |
|---|---|---|
| **Qualitative definition** | **Meaning** | **Value** |
| **Frequent** | Likely to occur many times *(has occurred frequently)* | **5** |
| **Occasional** | Likely to occur some times *(has occurred infrequently)* | **4** |
| **Remote** | Unlikely, but possible to occur *(has occurred rarely)* | **3** |
| **Improbable** | Very unlikely to occur *(not known to have occurred)* | **2** |
| **Extremely improbable** | Almost inconceivable that the event will occur | **1** |

Figure 5-2 – Safety risk probability table

## 5.5 THIRD FUNDAMENTAL – SAFETY RISK SEVERITY

5.5.1 Once the safety risk of an unsafe event or condition has been assessed in terms of probability, the second step in the process of bringing the safety risks of the consequence(s) of hazards under organizational control is the assessment of the severity of the consequence(s) of the hazard if its damaging potential materialise during operations aimed at delivery of services. This is known as assessing the safety risk *severity*.

5.5.2 Safety risk severity is defined as *the possible consequences of an unsafe event or condition, taking as reference the worst foreseeable situation*. The assessment of the severity of the consequence(s) of the hazard if its damaging potential materialises during operations aimed at delivery of services can be assisted by questions such as:

a) How many lives may be lost? (Employees, passengers, bystanders and the general public)

b) What is the likely extent of property or financial damage? (Direct property loss to the operator, damage to aviation infrastructure, third party collateral damage, financial impact and economic impact for the State)

c) What is the likelihood of environmental impact? (Spill of fuel or other hazardous product, and physical disruption of natural habitat)

d) What are the likely political implications and/or media interest?

5.5.3 Based on the considerations emerging from the replies to questions such as those listed in paragraph 5.5.2, the severity of the possible consequences of an unsafe event or condition, taking as reference the worst foreseeable situation, can be assessed using a safety risk severity table.

5.5.4 Figure 5-3 presents a typical safety risk severity table, also a five-point table. It includes an aviation definition for each level of the severity of the occurrence of an unsafe event or condition, an explanation of the meaning of each aviation definition, and the assignment of a letter to each aviation definition. Just like with the safety risk probability table, it must be stressed that this table is an example presented for educational purposes only, and the same caveats expressed in paragraph 5.4.6 apply in this case.

| Severity of occurrences | | |
|---|---|---|
| **Aviation definition** | **Meaning** | **Value** |
| **Catastrophic** | ➢ Equipment destroyed.<br>➢ Multiple deaths. | **A** |
| **Hazardous** | ➢ A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely.<br>➢ Serious injury.<br>➢ Major equipment damage. | **B** |
| **Major** | ➢ A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of increase in workload, or as a result of conditions impairing their efficiency.<br>➢ Serious incident.<br>➢ Injury to persons. | **C** |
| **Minor** | ➢ Nuisance.<br>➢ Operating limitations.<br>➢ Use of emergency procedures.<br>➢ Minor incident. | **D** |
| **Negligible** | ➢ Little consequences | **E** |

Figure 5-3 – Safety risk severity table

## 5.6 FOURTH FUNDAMENTAL – SAFETY RISK TOLERABILITY

5.6.1 Once the safety risk of the consequence(s) an unsafe event or condition has been assessed in terms of probability and severity, the third step in the process of bringing the safety risks of the consequence(s) of the unsafe event or condition under organizational control is the assessment of the tolerability of the consequence(s) of the hazard if its damaging potential materialises during operations aimed at delivery of services. This is known as assessing safety risk *tolerability*. This is a two-step process.

5.6.2 First, it is necessary to obtain an overall assessment of the safety risk. This is achieved by combining the safety risk probability and safety risk severity tables into a safety risk assessment matrix, an example of which is presented in Figure 5-4. For example, a safety risk probability has been assessed as occasional (4). The safety risk severity has been assessed as hazardous (B). The composite of probability and severity (4B) is the *safety risk* of the *consequences* of the *hazard* under consideration. Extending the discussion in paragraph 5.2, it can now be seen, through this example, that a safety risk is just a number or alpha-numerical combination and not a visible or tangible component of the natural world. The colour coding in the matrix in Figure 5-4 reflects the tolerability regions in the inverted triangle in Figure 5-1.

| Risk probability | Risk severity | | | | |
|---|---|---|---|---|---|
| | Catastrophic A | Hazardous B | Major C | Minor D | Negligible E |
| Frequent 5 | 5A | 5B | 5C | 5D | 5E |
| Occasional 4 | 4A | 4B | 4C | 4D | 4E |
| Remote 3 | 3A | 3B | 3C | 3D | 3E |
| Improbable 2 | 2A | 2B | 2C | 2D | 2E |
| Extremely improbable 1 | 1A | 1B | 1C | 1D | 1E |

Figure 5-4 – Safety risk assessment matrix

5.6.3 Second, the safety risk index obtained from the safety risk assessment matrix must then be transported to a safety risk tolerability matrix that describes tolerability criteria. The criterion for a safety risk assessed as 4B is, according to the tolerability table used in the example illustrated in Figure 5-5, "Unacceptable under the existing circumstances". In this case, the safety risk falls in the intolerable region of the inverted triangle. The safety risk of the consequences of the hazard is unacceptable. The organization must (a) allocate resources to reduce the exposure to the consequence(s) of the hazard(s), (b) allocate resources to reduce the magnitude or the damaging potential of the consequence(s) of the hazard(s), or (c) cancel the operation(s) if mitigation is not possible.

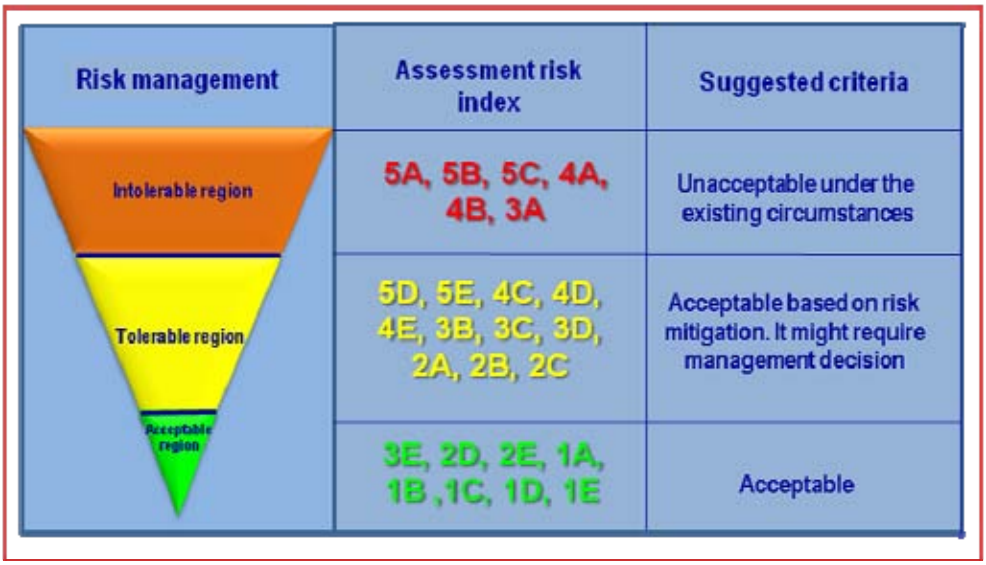



Figure 5-5 – Safety risk tolerability matrix

## 5.7 FIFTH FUNDAMENTAL – SAFETY RISK CONTROL/MITIGATION

5.7.1 In the fourth and final step of the process of bringing the safety risks of the consequence(s) of an unsafe event or condition under organizational control, control/mitigation strategies must be deployed. Generally speaking, control and mitigation are terms that can be used interchangeably. Both are meant to designate measures to address the hazard and bring under organizational control the safety risk probability and severity of the consequences of the hazard.

5.7.2 Continuing with the example presented in paragraph 5.6, the safety risk of the consequences of the hazard under analysis has been assessed as 4B ("unacceptable under the existing circumstances"). Resources must then be allocated to slide it down the triangle, into the tolerable region, where safety risks are ALARP. If this cannot be achieved, then the operation aimed at delivery of the service(s) that exposes the organization to the consequences of the hazard(s) in question must be cancelled. Figure 5-6 presents the process of safety risk management in graphic format.

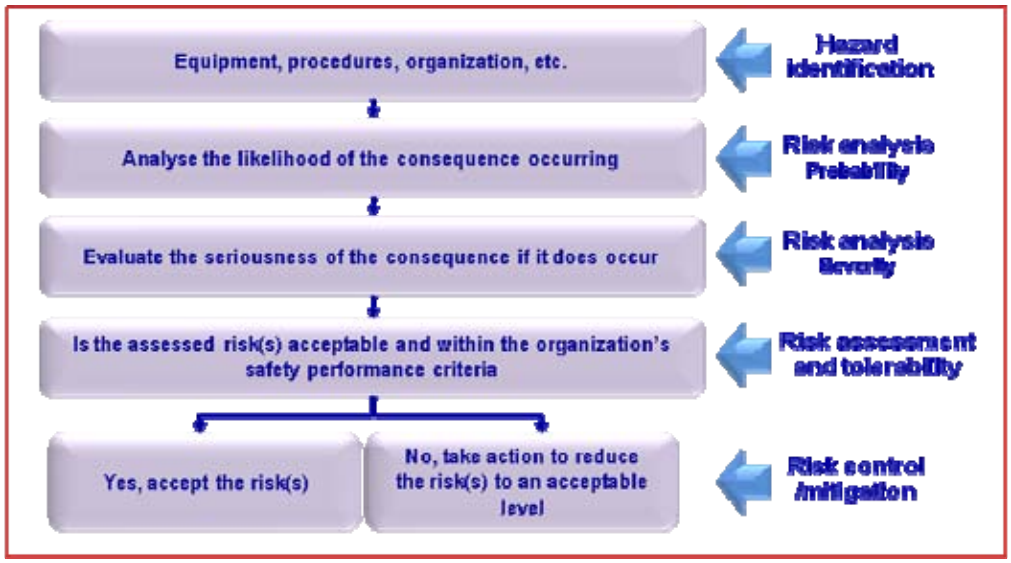



Figure 5-6 – The process of safety risk management

5.7.3 There are three generic strategies for safety risk control/mitigation:

- **Avoidance** – The operation or activity is cancelled because safety risks exceed the benefits of continuing the operation or activity. Examples of avoidance strategies include:
  - *Operations into an aerodrome surrounded by complex geography and without the necessary aids are cancelled.*
  - *Operations in RVSM airspace by non-RVSM equipped aircraft are cancelled.*
- **Reduction** –The frequency of the operation or activity is reduced, or action is taken to reduce the magnitude of the consequences of the accepted risks. Examples of strategies based on reduction of exposition include:
  - *Operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to day-time, visual conditions.*
  - *Operations by non-RVSM equipped aircraft are conducted above or below RVSM airspace.*
- **Segregation of exposure** – Action is taken to isolate the effects of the consequences of the hazard or build-in redundancy to protect against it. Examples of strategies based on segregation of exposure include:
  - *Operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to aircraft with specific/performance navigation capabilities.*
  - *Non RVSM equipped aircraft not allowed to operate into RVSM airspace.*

5.7.4 In evaluating specific alternatives for safety risk mitigation, it must be kept in mind that not all have the same potential for reducing safety risks. The effectiveness of each specific alternative needs to be evaluated before a decision can be taken. It is important that the full range of possible control measures be considered and that trade-offs between measures be considered to find an optimal solution. Each proposed safety risk mitigation option should be examined from such perspectives as:

a) ***Effectiveness***: Will it reduce or eliminate the safety risks of the consequence(s) of the unsafe event or condition? To what extent do alternatives mitigate such safety risks? Effectiveness can be viewed as being somewhere along a continuum, as follows:

1) Engineering mitigations: The mitigation **eliminates** the safety risk of the consequence(s) of the unsafe event or condition, for example, by providing interlocks to prevent thrust reverser activation in flight.

2) Control mitigations: The mitigation accepts the safety risk of the consequence(s) of the unsafe event or condition but adjusts the system to **mitigate such** safety risk by reducing it to a manageable level, for example, by imposing more restrictive operating conditions. Both engineering and control mitigations are considered "hard" mitigations, since they do not rely in flawless human performance.

3) Personnel mitigations: The mitigation accepts that engineering and/or control mitigations are not either efficient or effective, so personnel must be taught how to **cope** with the safety risk of the consequences of the hazard, for example, by adding warnings, revised checklists, SOPs and/or extra training. Personnel mitigations are considered "soft actions", since they rely on flawless human performance.

b) ***Cost/benefit***: Do the perceived benefits of the mitigation outweigh the costs? Will the potential gains be proportional to the impact of the change required?

c) ***Practicality***: Is the mitigation practical and appropriate in terms of available technology, financial feasibility, administrative feasibility, governing legislation and regulations, political will, etc.?

d) ***Challenge***: Can the mitigation withstand critical scrutiny from all stakeholders (employees, managers, stockholders/State administrations, etc.)?

e) ***Acceptability*** to each stakeholder. How much buy-in (or resistance) from stakeholders can be expected? (Discussions with stakeholders during the safety *risk assessment* phase may indicate their preferred risk mitigation option.)

f) ***Enforceability***: If new rules (SOPs, regulations, etc.) are implemented, are they enforceable?

g) ***Durability***: Will the mitigation withstand the test of time? Will it be of temporary benefit or will it have long-term utility?

h) ***Residual safety risks***: After the mitigation is implemented, what will be the residual safety risks relative to the original hazard? What is the ability to mitigate any residual safety risks?

i) ***New problems***: What new problems or new (perhaps worse) safety risks will be introduced by the proposed mitigation?

5.7.5 The most effective mitigations are the hard mitigations. Because hard mitigations are often expensive, organizations frequently resort to soft mitigations (such as training). In such cases, the organization is more often than not relinquishing responsibility for safety risk management to subordinates.

5.7.6 To summarise, safety risk control/mitigation strategies are mostly based on the deployment of additional safety defences, or in the reinforcement of existing ones. Defences were discussed in Chapter 2 and it is recalled that defences in the aviation system can be grouped under three general categories:

a) technology

b) training

c) regulations

5.7.7 As part of the safety risk control/mitigation, it is important to determine why new defences are necessary, or existing ones must be reinforced. The following questions may pertain to such determination:

a) Do defences to protect against the safety risk(s) of the consequences of the hazard(s) exist?

b) Do defences function as intended?

c) Are the defences practical for use under actual working conditions?

d) Is staff involved aware of the safety risk(s) of the consequences of the hazard(s), and the defences in place?

e) Are additional safety risk mitigation/control measures required?

5.7.8 Figure 5-7 presents the full safety risk/mitigation process in graphic format. Hazards are potential safety vulnerabilities inherent to the aviation system. Such vulnerabilities manifest themselves as an array of consequences. In order to manage safety it is necessary to assess the safety risks of the consequences of hazards, by assigning each safety risk an index. Each hazard can generate one or many consequences, and each consequence can be assessed one or many safety risks. The first step in the safety risk mitigation/control process is, therefore, hazard/consequence identification and safety risk assessment.

5.7.9 Once hazards and consequences have been identified and safety risks assessed, the effectiveness and efficiency of existing aviation system defences (technology, training and regulations) relative to the hazards/consequences in question must be evaluated. As a consequence of this evaluation, existing defences will be reinforced, new ones introduced, or both. The second step in the safety risk mitigation/control process is, therefore, evaluation of the effectiveness of the defences within the aviation system.

5.7.10 Based on the reinforcement of existing defences and/or the introduction of new ones, initial safety risks are re-assessed to determine whether they are now ALARP. The third step in the safety risk mitigation/control process is, therefore, control and/or mitigation action.

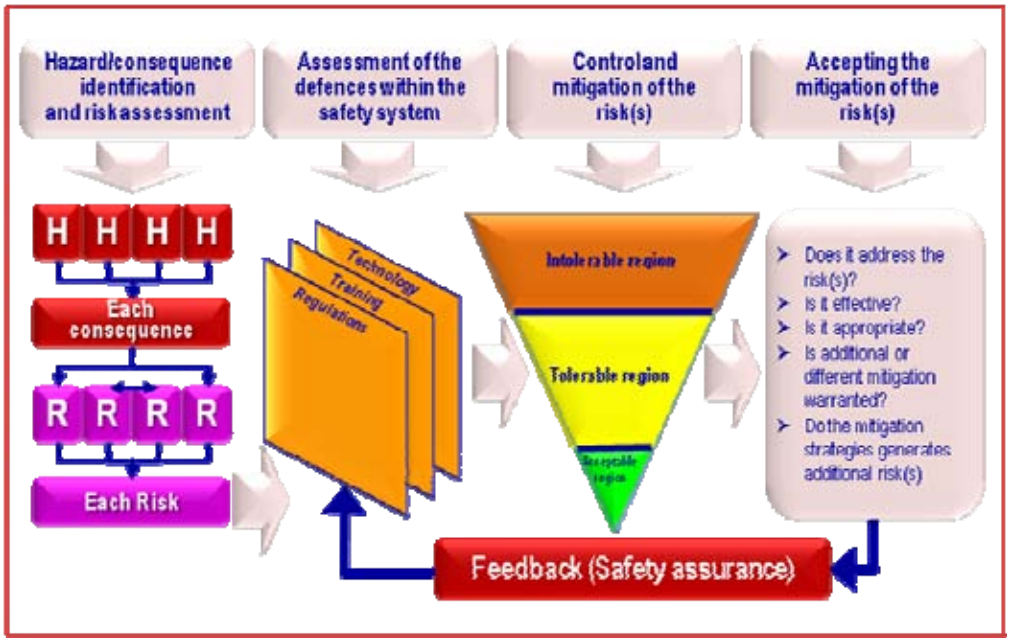



Figure 5-7 – The safety risk mitigation process

5.7.11 Following re-assessment of safety risks, the effectiveness and efficiency of the mitigation/control strategies must be confirmed. The fourth step in the safety risk mitigation/control process is accepting the mitigation of the safety risk. The following questions pertain:

a) Does the mitigation address the safety risk(s)?

b) Is the mitigation effective?

c) Is the mitigation appropriate?

d) Is additional or different mitigation warranted?

e) Do the mitigation strategies generate additional risk(s)?

5.7.12 Once the mitigation is accepted, the strategies developed and deployed must be, as part of the safety assurance process, feedback into the organization's defences upon which the mitigation strategy(ies) is based, to ensure integrity, efficiency and effectiveness of the defences under the new operational conditions.

## 5.8 THE FIVE FUNDAMENTALS OF SAFETY RISK MANAGEMENT – SUMMARY

5.8.1 The significant concepts regarding safety risk management discussed throughout this Chapter can be summarised, in bullet-type format, as follows:

- There is no such thing as absolute safety – In aviation it is not possible to eliminate all safety risks;
- Safety risks must be managed to a level "as low as reasonably practicable" (ALARP);
- Safety risk mitigation must be balanced against:
  - time
  - cost
  - difficulty of taking measures to reduce or eliminate the safety risk (i.e. managed);
- Effective safety risk management seeks to maximize the benefits of accepting a safety risk (most frequently, a reduction in either time and/or cost in the delivery of the service) while minimizing the safety risk itself.
- Communicate the rationale for safety risk decisions to gain acceptance by stakeholders affected by them.

5.8.2 Figure 5-8 presents the safety risk management process in its entirety at a glance. After a safety concern is perceived, hazards underlying the safety concern and potential consequences of the hazard(s) are identified and the safety risks of the consequences are assessed in terms of probability and severity, to define the level of safety risk (safety risk index). If the safety risk(s) is assessed as acceptable, action as appropriate is taken and the operation continues. For feedback purposes (safety library), the hazard identification and safety risk(s) assessment and mitigation are recorded.

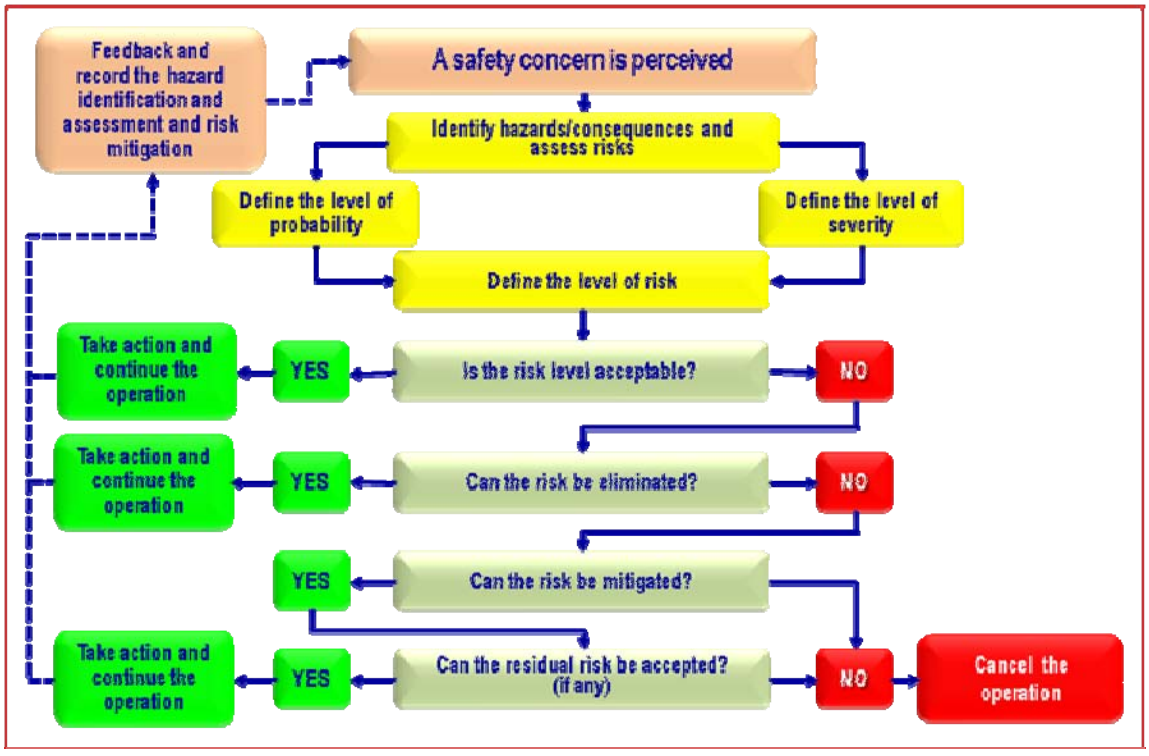



Figure 5-8 – The safety risk management process

5.8.3 If the safety risk(s) is assessed as unacceptable, the following questions become relevant:

a) ***Can the safety risk(s) be eliminated?*** If the answer is yes, then action as appropriate is taken and feedback to the safety library established. If the answer is no, then the next question is:

b) ***Can the safety risk(s) be mitigated?*** If the answer is no, the operation must be cancelled. If the answer is yes, mitigation action as appropriate is taken and then the next question is:

c) ***Can the residual safety risk be accepted?*** If the answer is yes, then action is taken (if necessary) and feedback to the safety library established. If the answer is no, then the operation must be cancelled.

5.8.4 Question c) above reflects the fact that mitigation strategies can never completely mitigate safety risk(s). It must be accepted that a residual safety risk will always exist, and the organization must ensure that the residual safety risks are also under control.

5.8.5 In order to provide a practical illustration of the safety risk management process, three different scenarios of safety risk management are presented in three attachments to this chapter. Appendix 1 includes an example of a safety risk management exercise at an aerodrome. Appendix 2 includes an example of a safety risk management exercise by an air traffic service provider. Appendix 3 includes an example of a safety risk management exercise by an airline.

- - - - - - - - - - - - - - - -

# Appendix 1 to Chapter 5

# ANYCITY INTERNATIONAL AIRPORT CONSTRUCTION PLAN

## SCENARIO

Anycity International Airport (AIA) has two parallel runways, one main and one secondary, and is planning to install drainage near the approach end of the secondary runway. Construction vehicles must cross the primary runway to gain access to the construction site. Because there are numerous operations during the day, a decision is made to do work at night, during lighter traffic, to avoid disruption of day operations. The AIA Safety Manager must evaluate the safety consequences of the plan for night construction of the drainage.

AIA Safety Action Group (SAG) has been tasked to support the AIA Safety Manager in evaluating the safety consequences of the construction plan. One immediate and obvious generic area of concern is the movement of construction vehicles to and from the work site that could lead to runway incursions. The SAG applies a safety risk management process to evaluate the safety consequences of the construction plan.

## AERODROME SYSTEM DESCRIPTION

One of the first tasks of the SAG is to describe the modified system under which the airport will conduct operations while construction is being carried out, as follows:

- Runway environment during construction at night, including a high volume of construction vehicle traffic between the ramp and the construction site.
- Existing driver training programme and the use of escorts for construction vehicles.
- Air traffic control tower, but no radio communications with construction vehicles, which are not radio-equipped.
- Signs, markings and lighting for the taxiways, runways, and construction area.

## HAZARD IDENTIFICATION PROCESS

The second task of the SAG is to identify the hazards and their possible consequences that may affect the aerodrome operation during construction, as follows:

1. State the generic hazard

   a) Airport construction

2. State the specific component(s) of the hazard

   a) Construction vehicles crossing primary runway

3. Assess the consequence(s) of the specific component (s) of the generic hazard

   a) Construction vehicles may deviate from prescribed procedure and cross the primary runway without an escort.

   b) Aircraft could conflict with a crossing vehicle.

## SAFETY RISK ASSESSMENT PROCESS

The third task of the SAG is to assess the safety risk(s) of the consequence(s) identified from the hazards and the existing defences, as follows:

1. The SAG assessment leads to the conclusion that there is a remote probability that a construction vehicle will deviate from prescribed guidelines and cross the primary runway without an escort.

2. There are night air carrier operations at the airport, so there is a remote probability that an aircraft would conflict with a crossing vehicle.

3. While the probability of an aircraft/construction vehicle conflict is remote, the SAG assesses that, should such conflict occur, the severity of the occurrence could be catastrophic.

4. The SAG assesses existing defences (driver training programme, use of escorts for construction vehicles, signs, markings and lighting).

5. Using the Safety Risk Assessment Matrix (Chapter 5, Figure 5-4) and the Safety Risk Tolerability Matrix (Chapter 5, Figure 5-5), the SAG assesses the safety risk index as 3A *(Unacceptable under the existing circumstances).*

6. The SAG concludes that the safety risk of the consequences of the hazard generated by movement of construction vehicles to the construction site is, under the prevailing conditions, unacceptable and that control/mitigation is necessary.

## SAFETY RISK CONTROL/MITIGATION PROCESS

The fourth and last task of the SAG is to mitigate the safety risk of the consequences of the hazards, as follows:

1. The SAG decides to control the safety risk of the consequences of the hazard by using an existing aerodrome perimeter road to gain access to the construction site. All construction vehicles will be escorted on the perimeter road.

2. With this mitigation, the SAG reassesses the probability of construction vehicles crossing the primary runway without an escort, or that aircraft could conflict with a crossing vehicle, as extremely improbable. Nevertheless, should an aircraft/construction vehicle conflict occur, the severity of such occurrence would still be catastrophic.

3. Use of the perimeter road as mitigation may delay construction vehicles due to added driving distance, but in the assessment of the SAG:

    a) while it does not entirely remove the possibility of the consequences of the hazard from occurring (construction vehicles may still cross the primary runway due to a number or combination of circumstances);

    b) it nevertheless brings the safety risks of the consequences (construction vehicle deviating from prescribed procedure and crossing the primary runway without an escort; and aircraft in conflict with a crossing vehicle) to a level as low as reasonably practicable (ALARP).

4. Using the Safety Risk Assessment Matrix (Chapter 5, Figure 5-4) and the Safety Risk Tolerability Matrix (Chapter 5, Figure 5-5), the SAG re-assesses the safety risk index as *1A (acceptable);*

5. The SAG documents this decision process for future follow-up with the Anycity International Airport Safety Manager.

## COMPLETE THE CORRESPONDING LOG

The hazard identification and safety risk management log below is used to provide a record of identified risks and the actions taken by nominated individuals. The record should be retained permanently in the "safety library" in order to provide evidence of safety risk management and to provide a reference for future risk assessments.

Having identified and ranked the safety risks, any existing defences against them should be identified. These defences must then be assessed for adequacy. If these are found to be less than adequate, then additional actions will have to be prescribed. All actions must be addressed by a specified individual (usually the line manager responsible) and a target date for completion must be given. The hazard identification and risk management log is not to be cleared until this action is completed.

**Table 1 – Hazard identification and safety risk management**

| Type of operation or activity | Generic hazard | Specific components of the hazard | Hazard-related consequences | Existing defences to control risk(s) and risk index | Further action to reduce risk(s) and resulting risk index |
|---|---|---|---|---|---|
| Airport operations | Airport construction | Construction vehicles crossing primary runway | a) Construction vehicles may deviate from prescribed procedure and cross the primary runway without an escort.<br>b) Aircraft could conflict with a crossing vehicle. | 1. The SAG assessment leads to the conclusion that there is a remote probability that a construction vehicle will deviate from prescribed guidelines and cross the primary runway without an escort.<br>2. There are night air carrier operations at the airport, so there is a remote probability that an aircraft would conflict with a crossing vehicle.<br>3. While the probability of an aircraft/construction vehicle conflict is remote, the SAG assesses that, should such conflict occur, the severity of the occurrence could be catastrophic.<br>4. The SAG assesses existing defences (driver training programme, use of escorts for construction vehicles, signs, markings and lighting).<br>5. Using the Safety Risk Assessment Matrix (Chapter 5, Figure 5-4) and the Safety Risk Tolerability Matrix (Chapter 5, Figure 5-5), the SAG assesses:<br>Risk index: *3A*<br>Risk tolerability: *Unacceptable under the existing circumstances* | 1. The SAG decides to control the safety risk by using an existing aerodrome perimeter road to gain access to the construction site. All construction vehicles will be escorted on the perimeter road.<br>2. With this mitigation, the SAG reassesses the probability of construction vehicles crossing the primary runway without an escort, or that aircraft could conflict with a crossing vehicle, as extremely improbable. Nevertheless, should an aircraft/construction vehicle conflict occur, the severity of such occurrence would still be catastrophic.<br>3. Use of the perimeter road as mitigation may delay construction vehicles due to added driving distance, but in the assessment of the SAG:<br>a) while it does not entirely remove the possibility of the consequences of the hazard from occurring (construction vehicles may still cross the primary runway due to a number or combination of circumstances);<br>b) it nevertheless brings the safety risks of the consequences (construction vehicle deviating from prescribed procedure and crossing the primary runway without an escort; and aircraft in conflict with a crossing vehicle) to an acceptable level.<br>4. Using the Safety Risk Assessment Matrix (Chapter 5, Figure 5-4) and the Safety Risk Tolerability Matrix (Chapter 5, Figure 5-5), the SAG re-assesses:<br>Risk index: *1A*<br>Risk tolerability: *Acceptable*<br>5. The SAG documents this decision process for future follow-up with the Anycity International Airport Safety |

| Type of operation or activity | Generic hazard | Specific components of the hazard | Hazard-related consequences | Existing defences to control risk(s) and risk index | Further action to reduce risk(s) and resulting risk index |
|---|---|---|---|---|---|
| | | | | | Manager. |

- - - - - - - - - - - - - -

# Appendix 2 to Chapter 5

# CONVERGING RUNWAYS OPERATION

## SCENARIO

An air traffic service provider has received feedback from airport users expressing safety concerns regarding converging runways operations at XYZ International Airport. XYZ International Airport consists of three runways, 08L/26R, 08R/26L, and 12/30 (see Figure 1 hereunder). Converging runway operations are occasionally conducted for runways 26R and 12. The air traffic service provider has requested its Safety Manager to re-evaluate the safety of the converging runway operations procedures for runways 26R and 12 at XYZ International Airport under the light of the concerns expressed by users.

The Safety Action Group (SAG) is requested to assist the ATS service provider Safety Manager in re-evaluating the safety of converging runway operations procedures at XYZ International Airport. The SAG includes representatives from the ATS service provider, airlines operating into XYZ International Airport and their airline pilots association, airport representatives as well as representatives from the State oversight authority. The generic safety concern is the converging flight paths for aircraft departing and arriving into XYZ International Airport. The SAG applies a safety risk management process to re-evaluate the safety of the converging runway operations.

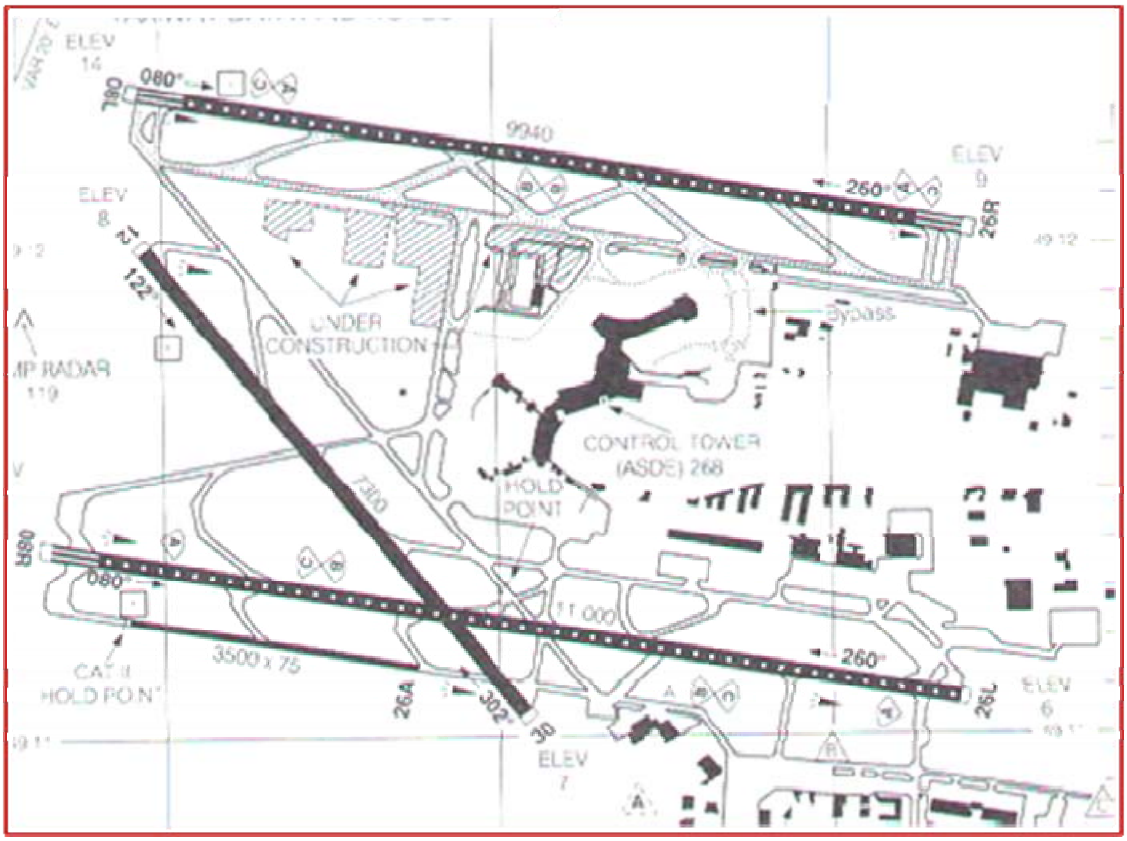



Figure 1 – XYZ International Airport

## SYSTEM DESCRIPTION

One of the first tasks of the SAG is to describe the system in which operation are being carried out, as follows:

- Three main runways and a small secondary runway service XYZ International Airport.

- The airport has about 325,000 movements per year.
- Runway 26L-08R is 11,000 feet long and is used for west and east departures and west and east arrivals. Runway 12/30 is 7,300 ft. Long. Runway 12 is used mostly for arrivals. Runway 30 is used sometimes for departures and seldom used for arrivals. Runway 12 physically crosses runways 08R-26L, and is considered to be "intersecting" runway. Runway 08L/26R is 9,940 ft. long and is used primarily for arriving traffic and occasionally for departing traffic. Runway 08L is used only for arrivals because of departure procedures that have not been established.
- Markings, signage and lighting on the airport meet both the oversight authorities as well as ICAO standards.
- There are two control frequencies used for tower control. One frequency covers the south (26L-08R) and west Runway (12-30). The second frequency covers the north Runway (26R-08L).
- The south runways (26L-08R) have converging runway approaches published to avoid conflict with traffic on 12. There are no converging approaches published for the north runways (26R-08L), as technically, they are not considered intersecting since they do not physically intersect. While Runway 12 has an ILS approach, it is generally a VFR runway with the majority of landings made from visual approaches.
- Runway 12 traffic information is currently passed to traffic on Runway 08R-26L because the runways are considered intersecting. Traffic on both runways is controlled on the same frequency. However, because 08L-26R and 12 do not physically intersect, traffic on these runways is controlled on different frequencies. As a result, traffic information is not shared.
- While IFR traffic separation is provided to IFR traffic on 26R, airport control service is provided to VFR and visual approaches to aircraft on 12. However, air traffic controllers will act immediately to resolve any known traffic conflicts. Standard procedure is to give traffic on runways 26R-08L priority and divert traffic on Runway 12.

## HAZARD IDENTIFICATION PROCESS

The second task of the SAG is to identify the hazards and their consequences that will affect the aerodrome operation, as follows:

1. State the generic hazard
   a) Converging flight paths on Runways 26R-08L and 12, irrespective of aircraft on approach or departure.
2. State the specific component(s) of the hazard.
   a) Aircraft rejects landing on 26R against traffic landing on 12.
   b) Aircraft takes off on 26R against traffic landing on 12.
   c) Aircraft approaches 08L against traffic landing on 12.
   d) An aircraft conducts a "side step" from an approach on Runway 08L to 08R or 08R to 08L against traffic landing on 12.
3. Assess the consequence(s) of the specific component (s) of the generic hazard.
   a) Wake turbulence encounter.
   b) Evasive action to avoid other traffic.
   c) Loss of control following maneuver to avoid other traffic.
   d) Runway overrun following an unstable approach.
   e) Midair collision at the departure end of Runaway 26R between aircraft approaching 12 and aircraft approaching 08L or departing 26R (worst case consequence).

## SAFETY RISK ASSESSMENT PROCESS

The SAG identified the defences supporting converging runway operations for runways 26R-08L and 12 at XYZ International Airport. Such defences take the form of technology, programmes and procedures aimed at reducing the safety risks of the consequences of converging flight paths for Runway 26R-08L and 12.

The defences include:

- Controller coordination procedures;
- Increased spacing to protect airspace for missed approaches during adverse weather;
- Restrictions on arrivals on Runway 12 when Runway 26R is used for departures;
- Aerodrome Surface Detection Equipment (ASDE);
- Runway Incursion Prevention Programme and Wildlife Control Programme;
- Airside driver initial and recurrent training and testing;
- Continual monitoring and statistical follow up of cross-winds limits;
- Availability and use of approach radar;
- Standards for runway occupancy time;
- Separate tower frequencies; and
- Markings and signage.

Based on these existing defences, the SAG, using the Safety Risk Assessment Matrix (Chapter 5, Figure 5-4) and the Safety Risk Tolerability Matrix (Chapter 5, Figure 5-5), assessed the safety risks of the consequences of converging flight paths for Runway 26R-08L and 12 as follows:

a) Wake turbulence encounter: probability remote, severity major. Safety risk tolerability: 3C (acceptable based on risk mitigation).

b) Evasive action to avoid other traffic: probability remote, severity major. Safety risk tolerability: 3C (acceptable based on risk mitigation).

c) Loss of control following maneuver to avoid other traffic: probability remote, severity hazardous. Safety risk tolerability: 3B (acceptable based on risk mitigation).

d) Runway overrun following an unstable approach: probability remote, severity hazardous. Safety risk tolerability: 3B (acceptable based on risk mitigation).

e) Midair collision at the departure end of Runaway 26R between aircraft approaching 12 and aircraft approaching 08L or departing 26R: probability improbable, severity catastrophic. Safety risk tolerability: 2A (acceptable based on risk mitigation).

## SAFETY RISK CONTROL/MITIGATION PROCESS

The SAG recognized that prohibiting operations on converging runways would effectively eliminate the worst possible consequence of converging flight paths for Runway 26R-08L and 12: a mid-air collision at the departure end of Runway 26R. However, safety management action must be efficient, not just effective. Prohibiting the use of converging runways would be inefficient.

The SAG concluded that there were no safety concerns at XYZ International Airport regarding converging runway operations for runways 26R and 12 that required urgent, immediate action. Existing defences for the safety risks of the consequences of converging flight paths for Runway 26R-08L and 12 at XYZ International Airport, including the worst-case scenario (a mid-air collision) are effective controls to keep safety risks ALARP (as low as reasonably practicable). Nevertheless, recommendations for reinforcing safety of operations at XYZ International Airport were made. While not of urgent nature, implementation of these recommendations would provide a greater margin of safety.

The recommendations include:

a) Initiate a continuing campaign to encourage flight crews to pass PIREPS to air traffic control units when weather conditions differ from those forecast or expected;

b) Study the appropriateness and effectiveness of the implementation of a Converging Runway Display Aid (CRDA) as an essential safety and capacity enhancement device at XYZ International Airport;

c) If CRDA is not implemented at XYZ International Airport, establish separation criteria and procedures for adjusting the landing aircraft spacing such that an aircraft that may reject a landing on runway 26R has protected airspace from aircraft that may be approaching runway 12;

d) Depict a range of approach speed constraints on arrival type charts; and modify air traffic controller communication procedures so traffic on 08L-26R is kept advised of intersecting traffic on runway 12;

e) Install an emergency frequency override so that one controller can switch to other controller's frequency to issue emergency instructions.

The SAG documents this decision process for future follow-up with the air traffic service Safety Manager.

## COMPLETE THE CORRESPONDING LOG

The hazard identification and safety risk management log below is used to provide a record of identified risks and the actions taken by nominated individuals. The record should be retained permanently in the "safety library" in order to provide evidence of safety risk management and to provide a reference for future risk assessments.

Having identified and ranked the safety risks, any existing defences against them should be identified. These defences must then be assessed for adequacy. If these are found to be less than adequate, then additional actions will have to be prescribed. All actions must be addressed by a specified individual (usually the line manager responsible) and a target date for completion must be given. The hazard identification and risk management log is not to be cleared until this action is completed.

**Table 1 – Hazard identification and safety risk management**

| Type of operation or activity | Generic hazard | Specific components of the hazard | Hazard-related consequences | Existing defences to control risk(s) and risk index | Further action to reduce risk(s) and resulting risk index |
|---|---|---|---|---|---|
| Air traffic control activities | Converging flight paths on Runways 26R-08L and 12, irrespective of aircraft on approach or departure | a) Aircraft rejects landing on 26R against traffic landing on 12.<br>b) Aircraft takes off on 26R against traffic landing on 12.<br>c) Aircraft approaches 08L against traffic landing on 12.<br>d) An aircraft conducts a "side step" from an approach on Runway 08L to 08R or 08R to 08L against traffic landing on 12. | a) Wake turbulence encounter.<br>b) Evasive action to avoid other traffic.<br>c) Loss of control following maneuver to avoid other traffic.<br>d) Runway overrun following an unstable approach.<br>e) Midair collision at the departure end of Runaway 26R between aircraft approaching 12 and aircraft approaching 08L or departing 26R (worst case consequence). | • Controller coordination procedures;<br>• Increased spacing to protect airspace for missed approaches during adverse weather;<br>• Restrictions on arrivals on Runway 12 when Runway 26R is used for departures;<br>• Aerodrome Surface Detection Equipment (ASDE);<br>• Runway Incursion Prevention Programme and Wildlife Control Programme;<br>• Airside driver initial and recurren training and testing;<br>• Continual monitoring and statistical follow up of cross-wind limits;<br>• Availability and use of approach radar;<br>• Standards for runway occupancy time;<br>• Separate tower frequencies; and<br>• Markings and signage<br>a) Wake turbulence encounter:<br>Risk index: 3C<br>Risk tolerability: Acceptable based on risk mitigation<br>b) Evasive action to avoid other traffic:<br>Risk index: 3C<br>Risk tolerability: Acceptable based on risk mitigation<br>c) Loss of control following maneuv to avoid other traffic:<br>Risk index: 3B<br>Risk tolerability: Acceptable based on risk mitigation<br>d) Runway overrun following an unstable approach:<br>Risk index: 3B<br>Risk tolerability: Acceptable based on risk mitigation<br>e) Midair collision at the departure end of Runaway 26R between aircraft approaching 12 and aircraft approaching 08L or departing 26R:<br>Risk index: 2A<br>Risk tolerability: Acceptable based on risk mitigation | a) Initiate a continuing campaign to encourage flight crews to pass PIREPS to air traffic control units when weather conditions differ from those forecast or expected;<br>b) Study the appropriateness and effectiveness of the implementation of a Converging Runway Display Aid (CRDA) as an essential safety and capacity enhancement device at XYZ International Airport;<br>c) If CRDA is not implemented at XYZ International Airport, establish separation criteria and procedures for adjusting the landing aircraft spacing such that an aircraft that may reject a landing on runway 26R has protected airspace from aircraft that may be approaching runway 12;<br>d) Depict a range of approach speed constraints on arrival type charts; and modify air traffic controller communication procedures so traffic on 08L-26R being advised of intersecting traffic on runway 12.<br>e) Install an emergency frequency override so that one controller can switch to other controller's frequency to issue emergency instructions. |

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 3 to Chapter 5

# COMMERCIAL OPERATION AT ANDES CITY INTERNATIONAL AIRPORT

## SCENARIO

Safe Airways is a medium size air operator with a fleet of fifteen modern technology twin-jet airliners. The airline is planning to start commercial operations into Andes City, a tourist resort located in the high mountains, surrounded by beautiful landscape and showcasing the vestiges of an ancient civilization. Andes City can only be reasonably served only by air from a nearest hub. Ground transportation can take more than two days through hazardous roads; therefore air transportation is the most suitable means of transportation.

Andes City is served by a high elevation aerodrome surrounded by a complex geography with no approach navigational aids, resulting in flight operations limited to day-time and visual conditions. Senior management of Safe Airways requests that the Director of Flight Operations implement the operation in compliance with all safety requirements and at the same time ensuring a maximum commercial payload, with due regard to aircraft performance and limitations. The planned operation would involve an early afternoon flight into Andes City, with a quick turn-around to the main base, ninety minutes away.

The Director of Flight Operations asks the Safety Manager, with the support of the Safety Action Group (SAG), to evaluate the safety consequences of the operation at Andes City International Airport. One immediate and obvious generic area of concern is the operation at a high elevation aerodrome surrounded by a complex geography with no approach navigational aids. The SAG applies a safety risk management process to evaluate the safety consequences of the operation at Andes City International Airport.

## SYSTEM DESCRIPTION

One of the first tasks of the SAG is to describe the system in which the operation is being carried out, as follows:

- Andes City International Airport is located in a valley at an elevation of 11.000 feet surrounded by mountains of more than 16.000 feet.
- The aerodrome has only one runway with a length of 3.400 m (11.155 ft), oriented east-west (09-27)
- Because of the topography, Runway 09 is exclusively used for landing and Runway 27 is exclusively used for take-off .
- A VOR is used for instrument letdown approach, located twenty miles west from the aerodrome in the valley.
- No ILS approach is available.
- No visual approaches are allowed, once a departing aircraft has been authorized to take-off until climb to an en-route altitude clear of all obstacles has been reported by the departing aircraft.
- The visual approach in VMC to Andes City International Airport starts at 18 000 feet over the VOR. If no ground contact is established at 18 000 ft, VMC approaches are not authorized by ATC.
- No landing visual aids are available.
- No take-off is permitted until an aircraft authorized by ATC to initiate its visual approach to Andes City International Airport has landed and announced clear of the runway after landing.
- The weather at Andes City International Airport is variable, often characterised by a high layer of clouds with a base around 19 000 to 21 000 feet.
- Outside temperature is high between 10:00 and 14:00 hours, affecting aircraft performance.
- Katabatic winds may impose the need for tailwind take offs from runway 27 after approximately 16:00 hours daily.
- In case of engine fire, engine-out or any emergency condition, return to the airport is mandatory, since weight and performance limitations would make it unlikely to comply with obstacle clearance net trajectory.

- The national Civil Aviation Authority requires that the airline shall demonstrate that the aircraft complies with the net trajectory and obstacle clearance during the approach, landing, take-off, climb and en-route phases, and can manoeuvre within the complex topography within the safety margins and aircraft limitations, to obtain the special operation authorization as part of it's the operator certificate.
- A test flight is required by the CAA when the operation is ready to launch, after the documentation has been reviewed and approved, and the flight and cabin crew received special training for the operation of Andes City International Airport.

## HAZARD IDENTIFICATION PROCESS

The second task of the SAG is to identify the hazards that will affect the Andes City International Airport operation and their consequences, as follows:

1. State the generic hazard
    a) Revenue operation at a high-altitude airport surrounded by complex geography
2. State the specific component(s) of the hazard
    a) Surrounding mountains
    b) High elevation aerodrome
    c) Lack of approach and landing navigational aids
    d) Lack of visual landing aids
    e) Conflicting traffic
    f) Slippery runway when wet
    g) Wildlife
3. Assess the consequence(s) of the specific component (s) of the generic hazard
    a) Controlled flight into terrain (CFIT) due to:
        i. Loss of critical engine during approach and landing.
        ii. Loss of critical engine during take-off after V1.
        iii. Loss of critical engine during en-route climb.
    b) Mid-air collision
    c) Landing overrun after landing
    d) Landing overrun following aborted take-off.
    e) Bird strike.

## SAFETY RISK ASSESSMENT PROCESS

***Note**. – Controlled flight into terrain due to loss of critical engine during take-off after V1 is the only consequence analyzed in this exercise. In an actual evaluation all consequences need to be analyzed and all safety risks assessed and mitigated.*

The third task of the SAG is to assess the effectiveness of existing defences to address the safety risk(s) of the consequence(s) identified from the hazards.

The SAG reviews existing safety defences that can be affected or missing in relation to this operation. These defences are mainly related to flight crew training and the procedures and limitations in the company operations manual in relation to similar operations.

The existing defences identified during the assessment were as follows:

1) VMC and day-light aircraft operation.
2) Aerodrome layout available in the national AIP.
3) ATC procedures in place at the aerodrome.
4) Company operations manual.

5) Dispatch performance manual.

6) Aircraft operating manual.

7) Recurrent training on engine failure before and after V1 and missed approach procedures.

8) CRM training.

SAG considers existing defences, mainly because they fail to address the specific operation at a high elevation aerodrome surrounded by complex geography.

Operational documentation is reviewed as well as current ATC procedures at Andes City International Airport.

Using the Safety Risk Assessment Matrix (Chapter 5, Figure 5-4) and the Safety Risk Tolerability Matrix (Chapter 5, Figure 5-5), the SAG assesses the safety risk index as 3A (Unacceptable under the existing circumstances).

## SAFETY RISK CONTROL/MITIGATION PROCESS

The fourth and last task of the SAG is to control and mitigate the identified safety risks of the consequences of a CFIT due to loss of critical engine during take-off after V1. After several meetings, the SAG proposes several mitigations. The proposed mitigations aim at reinforcing the defences and lowering the safety risk to "as lows as reasonably practicable" (ALARP). The mitigations include:

1. Develop take-off and climb procedures in case of the loss of a critical engine after V1, considering the possibility of a return to land.
2. Develop and provide training in the above procedures (full flight simulator and maintain qualification every six months).
3. Consider Andes City International Airport "special aerodrome operation" requiring special crew qualification, valid for only for one year unless renewed.
4. Provide appropriate "special aerodrome operation" training to cabin crews. (This mitigation does not address probability but severity – emergency evacuation – of the safety risk)
5. Ground operations personnel aware of the importance of providing accurate weather information, particularly surface winds after 16:00 hours.
6. Develop operational documentation and include it in the company operations manual and dispatch manual, for approval by the CAA.
7. No open Minimum Equipment List (MEL) critical items policy.
8. Maintenance Department to observe the engines of the aircraft allocated to the operation under the maintenance reliability programme.
9. Follow-up on safety measures and new defences implemented for the control and mitigation of the safety risks related to the operation in Andes City International Airport. A review of the effectiveness of the defences is planned 6 months and 12 months after the changes are implemented and the authorization is granted by the CAA.

Taking into account the new defences put in place for this special operation, the safety risk of a CFIT due to loss of critical engine during take-off after V1 is now assessed as Improbable (2 - Very unlikely to occur) although severity of a CFIT still remains Catastrophic (A – Equipment destroyed – Multiple deaths).

The operation now falls in the tolerable region and the resulting Risk index is 2A – Acceptable based on risk mitigation. It might require management decision (Refer to Chapter 5, Figure 5-8). The safety data and documentation resulting from the hazard identification and risk management processes is incorporated in the company "safety library".

## INDIVIDUAL RESPONSIBILITY TO IMPLEMENT MITIGATION MEASURES

The individual responsibilities to implement the proposed mitigation measures are as follows:

a) Mitigation measures 1, 6 and 9 – Director of flight operations

b) Mitigation measures 2, 3 and 4 – Flight training manager

c) Mitigation measure 5 – Manager, Dispatch

d) Mitigation measures 7 and 8 – Director of maintenance

## COMPLETION OF THE CORRESPONDING LOG

The hazard identification and risk management log below is used to provide a record of identified safety risks and the actions taken by nominated individuals. The record should be retained permanently in the "safety library" in order to provide evidence of safety risk management and to provide a reference for future risk assessments.

Having identified and ranked the safety risks, any existing defences against them should be identified. These defences must then be assessed for adequacy. If these are found to be less than adequate, then additional actions will have to be prescribed. All actions must be addressed by a specified individual (usually the line manager responsible) and a target date for completion must be given. The Hazard identification and risk management log is not to be cleared until this action is completed

**Table 3 – Hazard identification and risk management**

| Type of operation or activity | Generic hazard | Specific components of the hazard | Hazard-related consequences | Existing defences to control risk(s) and risk index | Further action to reduce risk(s) and resulting risk index | Responsible person |
|---|---|---|---|---|---|---|
| Flight operations | Revenue operation at a high-altitude airport surrounded by complex geography | Surrounding mountains<br>High elevation aerodrome<br>Lack of approach and landing navigational aids<br>Lack of visual landing aids<br>Conflicting traffic<br>Slippery runway when wet<br>Wildlife | a) Controlled flight into terrain (CFIT) due to:<br>i. Loss of critical engine during approach and landing.<br>ii. Loss of critical engine during take-off after V1.<br>iii. Loss of critical engine during en-route climb.<br>b) Mid-air collision<br>c) Landing overrun after landing<br>d) Landing overrun following aborted take-off.<br>e) Bird strike<br>*Note. – Controlled flight into terrain due to loss of critical engine during take-off after V1 is the only consequence analyzed in this exercise. In an actual evaluation all consequences need to be analyzed and all safety risks assessed and mitigated.* | 1) VMC and day-light aircraft operation.<br>2) Aerodrome layout available in the national AIP.<br>3) ATC procedures in place at the aerodrome.<br>4) Company operations manual.<br>5) Dispatch performance manual.<br>6) Aircraft operating manual.<br>7) Recurrent training on engine failure before and after V1 and missed approach procedures.<br>8) CRM training.<br>Risk index: *3A*<br>Risk tolerability: *Unacceptable under the existing circumstances* | 1. Develop take-off and climb procedures in case of the loss of a critical engine after V1, considering the possibility of a return to land.<br>2. Develop and provide training in the above procedures (full flight simulator and maintain qualification every six months).<br>3. Consider Andes City International Airport "special aerodrome operation" requiring special crew qualification, valid for only for one year unless renewed.<br>4. Provide appropriate "special aerodrome operation" training to cabin crews. (This mitigation does not address probability but severity – emergency evacuation – of the safety risk)<br>5. Ground operations personnel aware of the importance of providing accurate weather information, particularly surface winds after 16:00 hours.<br>6. Develop operational documentation and include it in the company operations manual and dispatch manual, for approval by the CAA.<br>7. No open Minimum Equipment List (MEL) critical items policy. | 1. Director of operations<br>2. Training manager<br>3. Training manager<br>4. Training manager<br>5. Manager, Dispatch<br>6. Director of operations<br>7. Director of maintenance |

| Type of operation or activity | Generic hazard | Specific components of the hazard | Hazard-related consequences | Existing defences to control risk(s) and risk index | Further action to reduce risk(s) and resulting risk index | Responsible person |
|---|---|---|---|---|---|---|
| | | | | | 8. Maintenance Department to observe the engines of the aircraft allocated to the operation under the maintenance reliability programme.<br>9. Follow-up on safety measures and new defences implemented for the control and mitigation of the safety risks related to the operation in Andes City International Airport. A review of the effectiveness of the defences is planned 6 months and 12 months after the changes are implemented and the authorization is granted by the CAA.<br>Risk index: *2A*<br>Risk tolerability: *Acceptable based on risk mitigation. It might require management decision* | 8. Director of maintenance<br>9. Director of operations |

- - - - - - - - - - - - - - -

# Chapter 6

# ICAO SAFETY MANAGEMENT REQUIREMENTS

## 6.1 OBJECTIVE AND CONTENTS

6.1.1 This chapter presents the ICAO safety management requirements included in Annexes 1 – *Personnel licensing*, 6 – *Operation of aircraft*, 8 – Airworthiness of aircraft, 11 – *Air Traffic Services*, 13 – *Aircraft accident and incident investigation* and 14 – *Aerodromes*. The chapter also presents the relationship between the State safety programme (SSP) and service providers safety management systems (SMS). The chapter includes the following:

- ICAO safety management requirements – General
- State safety programme (SSP)
- Acceptable level of safety (ALoS)
- Safety management system (SMS)
- SMS safety performance
- Management accountability
- SSP – SMS relationship
- Compliance and performance

## 6.2 ICAO SAFETY MANAGEMENT REQUIREMENTS – GENERAL

6.2.1 The ICAO safety management requirements encompass the following Annexes: Annex 1 – *Personnel licensing;* Annex 6 — *Operation of Aircraft, Part I — International Commercial Air Transport — Aeroplanes*, and *Part III — International Operations — Helicopters*, Annex 8 – *Airworthiness of aircraft;* Annex 11 — *Air Traffic Services*, Annex 13 – *Aircraft accident and incident investigation;* and Annex 14 — *Aerodromes*. These Annexes address the activities of approved training organizations, international aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes. In the case of Annex 1, the safety management requirements are limited to approved training organizations that are exposed to safety risks during the provisions of their services, exclusively.

6.2.2 The safety management requirements are aimed at two audience groups: States and service providers. In the context of this Manual, the term “service provider” refers to any organization providing aviation services. The term thus encompasses approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.

6.2.3 The ICAO safety management requirements can be grouped as addressing three distinct requirements:

a) requirements regarding the State safety programme (SSP), including the acceptable level of safety (ALoS) of an SSP;

b) requirements regarding safety management systems (SMS), including the safety performance of an SMS; and

c) requirements regarding management accountability vis-à-vis the management of safety during provision of services.

6.2.4 The ICAO safety management requirements introduce the notion of acceptable level of safety (ALoS) as the way of measuring the safety performance of an SSP, and the notion of safety performance as the way of measuring the safety performance of a service provider’s SMS.

## 6.3 STATE SAFETY PROGRAMME (SSP)

6.3.1 Annexes 1, 6, 8, 11, 13 and 14 include the requirement for States to establish a State safety programme (SSP), in order to achieve an acceptable level of safety in civil aviation. An SSP is a management system for the management of safety by the State.

6.3.2 An SSP is defined as *an integrated set of regulations and activities aimed at improving safety.* It includes specific safety activities that must be performed by the State, and regulations and directives promulgated by the State to support fulfilment of its responsibilities concerning safe and efficient delivery of aviation activities in the State. The responsibilities encompassed by the SSP include, in broad terms:

- Safety regulation
- Accident investigation
- Incident investigation
- Safety assurance
  - Mandatory reporting systems
  - Voluntary reporting systems
  - Safety data analysis and exchange
- Safety promotion.

6.3.3 In order to assist States in the establishment of the SSP, ICAO has developed a framework that includes both the components and elements of an SSP. The framework consists of four components and eleven elements, and is introduced in full in Chapter 11 of this Manual. The responsibilities encompassed by the SSP are not new. It is a reasonable expectation that most States are already discharging most of these responsibilities. What is new is the notion of the SSP itself, proposing one way of organizing the safety responsibilities and accountabilities of a State in a principled and structured manner, and measuring the effectiveness with which safety responsibilities are discharged and safety accountabilities fulfilled by the State. The organization of the safety responsibilities and accountabilities of a State serving certain principles and following a standard structure allows regulations and activities aimed at improving safety to be documented, explicit and traceable. While the long-term, strategic objective of an SSP is the improvement of safety in the State, the organization of an SSP aims at two short-term, tactical objectives: efficient and effective delivery of safety responsibilities and accountabilities by the State, and efficient auditing of safety responsibilities and accountabilities by the State.

6.3.4 The importance of the second objective, efficient auditing of safety responsibilities and accountabilities by the State, should not be underestimated. At the present time, the ICAO Universal Safety Oversight Audit Programme (USOAP) audits States safety responsibilities in a comprehensive manner, yet following a basic architecture proposed by the Annexes to the Convention on International Civil Aviation. The critical elements that a State's safety oversight function must monitor have been defined, and USOAP audits verify the status of implementation of elements and functions, on a compliance/non-compliance basis. It is envisioned that once the notion of SSP has achieved maturity and is deployed throughout States, USOAP will audit the SSP in a holistic manner rather than the elements of the safety oversight function, through an approach based on a continuous monitoring concept.

6.3.5 The notion of the SSP also aims at a third and medium-term objective: the transition from a predominantly prescriptive regulatory environment to an integrated regulatory environment combining prescriptive and performance-based regulatory approaches. In this transition, the notion of ALoS of an SSP and of safety performance of an SMS discussed later in this Chapter is fundamental. This transition, however, must start by clearly establishing the role of the State's safety oversight function within the SSP, and their mutual relationship. A brief discussion follows.

6.3.6 A State's safety oversight function is part of an SSP. The objectives of the State's safety oversight function, as traditionally practiced, are satisfied through administrative controls (inspections, audits and surveys) carried out by civil aviation authorities regularly. The critical elements of a State's safety oversight function do not, in themselves, constitute safety risk controls, as discussed in Chapter 5 and in Section 6.8. The SSP is necessary to turn the critical elements into safety risk controls. For example, a State's safety oversight function presently verifies that a State has a system of regulations, but neither requires a safety risk analysis to produce such regulations, nor does it monitor the effectiveness of regulations as safety risk controls. The SSP, on the other hand, considers regulations as safety risk controls and requires, through its safety risk management component, that the process of rulemaking be done using principles of safety risk management (identify hazards, assess the safety risks of the consequences of the hazards, and develop regulations that provide acceptable mitigation/control of the consequences of the hazards). On a second stage, the SSP monitors, through its safety assurance component, the effectiveness and efficiency of regulations as safety risk controls.

6.3.7 Clear articulation of the difference between regulations as administrative controls and regulations as safety risk controls underlies the shift from prescriptive regulation to performance-based regulation. The SSP, as proposed in the framework discussed in Chapter 11, is a first enabling step in such a shift. Furthermore, the integration into the SSP, as

appropriate, of the principles underlying the role of the critical elements of a State's safety oversight function will yield a more robust and effective SSP.

## 6.4 ACCEPTABLE LEVEL OF SAFETY (ALoS)

6.4.1 Annexes 1, 6, 8, 11, 13 and 14 require that the acceptable level of safety (ALoS) to be achieved (by an SSP) shall be established by the State.

6.4.2 The notion of ALoS is an essential ingredient for the effective operation of an SSP. Unless the notion of ALoS is understood and properly developed and implemented, it will be difficult to progress to a performance-based regulatory environment, and to monitor actual performance of an SSP. The operation of an SSP may then be reduced to simply "ticking boxes" under false pretences of managing safety.

6.4.3 The basic management axiom that one cannot manage what one cannot measure is discussed in elsewhere in the Manual. In any system, it is necessary to define a set of measurable performance outcomes in order to determine whether the system is truly operating in accordance with design expectations, as opposed to simply meeting regulatory requirements. The definition of a set of measurable performance outcomes also allows identifying where action may be required to bring operational performance of the system to meet the level of design expectations. Thus, measurable performance outcomes permit to assess the actual performance of activities critical to safety against existing organizational controls, so that safety risks can be maintained ALARP and necessary corrective action taken.

6.4.4 The introduction of the notion of ALoS also responds to the need to complement the historical approach to the management of safety based upon regulatory compliance, with a performance-based approach. A performance-based approach will assess the actual performance of activities critical to safety against existing organizational controls. Only through assurance of effective safety operational performance of the SSP – through the establishment and measurement of specific safety performance outcomes – can the objective of continuous improvement of safety underlying safety management be achieved.

6.4.5 In order to properly develop ALoS for an SSP, it is essential to understand the difference between two closely interrelated – and therefore sometimes confusing – yet quite distinct concepts: *safety measurement* and *safety performance measurement*.

6.4.6 **Safety measurement** refers to the quantification of the outcomes of high-level, high-consequence *events*, such as accident and serious incident rates. Safety measurement can also be applied to reflect the quantification of high-level State functions, such as the status of development/implementation of primary aviation safety legislation or its absence thereof, the status of development/implementation of specific operating regulations or its absence thereof, and the level of regulatory compliance within the State. Safety measurement is not a continuous process, but it is rather a spot check, normally conducted following pre-specified time frames, for example, annually, semi-annually or quarterly.

6.4.7 **Safety performance measurement** refers to the quantification of the outcomes of low-level, low-consequence *processes,* such as number of foreign object debris (FOD) events per specified number of ramp operations, or number or unauthorized ground vehicles events in taxiways per specific number of airport operations or during a specified period of time. Safety performance measurement is a non-stop activity, involving continuous monitoring and measurement of selected operational activities by an organization that are necessary to deliver the services the organization was constituted to deliver (provision of aerodrome services, of air traffic control, of training, etc.). Safety performance measurement thus provides a measure of the actual, operational performance of a management system, such as an SSP (or an SMS), beyond the absolute measures resulting from safety measurement (including regulatory compliance).

6.4.8 The ALoS of an SSP must be developed based upon a judicious combination of safety measurement and safety performance measurement. ALoS expresses the safety objectives of a State, and thus a reference against which the State can measure its own safety performance. In determining an ALoS, a State needs to consider such factors as the level of safety risk that applies, the cost/benefits of improvements to the system, and public expectations on the safety of the aviation industry.

6.4.9 The ALoS of an SSP can therefore be presented as a three-legged stool. One leg represents the *high level safety management objectives of the State*, the achievement of which is confirmed through safety measurement. The second leg represents the *minimum safety performance the State should deliver through its SSP*, the achievement of which is confirmed through safety performance measurement. These two are direct measures or indications of the safety performance of the SSP. The third leg is the safety performance measurement of service providers' SMS. This is an *indirect indication,* since the measurement of safety performance of service providers' SMS in aggregate form will indirectly reflect the safety performance of the SSP. (Figure 6-1)

6.4.10 In practice, an ALoS is expressed by two measures or metrics: safety performance indicators and safety performance targets. An ALoS is implemented through various safety requirements.

6.4.11 Safety performance indicators are short-term, tactical, measurable objectives reflecting the safety performance of an SSP. Safety performance indicators are expressed in numerical terms, and they should be obvious, measurable and linked to safety concerns identified and addressed by a State through its SSP. The safety performance indicators of an SSP should be developed on the basis of a combination of safety measurement and safety performance measurement. An example is provided.


**Figure 6-1 – ALoS of an SSP**

6.4.12 A State has identified Controlled Flight into Terrain (CFIT) events as a safety concern to be addressed by its SSP. It therefore sets a safety performance indicator of 0.08 CFIT events per 100,000 operations by large public transport aircraft in its airspace (high-consequence outcome, or safety measurement). The State has also identified airport operations safety as a safety concern to be addressed by its SSP and, through the safety risk management component of its SSP, has identified a specific concern regarding runway incursions. It therefore defines the following safety performance indicator: 1.2 low severity runway incursions per 10,000 operations in [five] State international airports (low consequence process, or safety performance measurement). These two safety performance indicators fulfil the conditions discussed in paragraph 6.4.11 above: they are expressed in numerical terms; they are obvious, measurable and related to safety concerns of the SSP. One safety performance indicator reflects safety measurement; the other reflects safety performance measurement.

6.4.12 Safety performance targets are long-term, strategic, measurable objectives reflecting the safety performance of an SSP. Safety performance targets should be obvious, measurable, and linked to the safety performance indicators (short-term objectives) of a safety concern of a SSP SMS. The safety performance targets of an SSP should be developed on the basis of a combination of safety measurement and safety performance measurement. An example is provided.

6.4.13 Subsequent to the definition of a safety performance indicator of 0.08 CFIT events per 100,000 operations by large public transport aircraft in its airspace, the State defines a safety performance target of reducing the number of CFIT events to 0.04 per 100,000 operations by 2010. Subsequent to the definition of 1.2 low severity runway incursions per 10,000 operations in [five] State international airports, the State defines a safety performance target of reducing low severity runway incursions per 10,000 operations in [five] State international airports to 0.6 by 2011. These safety performance targets fulfil the conditions discussed in paragraph 6.4.12 above: they are expressed in numerical terms, obvious, measurable, and linked to safety performance indicators of a safety concern of the SSP. One safety performance target reflects safety measurement; the other reflects safety performance measurement.

6.4.14 The safety requirements are the tools and means needed to achieve the safety performance indicators and safety performance targets of an SSP. They include the operational procedures, technology, systems and programmes to which measures of reliability, availability, performance and/or accuracy can be specified. An example of a safety requirement for the example of CFIT safety performance indicator/target would be the implementation of Constant Descent Arrivals (CDA) procedures, and arrival procedures charts designed for stabilised approaches. An example of safety requirement for the low severity runway incursion safety performance indicator/target would be deployment of a radar system in the State's five international aerodromes within the next 12 months, with a 98 per cent availability of critical equipment.

6.4.15 Safety performance indicators and safety performance targets of an ALoS may be different, as in the examples presented in the previous paragraphs, or they may be the same, i.e., the safety performance target would be to

maintain the specified safety performance indicator value over a specific time frame. For example, maintain 1.2 low severity runway incursions per 10,000 operations in [five] State international airports through 2011.

6.4.16 Three aspects must be considered when assessing whether specific safety performance indicators and safety performance targets of an ALoS are different or the same. First, consideration must be given to the availability of resources within the State to turn the safety performance indicator into a more demanding safety performance target. Second, consideration must be given to how expensive the safety requirements deemed necessary to change the safety performance indicator into a more demanding safety performance target are. Third, and most importantly, consideration must be given to whether the assessment of the safety risks of the consequence(s) of the hazards addressed by the safety performance indicator and safety performance target falls in the tolerable region of the safety risk management process discussed in Chapter 5, should the safety performance indicators and safety performance targets remain the same. A safety performance indicator may reflect a safety risk assessment that falls in the tolerable region under prevailing circumstances. However, changes in the system, growth and so forth may render such safety risk assessment invalid. The safety performance indicator must in this case be turned into a more demanding target to be valid in the changed environment.

6.4.17 A range of different safety performance indicators and safety performance targets will provide a better insight of the ALoS of an SSP than the use of a single indicator or target. In other words, an ALoS will always be expressed by a number of safety performance indicators and safety performance targets, never by a single one. An example of a range of safety performance indicators and safety performance targets for an SSP would be as follows:

- 50 general aviation aircraft incidents per 100,000 hours flown (safety performance indicator) with a 25 per cent reduction in three years (safety performance target);
- 200 major aircraft defect incidents per 100,000 hours flown (safety performance indicator) with a 25 per cent reduction over the last three-year average (safety performance target);
- 1.0 bird strike per 1,000 aircraft movements (safety performance indicator) with a 50 per cent reduction in five years (safety performance target);
- one runway incursion per 40,000 aircraft movements (safety performance indicator) with a 40 per cent reduction in a 12-month period (safety performance target); and
- 40 airspace incidents per 100,000 hours flown (safety performance indicator) with a 30 per cent reduction over the five-year moving average (safety performance target).

6.4.18 The safety requirements to achieve these safety targets and safety indicators include:

- the functions and activities of the civil aviation oversight authority ;
- the State's responsibility for accidents and major incidents investigation;
- a mandatory occurrence reporting system;
- a voluntary occurrence reporting system;
- a bird strike programme; and
- the deployment of radar systems in the State's five international aerodromes within the next 12 months.

6.4.19 It must be emphatically asserted that the notion of ALoS refers to national or State-level objectives, to be achieved through the SSP, as a means to verify satisfactory operational performance of the SSP. Therefore, reference must be always made to the *acceptable level of system of an SSP*. The safety performance indicators and safety performance targets of an ALoS provide a measurable way of ensuring and demonstrating the effectiveness of an SSP, beyond regulatory compliance. An SSP should fulfil all regulatory requirements as set forth by international and national regulations. Regulatory compliance still remains at the foundations of safety management. By selecting a combination of measurable operational performance outcomes, which are State-specific, and which build upon the foundations provided by regulatory compliance, the real effectiveness and efficiency of the safety management processes underlying an SSP can be assured.

6.4.20 The implementation of ALoS is above and beyond regulatory compliance with national and international requirements. Establishing ALoS for its SSP does not replace legal, regulatory, or other established requirements, nor does it relieve States from their obligations regarding the Convention on International Civil Aviation (ICAO Doc 7300) and its related provisions contained in the Annexes to the Convention Aviation.

6.4.21 As conclusion to the discussion on ALoS, Figure 6-2 summarises, in graphical format, the concepts discussed under this section regarding the ALoS of an SSP.


Figure 6-2 – State safety programme (SSP) – ALoS

## 6.5 SAFETY MANAGEMENT SYSTEM (SMS)

6.5.1 Annexes 1, 6, 8, 11, 13 and 14 establish that States shall require, as part of their SSP, that approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes implement a safety management system (SMS). An SMS is a management tool for the management of safety by an organization. The Annexes also establish that the SMS shall be accepted by the State and shall, as a minimum:

- identify safety hazards;
- ensure the implementation of remedial action necessary to maintain agreed safety performance;
- provide for continuous monitoring and regular assessment of the safety performance; and
- aim at a continuous improvement of the overall performance of the safety management system.

6.5.2 The four generic processes included in the ICAO SMS requirement above (identification of hazards, implementation of remedial action to address the safety risks of the consequences of hazards, continuous monitoring and continuous improvement) encompass the four basic safety problem-solving activities that support delivery of services by an organization: (a) finding out what is it that is wrong (*hazard identification*); (b) proposing and implementing a fix or fixes (*remedial action*); (c) making sure that the proposed fix or fixes work as intended (*continuous monitoring*); and (d) constantly improving the management system to ensure efficacy and efficiency of the delivery of services (*continuous improvement of the SMS*).

6.5.3 An SMS is defined as *a systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures*. The fundamentals of SMS are discussed in Chapter 7. Just as with the SSP, ICAO has developed an SMS framework to assist service providers in the implementation of SMS. The framework is composed of four components and twelve elements, and is introduced in full in Chapters 8 and 9.

## 6.6 SMS SAFETY PERFORMANCE

6.6.1 Annexes 1, 6, 8, 11, 13 and 14 establish that a service provider SMS shall ensure remedial action to maintain safety performance and shall continuously monitor and shall regularly assess such safety performance.

6.6.2 The notion of safety performance is an essential ingredient of the effective operation of an SMS as well as to progress towards a performance-based regulatory environment. It assists in monitoring actual performance of the SMS, and in avoiding just simply "ticking boxes". Just as with the SSP, it is necessary for an SMS to define a set of measurable performance outcomes in order to determine whether the system is truly operating in accordance with design expectations – not simply meeting regulatory requirements – and to identify where action may be required to bring the performance of the SMS to meet the level of design expectations. These measurable performance outcomes permit to assess the actual performance of activities critical to safety against existing organizational controls so that necessary corrective action is taken and safety risks can be maintained can be maintained ALARP.

6.6.3 A performance-based regulatory approach will assess the actual performance of activities critical to safety against existing organizational controls. Furthermore, only through assurance of effective safety performance of the SMS – through the establishment and measurement of specific safety performance outcomes – can the objective of continuous improvement of safety underlying safety management can be achieved.

6.6.4 The safety performance of an SMS is not directly related to the quantification of high-consequence outcomes (safety measurement) but rather to the quantification of the low-consequence process (safety performance measurement). The safety performance of an SMS represents safety performance measurement exclusively. Safety performance expresses the safety objectives of a service provider, in the form of measurable safety outcomes of specific low-level processes of the SMS. From the perspective of the relationship between State and service providers, safety performance provides objective evidence for the State to measure the effectiveness and efficiency that the SMS of service providers should achieve while the service providers conducts their core business functions. Such safety performance must be agreed between the State and service providers, as the minimum acceptable the service provider must achieve during the delivery of services. The safety performance of an SMS is thus a reference against which the State can measure safety performance of the SMS, this is, that the SMS works, above and beyond regulatory compliance. In agreeing to the safety performance of an SMS, it is necessary to consider such factors as the level of safety risk that applies, the cost/benefits of improvements to the system, and public expectations on the safety of the aviation industry.

6.6.5 Within each State, the safety performance of each SMS will separately be agreed between the State and individual aviation organizations. Agreed safety performance should be commensurate to the complexity of individual aviation organizations specific operational contexts; and availability of aviation organizations resources to address them. In practice, the safety performance of an SMS is expressed by two measures/metrics (safety performance indicators and safety performance targets) and implemented through various safety requirements.

6.6.6 Safety performance indicators are short-term, tactical, measurable objectives reflecting the safety performance of an SMS. They are expressed in numerical terms; they should be obvious, measurable and linked to the safety concerns of an SMS. Safety performance indicators reflect safety performance measurement **exclusively**. The safety performance indicators of an SMS should not reflect safety measurement. Since the safety performance of each SMS will separately be agreed between the State and individual aviation organizations, safety performance indicators will therefore differ between segments of the aviation industry, such as aircraft operators, certified aerodrome operators, ATS providers, etc. An example is provided.

6.6.7 A certified aerodrome operator has identified through its SMS safety concerns regarding foreign object debris (FOD) in ramp operations. It has also identified safety concerns regarding traffic of unauthorized vehicles in taxiways. It therefore defines the following safety performance indicators, following agreement with the State's civil aviation oversight authority: 15 FOD events in the apron per 10,000 operations, and 20 events of unauthorized vehicles on the taxiways per 10,000 operations. These safety performance indicators fulfil the conditions discussed in paragraph 6.6.6 above: they are expressed in numerical terms, obvious, measurable, and linked to safety concerns of the aerodrome SMS. Furthermore, both safety performance indicators reflect safety performance measurement.

6.6.9 Safety performance targets are long-term, strategic measurable objectives reflecting the safety performance of an SMS. Safety performance targets are expressed in numerical terms, they should be obvious, measurable, acceptable to stakeholders, and be linked to the safety performance indicator (short-term objective) of an SMS.

6.6.10 Continuing with the example discussed in paragraph 6.6.7, the aerodrome defines the following safety performance targets, following agreement with the State's civil aviation oversight authority: by January 2009, *reduce* to 8 FOD

events in the apron per 10,000 operations, and *maintain* 20 events of unauthorized vehicles on the taxiways per 10,000 operations. These safety performance targets fulfil the conditions discussed in paragraph 6.6.6 above: they are expressed in numerical terms, obvious, measurable, and linked to safety performance indicators of the aerodrome SMS. Furthermore, both safety performance targets reflect safety performance measurement.

6.6.11 Safety requirements are the tools and means needed to achieve the safety performance indicators and safety performance targets of an SMS. They include the operational procedures, technology, systems and programmes to which measures of reliability, availability, performance and/or accuracy can be specified. An example of a safety requirement for the example of safety performance indicators and safety performance targets of an SMS discussed above would be as follows: implement a thrice-daily walk-in ramp inspection programme, and develop and implement a training course for drivers and install [aerodrome-specific] taxiway signage.

6.6.12 Safety performance indicators and safety performance targets of the safety performance of an SMS may be different, or they may be the same. Three aspects must be considered when assessing whether specific safety performance indicators and safety performance targets of of the safety performance of an SMS are different or the same. First, consideration must be given to the availability of resources within the service provider to turn the safety performance indicator into a more demanding safety performance target. Second, consideration must be given to how expensive the safety requirements deemed necessary to change the safety performance indicator into a more demanding safety performance target are. Third, and most importantly, consideration must be given to whether the assessment of the safety risks of the consequence(s) of the hazard addressed by the safety performance indicator and safety performance target falls in the tolerable region of the safety risk management process discussed in Chapter 5, should the safety performance indicators and safety performance targets remain the same. A safety performance indicator may reflect a safety risk assessment that falls in the tolerable region under prevailing circumstances. However, changes in the system, growth and so forth may render such safety risk assessment invalid. The safety performance indicator must in this case be turned into a more demanding target to be valid in the changed environment.

6.6.13 A range of different safety performance indicators and safety performance targets will provide a better insight of the safety performance of the SMS of an aviation organization than the use of a single indicator or target. In other words, the safety performance of an SMS will always be expressed by a number of safety performance indicators and safety performance targets, never by a single one. Additional examples follow.

6.6.14 An aircraft operator has identified the approach and landing phases of flight operations as one major safety concern to be addressed by its SMS. It has also identified, though the safety risk management component of its SMS, a safety concern regarding unstable (or non-conforming) approaches in those aerodromes of the network served by non-precision approaches. It therefore defines the following safety performance indicator, following agreement with the State's civil aviation oversight authority: 10 unstable (or nonconforming) approaches per 1000 landing operations in aerodromes of the network served by non-precision approaches. Subsequently, the aircraft operator defines the following safety performance target, following agreement with the State's civil aviation oversight authority: within the next three years, reduce by fifty percent the number of unstable (or nonconforming) approaches per 1000 landing operations in aerodromes of the network served by non-precision approaches. The safety requirement to achieve the safety performance indicators and safety performance targets discussed above would be as follows: development of constant descent angle (CAD), GPS approaches in aerodromes of the network served by non-precision approaches.

6.6.15 A ATS provider has identified airport operations safety as one major safety concern to be addressed by its SMS, it has identified, though the safety risk management component of its SMS, a concern regarding runway incursions, and defined the following safety performance indicator: 0.8 Cat A and B (most serious) runway incursions per million operations through 2009. Subsequently, the ATS provider defines the following safety performance target: by 2010 reduce Cat A and B (most serious) runway incursions to a rate of not more than 0.5 per million operations.

6.6.14 The definition of safety performance of an SMS is a requirement that goes above and beyond regulatory compliance with national and international requirements. Establishing safety performance for an SMS does not replace legal, regulatory, or other established requirements, nor does it relieve service providers from their obligations under relevant national regulations, and those arising from the Convention on International Civil Aviation (ICAO Doc 7300) and its related provisions contained in the Annexes to the Convention Aviation.

6.6.15 As conclusion to the discussion on safety performance, Figure 6-3 summarises, in graphical format, the concepts discussed under this section.


Figure 6-3 – Service provider' SMS – Safety performance

## 6.7 MANAGEMENT ACCOUNTABILITY

6.7.1 The third and last group in the ICAO safety management requirements in Annexes 1, 6, 8, 11, 13 and 14 refers to management accountability vis-à-vis the management of safety during provision of services. The ICAO requirements dictate that an accepted safety management system shall clearly define lines of safety accountability throughout the approved training organizations that are exposed to safety risks during delivery of services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, including direct accountability for safety on the part of senior management.

6.7.2 The contribution of management to the management of safety is discussed in Chapters 3 and 8, and no further discussion is considered necessary. Mention must be made, however, to a language issue: the use of the term *accountability* in the ICAO safety management requirements. In English language, the notion of *accountability* is different to the notion of *responsibility*. The latter refers to the situation where a person must execute specific actions, while the notion of accountability extends this to the obligation or willingness to assume the responsibility for the execution of such actions. To express it safety management terms, *safety responsibilities* are those duties which describe the safety purpose of what an individual is required to do. *Safety accountabilities* are statements of what the individual is required to deliver, either directly or through supervision and management of others, including those to whom the individual has delegated responsibility. There is clearly a significant difference between both terms. However, this is a nuance that exists only in the English language. Therefore, the term *responsibility* in regards to management in the ICAO safety management requirements, as included in other than the English language version of Annexes 1, 6, 8, 11, 13 and 14, must be understood in the sense of the English term *accountability*.

6.7.3 Successful safety management requires the active participation of all levels of management and supervision. This should be reflected in the structure of the organization and in published safety accountabilities. The organization should define, document, and communicate – with the aid of organizational diagrams or charts – responsibilities, accountabilities, and authorities. Senior management accountability and functional responsibilities are further discussed in Chapter 8.

## 6.8 SSP – SMS RELATIONSHIP

6.8.1 A clear understanding of the relationship between an SSP and an SMS is essential for concerted safety management action within States. This relationship can be expressed in the simplest terms as follows: States are responsible for developing and establishing an SSP, service providers are responsible for developing and establishing an SMS. This is a very important point: States are not expected to develop an SMS; rather the SSP fulfils the equivalent role. Nevertheless, States are responsible, as part of the activities in its SSP, to accept and oversee the development, implementation and

operational performance of the service providers SMS. In overseeing the safety performance of a service provider's SMS, the notion of ALoS of the SSP, discussed in paragraph 6.6 hereunder, plays a fundamental role in the relationship between an SSP and an SMS. The relationship between an SSP and an SMS is further illustrated in Figure 6.4, and is further discussed in Chapter 11.

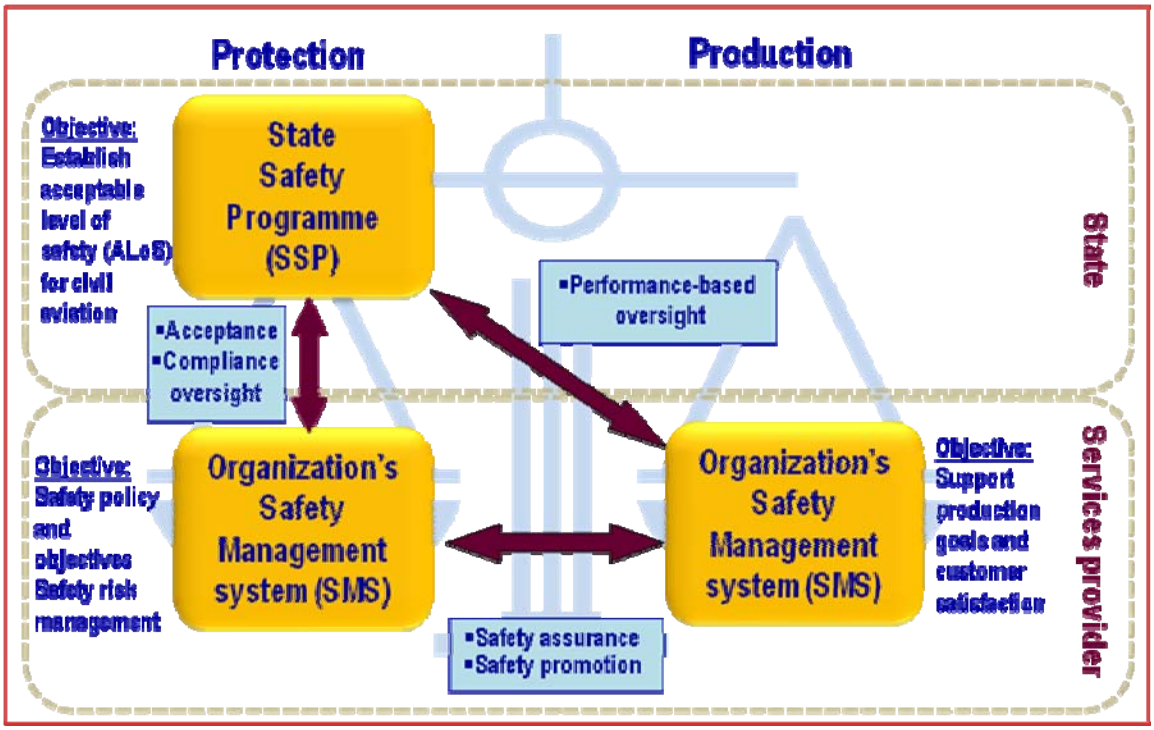



Figure 6-4 – SSP-SMS relationship

6.8.2 Chapter 3 discusses a potential management dilemma that may arise when considering the management of safety as an organizational process, and safety management as a core business function. Such potential dilemma, presented as the "dilemma of the two Ps" provides an appropriate background to explain the relationship between an SSP and an SMS.

6.8.3 The SSP is situated on the protection side of the balance mediating between protection and production in Figure 6-4. The SSP aims at ensuring public safety by controlling safety risks at a State level. An SSP has no production objectives, as such. Although efficiency is expected from State's aviation organizations, they have no specific deliverables in terms of products or services aimed at making a profit. The basic objective of a State, through its SSP, is to ensure to the extent possible public safety during service delivery by service providers. This objective is achieved by defining ALoS for the SSP, and through the control of safety risks within the State by the two "operational components" of the SSP: safety risk management and safety assurance.

6.8.4 A service provider SMS is only partly situated on the protection side of the balance since, unlike the State, a service provider has specific deliverables in terms of products or services aimed at making a profit. The objective of a service provider SMS is, in terms of protection, the control safety risks that are a consequence of activities and processes related to the delivery of the products or services that the organization specialises in. The service provider achieves the control of safety risks during service delivery mainly through the two "operational components" of the SMS: safety risk management and safety assurance, with safety policy and objectives and safety promotion playing a supporting role yet important role.

6.8.5 The State, as part of its SSP, initially accepts a service provider SMS. This acceptance is mostly prescriptive: the State, most likely through its civil aviation oversight authority, will verify that the components and elements proposed by the service provider SMS comply with existing regulations and directives promulgated by the State. It is important to note that acceptance is mostly an administrative process: the State approves a blueprint of a management system and a plan for action for its development and implementation. In simple language, acceptance means mostly "ticking boxes". But acceptance, while ensuring regulatory compliance, does not guarantee proper SMS performance. Compliance acceptance and oversight is indicated by the vertical arrow linking the SSP and the SMS in Figure 6-4. The way for the State to ensure proper SMS performance (i.e., that the SMS really works) would be to oversee it during actual performance of the activities aimed at delivery of services.

6.8.6 In order to verify SMS performance, the civil aviation oversight authority of the State has to conduct oversight of its performance on a periodic basis, during the course of activities aimed at delivery of services. This would prove to be difficult if not impossible in practice, hence the safety performance indicators and safety performance targets of an SMS. While compliance acceptance and oversight as discussed in 6.8.5 above is prescriptive-based, oversight of safety performance indicators and targets is performance-based. The notion safety performance discussed in section 6.6 thus extends to a service provider SMS the notion of ALoS of an SSP discussed in section 6.4 . Safety performance is to an SMS what ALoS is to an SSP.

6.8.7 Safety performance measurement of an SMS includes the definition of safety performance indicators, safety performance targets and safety requirements. These key, agreed indicators and targets are representative of the generic hazards in the operational context in which the service providers conducts activities related to delivery of services, and provide a performance-based oversight process with a fair picture of the performance of the SMS. By defining a prioritised set of short-term and medium-term safety objectives specific to the particular service provider operation, by implementing mitigation strategies against the safety risks of the consequences of the hazards underlying the specific safety objectives, and by establishing metrics and timelines that allow measurement of the effectiveness of the mitigation strategies, the service provider is providing the oversight authority with measurable means to verify SMS safety performance – or its lack thereof – beyond regulatory compliance.

6.8.8 Shifting the discussion to the production side of the balance mediating between protection and production in Figure 6-4, an SSP, as already discussed, has no production objectives as such, but a service provider certainly does. The objective of the production activities of a service provider is to achieve commercial goals and deliver customer satisfaction. The SMS is the means the service provider utilises to ensure that the safety risks of the consequences of the hazards it must face while pursuing production objectives remain under organizational control. The service provider SMS identifies safety risks and the mitigations necessary to keep them under organizational control through safety risk management initially. Once operations start, control of safety risks and monitoring of mitigations is accomplished through the continuous process of safety assurance, supported by safety promotion. Safety risk management, safety assurance and safety promotion thus provide the means for an organization to maintain the balance between production and protection.

6.8.9 While the traditional role of a State is represented in the protection side as it pertains to the acceptance of the SMS and its administrative oversight in terms of regulatory compliance, under the SSP there is a role for the oversight function in the production side as well. Deficiencies in hazard identification and safety risk management, as well as in the development of mitigation strategies, are often related to allocation of resources. This is usually the case where allocation of resources is biased towards production activities. Deficiencies in hazard identification and safety risk management, as well as in the development of mitigation strategies will also be made evident by the inability to meet the agreed safety performance of the services provider's SMS, because of an imbalanced allocation of resources to production and protection. Therefore, in exercising performance-based oversight as described in paragraph 6.8.7, in overseeing SMS operational performance against agreed SMS' safety performance specific to the service provider, biases in the allocation of resources as well as safety performance of the SMS as a whole will become obvious: lack of resources will lead either non-identification of safety hazards, to flawed safety risk management, and consequently to poor safety performance of the SMS. In such case, although perhaps regulatory-compliant, the service provider SMS will not be effective. Performance-based acceptance and oversight is represented in Figure 6-4 by the diagonal arrow linking the SSP and the organization production processes.

## 6.9 COMPLIANCE AND PERFORMANCE

6.9.1 The justification for the implementation of safety management practices through the SSP and the SMS is the growing conviction within aviation about the need to complement the existing compliance-based approach to safety with a performance-based approach, with a view of achieving a realistic implementation of both the SSP and the SMS. The subject has already been discussed in this chapter under the SSP and its companion ALoS. This section presents a summary conclusion, highlighting the significant points.

6.9.2 The quest for safety management and a performance-based approach to safety is based upon the deployment and effective utilization of safety risk controls. From the perspective of the State, the most effective safety risk controls at its disposal are safety regulations.

6.9.3 In a compliance-based safety environment, the approach to safety management is rigid and prescriptive, as discussed in Chapter 3 as well as in this chapter. In a compliance-based safety environment, safety regulations are used as **administrative controls.** A strict -framework is supported by inspections and audits with one exclusive objective: regulatory compliance.

6.9.4 In a performance-based safety environment, the approach is flexible and dynamic. In such an environment, safety regulations are used as **safety risk controls.** A regulatory framework in which regulations are developed in response to and as controls to safety risks is implemented, and oversight of compliance with the regulatory framework is supported by

safety data-based identification and prioritization of safety risks, with two objectives: regulatory compliance, but most importantly, verification of effective safety performance.


Figure 6-5 – SSP – Prescription versus performance

6.9.5 In a performance-based safety environment, there is a need to define a set of **measurable performance objectives** to determine whether an SSP or an SMS is operating in accordance with design expectations, beyond regulatory compliance. Measurable performance objectives permit to assess the actual performance of activities critical to safety against existing organizational controls so that necessary corrective or preventive action taken and safety risks can be maintained as low as reasonably practicable (ALARP).

6.9.6 The notions of ALoS for the SSP and of safety performance for the SMS are essential ingredients of the effective operation of both an SSP and SMS. They provide the foundations for a performance-based regulatory environment, in order to monitor the actual performance of an SSP or SMS, beyond regulatory compliance. Only through the establishment and measurement of specific safety performance objectives – through assurance of effective safety performance of an SSP/SMS – can the objective of continuous improvement of safety performance underlying an SSP/SMS be achieved.

6.9.7 The safety performance indicators and safety performance targets provide a measurable way of ensuring and demonstrating the effectiveness of an SSP or an SMS, beyond regulatory compliance. Regulatory compliance still remains at the foundations of safety management for the State as well as for service providers. Figures 6-4 and 6-5 build upon the examples of safety performance indicators, safety performance targets and safety requirements of and SSP and an SMS discussed in this Chapter, to illustrate where and how prescription and performance fit within an SSP and an SMS.

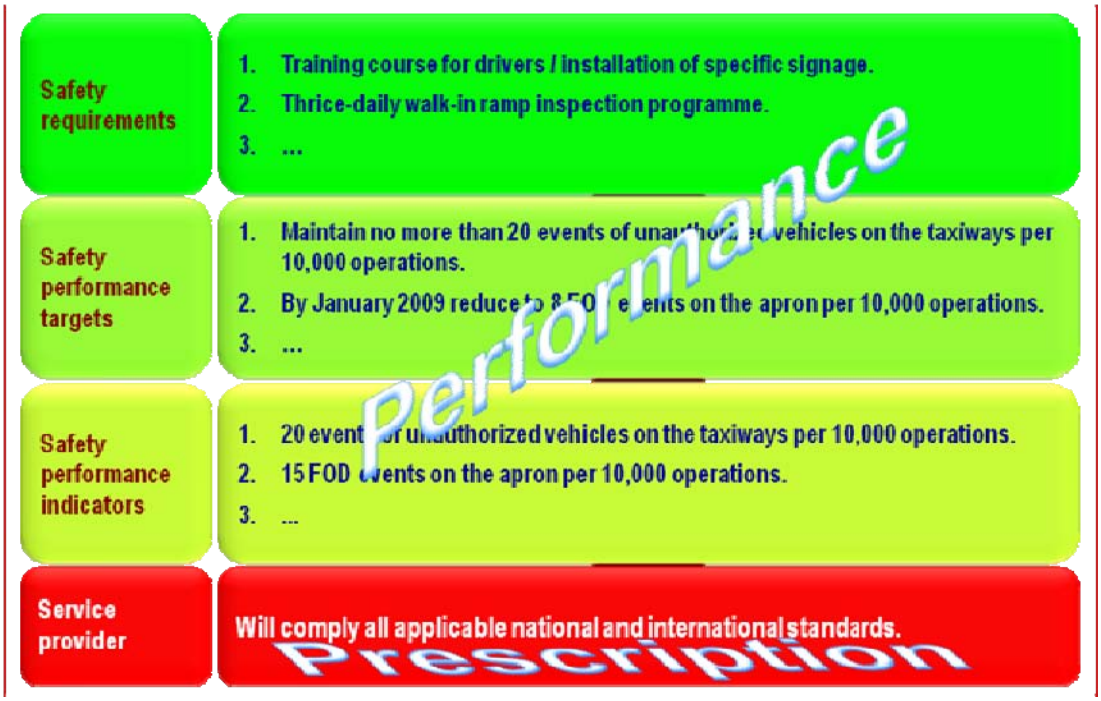



Figure 6-6 – SMS – Prescription versus performance

6.9.8 In summary, in accordance to the ICAO harmonised safety management requirements:

- States shall establish a State safety programme (SSP), in order to achieve an acceptable level of safety (ALoS) in civil aviation.
- The acceptable level of safety (ALoS) to be achieved shall be established by the State.
- Service provides shall implement a safety management system (SMS) that:
  - Identifies safety hazards;
  - Ensure ensures remedial action to maintain safety performance;
  - Provides continuing monitoring and regular assessment of the safety performance; and
  - Aims at a continuous improvement of the overall performance of the SMS.

- - - - - - - - - - - - - - -

# Chapter 7

# INTRODUCTION TO SAFETY MANAGEMENT SYSTEMS (SMS)

## 7.1 OBJECTIVE AND CONTENTS

7.1.1 This chapter describes the basic features of safety managements systems (SMS), and discusses the role and importance of properly describing the system (system description) and conducting a gap analysis before starting the SMS implementation process. The chapter also discussed the relationship between SMS and quality management systems (QMS). The chapter includes the following:

- Introductory concepts
- SMS features
- System description
- Gap analysis
- SMS and QMS
- SSP/SMS and the accident investigation process
- Management systems integration
- Clarifying terms
- Clarifying slogans

## 7.2 INTRODUCTORY CONCEPTS

7.2.1 An SMS can be likened to a toolbox. It is a toolbox that contains the tools that an aviation organization needs to be able to control the safety risks of the consequences of the hazards it must face during the delivery of the services that are the reason why the organization is in business. In many cases the organization itself generates the hazards during service delivery. It is important to acknowledge that SMS itself is neither a tool nor a process. SMS is the actual toolbox, where the actual tools employed to conduct the two basic safety management processes (hazard identification and safety risk management) are contained and protected. What an SMS does for an organization is providing a toolbox that is appropriate, in size and complexity, to the size and complexity the organization.

7.2.2 As a toolbox (Figure 7-1), SMS ensures that when specific tools are needed for hazard identification and safety risk management, (a) the right tools for the task at hand are available for the organization to use, (b) tools and task are properly related, (c) the tools are commensurate to the needs and constraints of the organization, and (d) the tools can be easily found within the tool box, without unnecessary waste of time or resources. This perspective is important, because SMS simply is a protective shell that ensures proper and timely storage, availability and utilization of the tools needed to deliver specific safety management processes in the organization. Without the proper tools inside, SMS is only an empty shell.

7.2.3 Chapter 3, in its closing summary, sketches several characteristics or distinguishing features of safety management. One important characteristic is that safety management is not circumscribed to just one specific activity of the organization, generally the most conspicuous (for example, flight operations in an airline), that might generate hazards. Safety management addresses all the operational activities of the entire organization. The scope of SMS, therefore, encompasses most of the activities of the organization, and certainly all operational activities that support delivery of services and contain the potential to generate hazards. The scope of an SMS directly includes operations, maintenance, repair, support services, training and checking and other operational activities. The scope of an SMS indirectly includes, as appropriate and relevant for service delivery, other organizational activities that support operational activities, such as finance, human resources, legal and so forth, as discussed in Chapter 2.


Figure 7-1 – SMS – A toolbox

7.2.4 SMS must start from senior management. This is neither a rhetorical nor a philosophical statement, but one which is grounded on very concrete reasons. The management of safety as a core business function of an organization requires, just like any other core business function, resources. The allocation of resources is eminently a function of senior management, in that senior management has both the authority and the responsibility for resource allocation. If senior management is not appraised of role and objectives of the organization's SMS or involved at an appropriate level in the organization's SMS, then senior management shall not have an appreciation of the extent of the threat that safety risks represent to the capabilities of the organization. Without such appreciation, allocation of resources may fall short of real needs. In other words, the "dilemma of the two Ps" discussed in Chapter 3 will likely surface and remain unresolved.

7.2.5 SMS aims to make continuous improvement to the overall level of safety of an organization. In accordance with the nature of safety management as a core business function, SMS involves non-stop, daily hazard identification, safety data collection and analysis, safety risks estimation, and implementation of mitigation strategies. There is no specific point at which the operation of an SMS stops or slows down. An SMS operation is a constant, never-ending vigil that aims at maintaining and, if possible, raising the safety bar to levels that are commensurate with the organization's strategic objectives and supporting core business functions. In this sense, SMS proposes a profound difference with the traditional notion of accident investigation, in which the activity was mostly restricted to wait for the "bad news", extract as many safety lessons as possible from them, and distribute the safety lessons to prevent similar accidents. SMS actively looks for trouble, continuously searches for bad news, to contain trouble and bad news before they hit the organization by surprise.

7.2.6 All aviation stakeholders contribute and play a role in SMS. This, again, is neither a rhetorical nor a philosophical statement, but it is also grounded on very concrete reasons. It is important to identify and involve aviation system stakeholders to ensure that stakeholders' inputs and knowledge relevant to safety risk(s) decisions are taken into consideration before such decisions are taken.

7.2.7 Furthermore, given the breadth of activities an SMS encompasses, and the broad-ranging nature of these activities, multi-sectarian input to the safety risk decision making process is essential. The following list provides an example of different stakeholders that at different times might be called upon to assist or provide input to the decision making process on safety risks:

- Aviation professionals;
- Aircraft owners and operators;
- Manufacturers;
- Aviation regulatory authorities;
- Industry trade associations;
- Regional air traffic service providers;
- Professional associations and federations;

- International aviation organizations;
- Investigative agencies; and
- The flying public.

7.2.8 Stakeholders can assist organizational decision-makers by ensuring that communication about the safety risk(s) under consideration takes place early, and in a fair, objective and understandable way. For safety communication to be credible, it must be consistent with the facts, with previous statements from management and with the messages from other authorities. These messages need to be expressed in terms the stakeholders can understand.

## 7.3 SMS FEATURES

7.3.1 Three features characterise an SMS:

a) Systematic;

b) Proactive; and

c) Explicit.

7.3.2 An SMS is *systematic* because safety management activities are in accordance with a pre-determined plan, and applied in a consistent manner throughout the organization. A long-range plan to keep the safety risks of the consequences(s) of hazards under control is developed, approved, implemented and operated on a non-stop, daily basis. As consequence of its systematic and strategic nature, SMS activities aim at gradual but constant improvement, as opposed to instant dramatic change. The systematic nature of SMS also leads to a focus on processes rather than outcomes. Although outcomes (i.e. adverse events) are duly considered to extract conclusions that support the control of safety risks, the main focus of SMS is the capture of hazards, which are the precursors to outcomes, during the course of the routine operational activities (processes) that the organization engages into during delivery of services.

7.3.3 An SMS is *proactive* because it builds upon an approach that emphasizes hazard identification and safety risk control and mitigation, before events that affect safety occur. It involves strategic planning seeking to keep safety risks under the constant control of the organization, instead of engaging in repair action when experiencing an adverse event, and then reverting to a "sleep mode" until the next adverse event is experienced and repair action is re-engaged. In order to sustain effective hazard identification, constant monitoring of operational activities necessary for the provision of services is conducted. This in turn allows for collection of safety data on hazards, allowing data-driven organizational decisions on safety risks and their control, as opposed to formulating decisions on safety risks based on opinion or, even worst, on bias or prejudice.

7.3.4 Lastly, an SMS is *explicit* because all safety management activities are documented, visible and, therefore, defensible. Safety management activities and the ensuing safety management know-how of the organization are formally recorded in official documentation, that is available for anyone to access to. Thus, safety management activities are transparent. In this respect, the "safety library" discussed in Chapter 4 plays a fundamental role in ensuring that safety management activities and know-how are documented in formal organizational structures and do not reside in the heads of individuals. An organization that allows a situation to develop where safety management activities and know-how reside in the heads of individuals exposes itself to a highly volatile situation in terms of preservation of safety activities and know-how.

## 7.4 SYSTEM DESCRIPTION

7.4.1 A system description is the first prerequisite to the development of an SMS. Chapter 2 discusses the interrelationship among people, context and safety in aviation environments. The discussion proposes that the sources of safety vulnerabilities during the delivery of services are found in mismatches in the interface between people and the other components of the operational context in which people conduct their service-delivery related activities. Potential safety vulnerabilities as consequence of the interactions between people and other components of the operational context can specifically be characterised in terms of hazards, which have identifiable and controllable elements. Hazards are unique components of production systems, and most hazards unleash their damaging potential as a consequence of operational interactions among the different components of the system.

7.4.2 A simple example follows. Fuel is a component of the aviation system and, just like any source of energy, a hazard. While it is stored in underground tanks, untouched, the probability of fuel as a hazard unleashing its damaging potential is low. Aircraft are also components of the aviation system. People must fuel aircraft. During fuelling operations by people (an operational interaction essential for service delivery) the damaging potential of fuel as a hazard increases significantly. Fuelling procedures are then implemented to bring the safety risks of fuelling operations under organizational

control. These procedures are based on the identification and control of the elements of the hazard. The identification of the elements of hazards and, to a large extent, the control, relies as first and essential step in the system description.

7.4.3 The example used in Chapter 2 to explain the interrelationship among people, context and safety in aviation environments is also useful to explain a system description.

7.4.4 Figure 7.2 depicts an environment in which a service delivery activity takes place. The service in question is the delivery of small packages to the other side of the mountains by people (the caveman). The combination of people involved in service delivery, the tools and means that the people will utilise, and the features of the environment constitutes the operational context in which the service delivery activity will take place. The system in question is a socio-technical system (i.e. a system that combines people and technology) for delivery of packages. Since the sources of safety vulnerability are specifically characterised as hazards that can be found in mismatches in the interface between people and other components of the operational context in which people conduct their service-delivery related activities, the first step in identifying such mismatches is describing the system in terms of components and their interactions.

7.4.5 A description of this system in term of its components and their interactions, utilising the SHEL(L) model discussed in Chapter 2 as an aid, could be as follows. The function of the socio-technical system is package delivery. It interfaces with other systems: a topographical system, a weather system, a wildlife system. There is a social component: people. There are human performance considerations which are fundamental for system operation: how will people perform when interacting with the lions, with the mountains and with the weather. There are hardware components in the system: the road across the mountains, the warning signs. There are also software components: documentation, procedures and training to guide people in the operation and interaction with the system (how to deal with the lions, how to negotiate the curves in the road, how to protect against the weather) while at the same time ensuring service delivery (packages must be delivered intact at the other side of the mountain).

7.4.6 In formal or technical terms, a system description in aviation should include the following:

- the system interactions with other systems in the air transportation system;
- the system functions;
- required human performance considerations of the system operation;
- hardware components of the system;
- software components of the system, including related procedures that define guidance for the operation and use of the system;
- the operational environment; and
- contracted and purchased products and services.

7.4.7 Appendix 1 to this chapter provides guidance on system description.

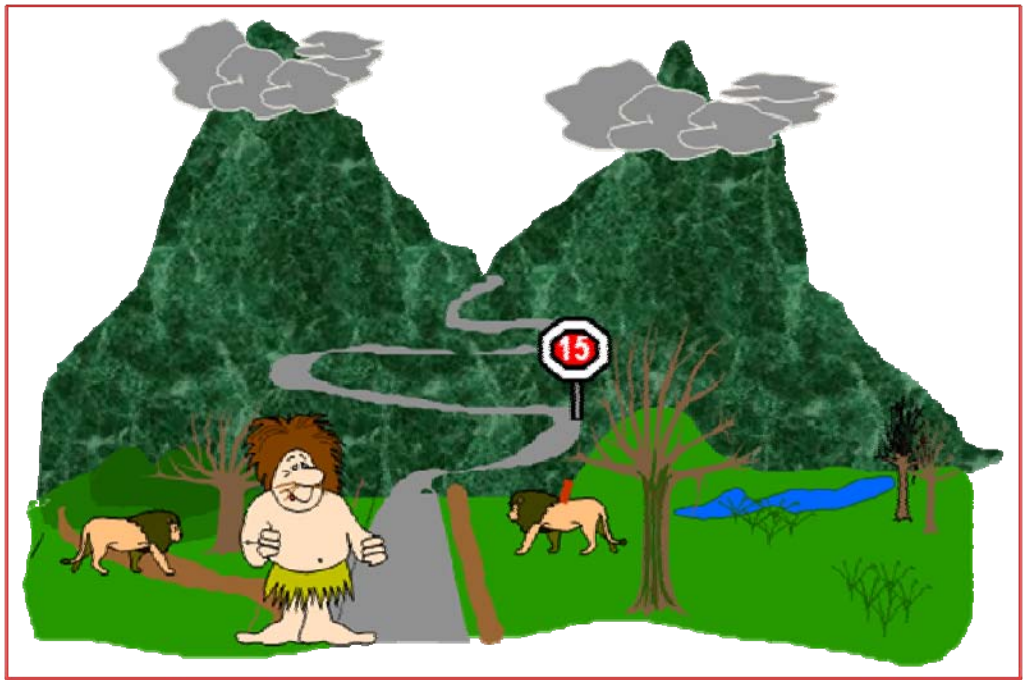



Figure 7-2 – System description

## 7.5 GAP ANALYSIS

7.5.1 The first step in identifying sources of safety vulnerability specified as hazards in the interfaces between people and other components of the system is the system description. Once the system is described in term of components and interactions, the second step is to address safety vulnerabilities specified as hazards in the interfaces between people and other components of the system by an analysis of the resources already present in the system. The analysis has two objectives: first, to identify eventual mismatches in the interfaces between the different components identified through the system description. These mismatches are safety vulnerabilities. Second, to identify whatever additional resources might be considered necessary to smooth rough interfaces, to assist people involved in delivery of services in safely and efficiently discharging their tasks. This analysis is known as gap analysis.

7.5.2 From the perspective of SMS, a gap analysis is basically an analysis of the safety arrangements existing within the organization. The gap analysis is important because the basic organizational structures necessary to start developing an SMS may exist in the organization: it will seldom be necessary to start to build an SMS from scratch, because most organizations will have in place and functioning various activities related to an SMS. The development of SMS should take advantage of and build upon existing organizational structures.

7.5.3 Returning to Fig 7-2, and keeping in mind that the service provided by the system is the delivery of small packages at the other side of the mountains by people, a simple gap analysis is exemplified. The guiding question for the analysis should be: are the operational personnel (in this case, the caveman) who are actually going to deliver the service properly equipped with the necessary resources to do so? The reply to these question must address both safety (i.e. is personnel properly equipped to deliver the service *safely*?) and efficiency (i.e. is personnel properly equipped to deliver the service *efficiently*?)


Figure 7-3 – Gap analysis

7.5.4 The SHEL(L) Model, discussed in Chapter 2, is a useful tool to reply the question and guide the gap analysis. The caveman is the Liveware (L). The road, the STOP sign and the speed sign, and the tunnel near the top of the mountain pass are the Hardware (H). The trees, the lions, the mountains and the clouds are the Environment (E). Although not visible, the training the caveman has received and the procedures and instructions he must follow to deliver the service are the Software (S). As shown in Figure 7-3, the gap analysis would produce the following results when compared to Figure 7-2:

- The caveman must travel though the mountain, in a circuitous and probably uneven road, but he is barefooted. He might therefore hurt his feet and experience a fall (safety) and/or make progress at a slow pace and therefore delay the delivery of packages (efficiency). The gap analysis suggests that providing footgear would then be important to address a mismatch in the interface between the caveman (L) and the road (H).
- The clouds in the pass at the top of the mountains may generate rain and thunderstorms. Providing headgear would then protect the caveman, and address a mismatch in the interface between caveman (L) and the clouds (E).
- The lions are a clear hazard to the caveman and to the delivery of the service. The STOP sign is a resource that already exists in the system, intended to alert the caveman about the hazard (i.e. entering a particularly dangerous zone). Nevertheless, a self-defence tool would be an appropriate additional resource. Proving a spear for the caveman would therefore address a mismatch between the caveman (L) and the lions (E).
- In addition to the STOP sign, yellow “hold” lines painted in the road just before entering the particularly dangerous zone would increase awareness and direct the attention of the caveman towards the lions, thus supplementing the spear as an additional resource to address the mismatch between the caveman (L) and the lions (E).
- The caveman has no equipment to carry the small packages, so that his hands are free to handle the spear as well as to maintain better balance and stability while travelling in the rough and uneven mountain road. A backpack to carry the packages would be an additional resource to address a mismatch in the interface between the caveman (L) and the lions (E) and the caveman (L) and the road (H).

- There is a speed sign that indirectly alert travellers the beginning of a winding road. The speed sign does not convey an unequivocal message about the upcoming road conditions. A dedicated and obvious alerting sign is an additional resource to address a mismatch in the interface between the caveman (L) and the road (E).
- There is no warning that the pass at the top of the mountain is through a tunnel. An alerting sign is an additional resource to address a mismatch in the interface between the caveman (L) and the road (E).
- Etc.

7.5.5 A gap analysis thus reveals the resources, structures and safety arrangements existing in the system to address safety vulnerabilities specified in terms of hazards, that arise as a consequence of the interaction of people and other components of the operational context. It also reveals additional resources, structures and safety arrangements that would be necessary to mitigate safety vulnerabilities and increase operational resilience to hazards.

7.5.6 Once the gap analysis is complete and fully documented, the resources, structures and arrangements that have been identified as missing or deficient will form, together with those already existing, the basis of the SMS implementation plan. Organizations may format their SMS implementation plan to suit their individual needs, however, a spreadsheet format, Gantt chart or MS Project type layout is recommended for ease of viewing and tracking. Each item will be assessed to determine how the organization will create or modify policies, objectives, procedures or processes to incorporate the required SMS components and elements. Appendix 2 to this chapter provides an example of a gap analysis for service providers with suggested questions to assist an organization in finding out what is missing when they have described their own system in the organization.

## 7.6 SMS AND QMS

7.6.1 Quality management has been established in many segments of the aviation system for a long time. Many aviation organizations have implemented and operated quality control (QC) and/or quality assurance (QA) for a number of years.

7.6.2 A QA programme defines and establishes an organization's quality policy and objectives. It ensures that the organization has in place those elements necessary to improve efficiency and reduce service-related risks. If properly implemented, a QA ensures that procedures are carried out consistently and in compliance with applicable requirements, that problems are identified and resolved, and that the organization continuously reviews and improves its procedures, products and services. QA should identify problems and improve procedures in order to meet corporate objectives.

7.6.3 The application of QA principles to safety management processes helps ensure that the requisite system-wide safety measures have been taken to support the organization in achieving its safety objectives. However, QA can not, by and in itself and as proposed by quality dogma, "assure safety". It is the integration of QA principles and concepts into an SMS under the safety assurance component (discussed in Chapter 9), that assists an organization ensuring the necessary standardization of processes to achieve the overarching objective of managing the safety risks of the consequence(s) of hazards the organization must confront during the activities related to the delivery of services.

7.6.4 QA principles include procedures for monitoring the performance of all aspects of an organization, including such elements as:

a) design and documentation of procedures (e.g. SOPs);

b) inspection and testing methods;

c) monitoring of equipment and operations;

d) internal and external audits;

e) monitoring of corrective actions taken; and

f) use of appropriate statistical analysis, when required.

7.6.5 A few aviation organizations have integrated their QC and QA programmes into what is called quality management systems (QMS). A number of internationally accepted standards regarding quality assurance are currently in use. The standards of choice depend on the size, complexity and the product of the organization. Standard ISO 9001-2000, for example, is one set of international standards developed by ISO and used by many organizations to implement an in-house quality management system. Using such systems also ensures that the organization's suppliers or contractors have appropriate quality management systems in place.

7.6.6 In view of the long history of QA/QC in aviation, the relative youth of SMS and the fact that specific SMS processes nurture on quality principles, the potential for misperceptions and misunderstandings in the relationship between SMS and QMS is real. It is thus essential to define this relationship from a synergistic rather than antagonistic perspective, and the relative contribution of SMS and QMS to the attainment of overall organizational goals, and in particular to the organization's safety goals.

7.6. 7 It is accurate to say that SMS and QMS share many commonalities. They both:

a) have to be planned and managed;

b) depend upon measurement and monitoring;

c) involve every function, process and person in the organization; and

d) strive for continuous improvement.

7.6.8 Because SMS and QMS share many commonalities, there might be a tendency to assume that an organization that has established and operates a QMS does not need, or already has, an SMS. However, in the same way that SMS and QMS share commonalities, there are important differences between both, as well as shortcomings in the effectiveness of QMS to achieve by itself the overarching objective of managing the safety risks of the consequence(s) of hazards the organization must confront during the activities related to the delivery of services.

7.6.9 Quality management was introduced in the 1960s, when understanding of human performance, organizational factors and their impact in safety was far less developed than today. Therefore, notwithstanding modifications and continuous updating over time, quality management is less effective at identifying high-level/high-consequence problems such as the complex latent failure pathway that can lead to disaster. Furthermore, the bureaucracy of auditing and the process of attaining formal quality accreditation have all the potential of becoming end in themselves: the objective of hanging a banner with an ISO accreditation under the entrance of corporate headquarters may distract from the generation of safety practices and lead to a loss of focus, safety-wise.

7.6.10 SMS focuses on human performance, Human Factors and organizational factors, and integrates into these, as appropriate, quality management techniques and processes to contribute to the achievement of safety satisfaction. The objective of SMS is to identify the safety hazards the organization must confront – and that in many cases it generates – during delivery of services, and to bring the safety risks of the consequences of these hazards under organizational control. In broad terms, the first imperative of this objective – hazard identification – is accomplished through the safety risk management component of an SMS (discussed in Chapter 9), which is based upon safety management principles and practices. The second imperative – bringing the safety risks under organizational control – is accomplished through the safety assurance component of an SMS (also discussed in Chapter 9), which is based upon the integration of safety and quality management principles and practices.

7.6.11 Succinctly, then, SMS differs from QMS in that:

- SMS focuses on the safety, human and organizational aspects of an organization (i.e. safety satisfaction); while
- QMS focuses on the product(s) and service(s) of an organization (i.e. customer satisfaction).

7.6.12 Once commonalities and differences between SMS and QMS have been established, it is possible to establish a synergistic relationship between both systems. It cannot be stressed strongly enough that the relationship is complementary, never adversarial, and it can be summarized as follows:

- SMS builds partly upon QMS principles;
- SMS should include both safety and quality policies and practices; and
- The integration of quality principles, policies and practices – insofar as SMS is concerned – should be focused towards the support of the management of safety.

7.6.13 Establishing a complementary relationship between SMS and QMS leads to establish also complementary contributions of each system to the attainment of the organization's safety goals:

- SMS results in the design and implementation of organizational processes and procedures to identify safety hazards and their consequences, and bring associated safety risks in aviation operations under the control of the organization;
- The integration of QMS into SMS provides a structured approach to monitor that processes and procedures to identify safety hazards and their consequences, and bring associated safety risks in

aviation operations under the control of the organization function as intended and, when they do not, to improve them.

7.6.14 It must be stressed that the ICAO safety management requirements included in Annex 1, Annex 6, Annex 8, Annex 11 and Annex 14 and discussed in Chapter 6 are limited to SMS. There are no ICAO requirements in the aforementioned Annexes in regard to QMS, with the sole exception of such a requirement for approved maintenance organizations (AMO) in Annex 6, Part I, Chapter 8.

## 7.7 SSP/SMS AND THE ACCIDENT INVESTIGATION PROCESS

7.7.1 Just like with the relationship between SMS and QMS, the relationship between - in this case - the SSP or an SMS, and the accident investigation process, and the role that the accident investigation process plays under a safety management environment, has been a matter of discussion within the safety community. While discussions have mostly focussed around the relationship between SMS and the accident investigation process, the SSP must unquestionably be part of the discussion. Just like the relationship between SMS and QMS, it can never be stated emphatically enough that the relationship between the SSP/SMS and the accident investigation process is one of absolute complementarities and synergy. They are all essential tools of a mature safety management process.

7.7.2 Under the safety management process, the daily activities involved in managing safety as yet another organizational process, as discussed in Chapter 3, are delivered by the SSP or an organization's SMS. An accident (or serious incident) represents the ultimate failure of the SSP or an SMS (or both), as the managerial systems guiding the activities necessary for managing safety in the State or in an organization respectively. When such ultimate failure occurs, the accident investigation process sets in motion to find out the reasons for the failure in the safety management activities, and to generate the necessary countermeasures so failure does not repeat. Thus, in a safety management environment, the accident investigation process plays a clear role, and brings a distinct contribution, as the goalkeeper, the ultimate custodian of safety in the aviation system, that deploys when all safety defences and barriers in the system have failed.

## 7.8 MANAGEMENT SYSTEMS INTEGRATION

7.8.1 Aviation organizations are oftentimes described as “a system of systems”. This is because aviation organizations must develop, implement and operate a number of different management systems to achieve their production goals through the delivery of services. Typical management systems an aviation organization might need to operate include:

- Quality management system (QMS);
- Environment management system (EMS);
- Occupational health and safety management system (OHSMS);
- Safety management system (SMS); and
- Security management system (SEMS).

7.8.2 There is a developing tendency in civil aviation to integrate all these different management systems. There are clear benefits in such integration:

a) Reduction of duplication and therefore of costs;

b) Reduction in overall organizational risks and increase profitability;

c) Balance of potentially conflicting objectives;

d) Elimination of potentially conflicting responsibilities and relationships; and

e) Diffusion of power systems.

7.8.3 However, there are different ways to integrate all these systems, and in particular to integrate SMS with other management systems in the operation of the organization. Aviation organizations should be encouraged to integrate their management system for quality, safety, security, occupational health and safety, and environmental protection management. This integration, however, is presently beyond the scope of the harmonized ICAO safety management requirements and of this manual.

## 7.9 CLARIFYING TERMS

7.9.1 In order to develop common understanding in the use of terminology related to different safety management activities which are carried out under the responsibility of service providers and/or the civil aviation oversight authorities, the following convention is intended to clarify three specific term as used in the context of this Manual:

- **Safety oversight** is what the State performs with regard to the operators/service providers' SMS;
- **Safety assurance** is what the State performs with regard to the safety performance of its SSP and operators/service providers perform with regard to the safety performance of their SMS, including monitoring and measurement; and
- **Safety audit** is what the State performs with regard to the structure of its SSP and the operators/service providers perform with regard to the structure of their SMS.

*Note – **Safety oversight audit** is what the ICAO USOAP performs with regard to the CAA's State Safety Programme (SSP) and its safety oversight capabilities in accordance with ICAO SARPs and related guidance material.*

## 7.10 CLARIFYING SLOGANS

7.10.1 There is a long established tendency in aviation to rely on slogans to create awareness about safety problems, a tendency that oftentimes confuses slogans with principles. There is a big difference between slogans and principles. The latter clearly enunciate precise guidance which is based in sound knowledge and provide all-encompassing statements of how to conduct a particular endeavour. The former articulate oblique reference which is based on conventional and sometimes questionable popular wisdom (folk knowledge), and more often than not are misleading representations of how to tackle an issue. It would appear beyond sensible reason to pursue a critical endeavour such as the management of safety, and the deployment of SSP/SMS based on "sloganism". However, the potential does exist. This section reviews and sets forth to destroy, mostly by applying the basic safety and safety management concepts discussed in Chapter 2 and 3, five of aviation's most cherished safety slogans:

- In aviation, safety is first.
- Safety is everybody's responsibility.
- If ain't broke, why fix it?
- If you believe safety is expensive, try an accident.
- 70% accidents are due to human error.

7.10.2 ***In aviation, safety is first.*** Organizations in production systems are formed to pursue – as the name clearly suggests – some production goal, such as manufacturing automobiles, extracting oil or, such as is the case in commercial aviation, transporting people and goods by air. Organizations in production systems need to make money as a consequence of their activities, so they can secure the necessary resources to continue pursuing their production goals. It is therefore hard to see how safety could possibly be the first priority in aviation; one would rather think that money is first. As discussed in Chapter 2, safety in aviation is a question of sensible, co-ordinated prioritization of production and protection goals, so that organizations in aviation can make money safely. However, the mix-up of priorities embodied by this slogan has occasionally led to aberrant endeavours. In fact, the most frequent argument advanced by pathogenic organizations when caught by adverse events is that, notwithstanding evidence to the contrary, they can not understand how the bad outcome in question could have possibly happened to them, since "in our company, safety is first". It is a matter of historical record that organizations which have hidden behind this slogan – and have not backed it up with appropriate action - are among the worst safety offenders in the trade.

7.10.3 ***Safety is everybody's responsibility.*** This slogan is a puzzling one. When we feel sick; we visit a physician. When we need legal counsel, we consult an attorney. If water does not come out of the faucet, we call the plumber. However, when facing safety problems, all of us in aviation presume to be subject-matter experts, particularly if we have some years of experience in the trade. The truth of the matter is that all this slogan does is blowing smoke, since only trained specialists can address present-day safety problems in a context-relevant, effective, efficient manner. The best run organizations in aviation have dedicated safety personnel, professionally qualified, with specific job descriptions and with defined responsibilities and organizational access. These professionals assume responsibility as the safety monitors of the organization. They coordinate plans to assess and reinforce the organization's intrinsic resistance to the potential hazards inherent to aviation, for the rest of the personnel to follow. They do not point fingers when they discover un-managed hazards and safety problems, but work on the documentation and description of the problems, as prerequisite for the development of solutions. Chapter 8 develops

these ideas in some depth. Pathogenic organizations dilute this responsibility among all sectors and all personnel, and as a consequence few, if any, take an active stance in safety matters. Blowing smoke is however convenient because it provides for a cover screen when the fallacy in this slogan is uncovered by the proverbial trail of wreckage. As it turns out to be, "everybody's" office at corporate headquarters is rather difficult to find in the aftermath of a bad outcome, and punishment of operational personnel is the inevitable follow up.

7.10.4 ***If ain't broke, why fix it?*** The proposal in this slogan is that there is no need to be concerned about safety as long as there are no accidents, that the system is safe as long as people are not hurt, metal is not bent, and the organization is not exposed to criticism and embarrassment. In other words, the slogan proposes that accidents – or their lack thereof – are reliable indicators of system safety. An alternative view to this school of thought proposes that, if structures and processes afforded by state-of-the-art knowledge are in place to keep the system under continuous surveillance for signals of hazards, accidents are unfortunate "noise in the system". Beyond other falsehoods underlying this slogan, as discussed in Chapter 3, waiting until the system breaks down before attempting to address safety deficiencies might turn out to be onerous beyond reason. Furthermore, when the system breaks down, human life is at stake, which raises ethical questions in relation to this approach. Since the financial and human costs associated with only undertaking remedial action after experiencing an accident are inevitably high, there are compelling economic and ethical reasons to fix the system before it breaks. However, too often is the case in aviation at large that we continue to wait until we experience accidents before we take mitigating action.

7.10.5 ***If you believe safety is expensive, try an accident***. The popular belief reflected by this slogan is that it is possible to anticipate all flaws in the system which might eventually lead to accidents, namely by observing professional behaviours, exercising discipline and adhering to the rules. Simply put, regulatory compliance and "going by the book" are guarantee enough for safety. Unfortunately – as the practical drift discussed in Chapter 3 illustrates – the real world does not work like this. It is possible – and sensible – to perform proactive checks of system performance and engage in proactive endeavours, in a similar manner as humans visit family physicians and engage in fitness programmes. As already mentioned, once state-of-the-art structures and processes are in place, accidents, like illness and death, become ultimately a matter of statistical chance. If the objective is to avoid accidents exclusively, organizations indulge themselves in gambling (and in the process delude themselves and their customers). If the objective is to monitor the processes engaged by the organization while pursuing its production goals in order to ascertain their intrinsic resistance to the hazards inherent to aviation, then organizations exercise management (of safety). Even if sound safety management is exercised, it is impossible to cancel all sources of hazards inherent to aviation. The window of opportunity for accident, small as it might be, will always be cracked open: accidents – like death – will periodically arrive. The window of opportunity will be almost closed if an "organizational fitness" programme is exercised, but if organizations aim exclusively at avoiding accidents, then maintaining the organizational fitness will not be promoted and safety indeed becomes an accident. Under a "fitness programme", accidents are noise in the system, and the record shows that quite healthy organizations manned by sensibly-trained personnel, equipped with resources commensurate to their production goals and with well-designed procedures can suddenly find themselves involved in nasty occurrences. By opposition, pathogenic organizations, with doubtfully-qualified personnel, seriously under-resourced, with substandard practices and a record of close-calls manage to stay away from harm's way simply because of luck.

7.10.6 ***Seventy percent of accidents are caused by human error***. This slogan has been saved for the end because it epitomises how misleading the arm-chair wisdom underlying slogans can be. Consider the aviation system: humans conceive the blueprint of the system, and once they are satisfied with what they conceived, they set forth to design it. Humans then build the system and when the system is functional, humans make it work. In order to exhibit the behaviours necessary to achieve the system's objectives, humans train other humans who are going to make the system work day after day. Humans make strategic and tactical decisions about system performance, and when hazards are identified, humans devise and deploy the necessary countermeasures to protect the system from such hazards. Simply put: humans design, manufacture, train, operate, manage and defend the system. Therefore, when the system breaks down, it is of necessity that human error is a foregone conclusion, that some human flaw of one kind or another must be underlying the occurrence. From this perspective and depending upon the level of observation, *one hundred percent* of accidents are arguably caused by human error.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 1 to Chapter 7

# GUIDANCE ON SYSTEM DESCRIPTION

## Introduction

A system description is the first prerequisite activity for the development of an SMS in an organization. Every system contains inherent potential safety vulnerabilities, which are characterised in terms of hazards. The hazard identification process can only identify hazards that come within the scope of the system description. The boundaries of the system, as per its formal description, must therefore be sufficiently wide to encompass all possible hazards that the system could confront or generate. In particular, it is important that the description includes the interfaces both within the system, as well as the interfaces with the larger systems of which the system being assessed is a part.

A detailed description of the system should include:

a) the purpose of the system;

b) how the system will be used;

c) the system's functions;

d) the system's boundaries and the external interfaces; and

e) the environment in which the system will operate.

The safety consequences of a potential loss or degradation of the system will be determined, in part, by the characteristics of the operational environment in which the system will be integrated. The description of the environment should therefore include any factors that could have a significant effect on safety. These factors will vary from one organization to another. They could include, for example, air and ground traffic characteristics, aerodrome infrastructure and weather-related factors. The description of the system should also address contingency procedures and other non-normal operations, for example, failure of communications or navigation aids. An example of a system description, in this case of an aerodrome, is detailed below.

## SYSTEM DESCRIPTION OF AN AERODROME

A system description of an aerodrome should include facilities, equipment, personnel, processes and procedures necessary for the operation of the aerodrome. The different functions may include:

1. **Operational management**

   **a)** Movement area access control;

   - Air
   - Land
   - Sea

   **b)** Aerodrome emergency planning;

   - Emergency procedures manual
   - Emergency simulation practices

   **c)** Rescue and fire fighting;

   - Capability
     - Equipment
     - Foam/water/dry powder discharge rate
   - Facility maintenance
   - Staff training and experience

- Equipment mobilization plan
- Reduction of capability (notice)
- Water hydrant system

d) Movement area inspection and maintenance;
   - Aerodrome manual
   - Inspection forms
   - Maintenance

e) Visual aids maintenance;
   - Inspections
   - Schedule

f) Construction management;
   - Control of works
   - Site management

g) Apron safety management, including vehicle traffic;
   - Rules and regulation for airside operations
   - Airside management
     - Airside vehicle management
     - Airside vehicle license
     - Vehicle examination
     - Safety specification
     - Aircraft servicing coordination
   - Equipment parking
   - Apron discipline
   - Push-back operations
   - Traffic signs and markings
   - Stand allocation
   - Aircraft damage control
   - Fuel spillage control
   - Vehicle and equipment damage control
   - Apron safety check lists including ramp activity audit and working on height
   - Contracted and sub-contracted activities

h) Wildlife hazard management;
   - Bird control management
   - Observation
   - Bird strike report management

i) Obstacle control;
   - Airport boundary

- Outside airport
- Runway strip
- Regulation and survey
- Approval of building construction under flight path

j) Disabled aircraft removal;

- Equipment compatible with aircraft type
- Maintenance for readiness
- Deployment scheme
- Establishment of outsourcing procedures / contact

k) Dangerous goods handling;

- Limitation of dangerous goods on aircraft
- Storage and loading
- Establishment of training programmes
- Acceptance of dangerous goods by operators
- Emergency response guidance for aircraft incidents involving dangerous goods

l) Low visibility and adverse weather operations; and

- Procedures
- Coordination with air traffic services
- Responsibility of organizations involved

m) Radio navigational aids installations and maintenance.

- NOTAMS

2. **Aerodrome management**

a) Slots negotiation and allocation;
b) Flight dispatch;
c) Follow-me guidance and marshalling;
d) Movement area management and stand allocation;
e) Low visibility operations CAT II and CAT III;
f) Control of traffic rules and licensing regulations; and
g) Cleaning, waste removal and pest control.

3. **Passenger terminal building management**

a) Management of passengers, baggage flows and facilities;
b) Passengers and public information;
c) VIP and CIP assistance;
d) Left luggage;
e) Porter assistance;
f) Trolleys management; and

g) Cleaning and pest control.

**4) Air traffic and aeronautical information and communications services**

a) Air traffic control (aerodrome control under low visibility operations);
b) Flight information and alerting services;
c) Aeronautical information services (International NOTAM office and pre-flight information service); and
d) Aeronautical telecommunications services.

**5) Safety and security management**

a) Implementation and monitoring of the SMS;
   - Safety manager
   - Hazard identification and assessment of the consequences
   - Risks assessment, control and mitigation
   - Safety assurance
   - Safety action groups
   - Safety management system manual (SMSM)
b) Implementation and monitoring of the security programme;
c) Implementation and monitoring of the aerodrome emergency plan (AEP); and
d) Process the applications for the issuance of access cards.

- - - - - - - - - - - - - - -

# Appendix 2 to Chapter 7

# GUIDANCE ON THE DEVELOPMENT OF AN SMS GAP ANALYSIS FOR SERVICE PROVIDERS

### Gap analysis

The implementation of an SMS requires a service provider to conduct an analysis of its system to determine which components and elements of an SMS are currently in place and which components and elements must be added or modified to meet the implementation requirements. This analysis is known as gap analysis, and it involves comparing the SMS requirements against the existing resources in the service provider.

This guidance provides, in checklist format, information to assist in the evaluation of the components and elements that comprise the ICAO SMS framework and to identify the components and elements that will need to be developed. Once the gap analysis is complete and documented, it will form one basis of the SMS implementation plan.

The gap analysis form included in this guide can be used as a template to conduct a gap analysis. Each question is designed for a "Yes" or "No" response. A "Yes" answer indicates that the service provider already has the component or element of the ICAO SMS framework in question incorporated into its system and that it either matches or exceeds the requirement. A "No" answer indicates that a gap exists between the component/element of the ICAO SMS framework and the system of the service provider.

*Note. – Within the context of this guidance the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.*

### ICAO SMS framework

The ICAO SMS framework consists of four components and twelve elements, and its implementation shall be commensurate with the size of the organization and the complexity of the services provided.

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

**SMS GAP ANALYSIS FOR SERVICE PROVIDERS**

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| Component 1 – SAFETY POLICY AND OBJECTIVES | | | |
| Element 1.1 – Management commitment and responsibility | | | |
| SMM (Doc 9859) Chapter 8 | Is there a safety policy in place? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapters 3 and 8 | Does the safety policy reflect organizational commitments regarding safety management? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapters 3 and 8 | Does the safety policy include a clear statement about the provision of the necessary resources for the implementation of the safety policy; | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapters 3 and 8 | Does the safety policy include the safety reporting procedures? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the safety policy clearly indicate which types of operational behaviours are unacceptable? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the safety policy include the conditions under which exemption from disciplinary action would be applicable? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Is the safety policy signed by the Accountable Executive? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Is the safety policy communicated, with visible endorsement, throughout the [organization]? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Is the safety policy periodically reviewed to ensure it remains relevant and appropriate to the [organization]? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Is there a formal process to develop a coherent set of safety objectives? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Are the safety objectives linked to the safety performance indicators, safety performance targets and safety requirements? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Are the safety objectives publicized and distributed? | ☐ Yes<br>☐ No | |
| Element 1.2 – Safety accountabilities | | | |
| SMM (Doc 9859) Chapters 8 and 10 | Has the [organization] identified an Accountable Executive who, irrespective of other functions, shall have ultimate responsibility and accountability, on behalf of the [organization], for the implementation | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| | and maintenance of the SMS? | | |
| SMM (Doc 9859) Chapter 8 | Does the Accountable Executive have responsibility for ensuring that the safety management system is properly implemented and performing to requirements in all areas of the [organization]? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the Accountable Executive have full control of the financial resources required for the operations authorized to be conducted under the operations certificate? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the Accountable Executive have full control of the human resources required for the operations authorized to be conducted under the operations certificate? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the Accountable Executive have direct responsibility for the conduct of the organization's affairs? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the Accountable Executive have final authority over operations authorized to be conducted under the operations certificate? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapters 8 and 10 | Has the organization identified the accountabilities of all members of management, irrespective of other functions, as well as of employees, with respect to the safety performance of the SMS? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Are the safety responsibilities, accountabilities and authorities documented and communicated throughout the [organization]? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Has the [organization] Included a definition of the levels of management with authority to make decisions regarding safety risk tolerability? | ☐ Yes<br>☐ No | |
| Element 1.3 – Appointment of key safety personnel | | | |
| SMM (Doc 9859) Chapter 8 | Has the organization appointed a qualified person to manage and oversee the day-to-day operation of the SMS? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the person overseeing the operation of the SMS fulfil the required job functions and responsibilities? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 8 | Are the safety authorities, responsibilities and accountabilities of personnel at all levels of the organization defined and documented? | ☐ Yes<br>☐ No | |
| Element 1.4 – Coordination of emergency response planning | | | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 8 | Does the [organization] have an emergency response/contingency plan appropriate to the size, nature and complexity of the organization? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the [organization] coordinate its emergency response/contingency procedures with the emergency/response contingency procedures of other organizations it must interface with during the provision of services? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the [organization] have a process to distribute and communicate the coordination procedures to the personnel involved in such interaction? | ☐ Yes ☐ No | |
| Element 1.5 – SMS Documentation | | | |
| SMM (Doc 9859) Chapters 4 and 8 | Has the [organization] developed and maintains a safety library for appropriate hazard documentation and documentation management? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 4 and 8 | Has the [organization] developed and maintains SMS documentation in paper or electronic form? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 7, 8 and 10 | Is the SMS documentation developed in a manner that describes the SMS and the consolidated interrelationships between all the SMS components? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 8 and 10 | Has the service provider developed an SMS implementation plan that ensures that the SMS meets the organization's safety objectives? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 8 and 10 | Has the SMS implementation plan been developed by a person or a planning group which comprises an appropriate experience base? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 8 and 10 | Has the person or planning group received enough resources (including time for meetings) for the development of the SMS implementation plan? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Is the SMS implementation plan endorsed by the senior management of the [organization]? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Is the SMS implementation plan regularly reviewed by the senior management of the [organization]? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 8 and 10 | Does the SMS implementation plan propose an implementation of the SMS in phases? | ☐ Yes ☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 8 | Does the SMS implementation plan explicitly address the coordination between the service provider SMS and the SMS of other organizations the [organization] must interface with during the provision of services? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Has the service provider developed a safety management system manual (SMSM) as a key instrument for communicating the organization's approach to safety to the whole [organization]? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the SMSM document all aspects of the SMS, including among others the safety policy, objectives, procedures and individual safety accountabilities? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the SMSM clearly articulate the role of safety risk management as initial design activity and the role of safety assurance as continuous activity? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Are relevant portions of SMS related documentation incorporated into approved documentation, such as Company Operations Manual, Maintenance Control/Policy Manual, Airport Operations Manual, etc, as applicable? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the service provider have a records system that ensures the generation and retention of all records necessary to document and support operational requirements? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Is the service provider records system in accordance with applicable regulatory requirements and industry best practices? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 8 | Does the records system provide the control processes necessary to ensure appropriate identification, legibility, storage, protection, archiving, retrieval, retention time, and disposition of records? | ☐ Yes ☐ No | |
| Component 2 –SAFETY RISK MANAGEMENT | | | |
| Element 2.1 – Hazard identification | | | |
| SMM (Doc 9859) Chapters 3 and 9 | Does the [organization] have a formal safety data collection and processing system (SDCPS) for effectively collecting information about hazards in operations? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 3, 4 and 9 | Does the [organization] SDCPS include a combination of reactive, proactive and predictive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 3, 9 and 10 | Does the [organization] have reactive processes that provide for the capture of information relevant to safety and risk management? | ☐ Yes ☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapters 9 and 10 | Has the service provider developed training relevant to reactive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 9 and 10 | Has the service provider developed communication relevant to reactive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is reactive reporting simple, accessible and commensurate with the size of the service provider? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 9 and 10 | Are reactive reports reviewed at the appropriate level of management? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a feedback process to notify contributors that their reports have been received and to share the results of the analysis? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 3, 9 and 10 | Does the service provider have proactive processes that actively look for the identification of safety risks through the analysis of the organization's activities? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 9 and 10 | Is there training relevant to proactive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 9 and 10 | Has the service provider developed communication relevant to proactive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is proactive reporting simple, accessible and commensurate with the size of the service provider? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 3, 9 and 10 | Does the service provider have predictive processes that provide the capture of system performance as it happens in real-time normal operations? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 9 and 10 | Is there training relevant to predictive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Has the service provider developed communication relevant to predictive methods of safety data collection? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is the predictive safety data capture process commensurate with the size of the service provider? | ☐ Yes ☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| Element 2.2 – Safety risk assessment and mitigation | | | |
| SMM (Doc 9859) Chapters 9 and 10 | Has the [organization] developed and maintains a formal process that ensures analysis, assessment and control of the safety risks in the [organization] operations? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 4, 9 and 10 | Does the [organization] SMS documentation clearly articulate the relationship between hazards, consequences and safety risks? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapters 5 and 9 | Is there a structured process for the analysis of the safety risks associated to the consequences of identified hazards, expressed in terms of probability and severity of occurrence? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 5 and 9 | Are there criteria for assessing safety risks and establishing safety risk tolerability (i.e., the acceptable level of safety risk the organization is willing to accept? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 5 and 9 | Does the service provider have safety risk mitigation strategies that include corrective/ preventive action plans to prevent recurrence of reported occurrences and deficiencies? | ☐ Yes ☐ No | |
| Component 3 – SAFETY ASSURANCE | | | |
| Element 3.1 – Safety performance monitoring and measurement | | | |
| SMM (Doc 9859) Chapters 9 and 10 | Has the [organization] implemented internal process by which the safety performance of the organization is verify and to validate the effectiveness of safety risks controls? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Are the following tools included in those processes?<br>Safety reporting systems ☐ Yes ☐ No<br>Safety studies ☐ Yes ☐ No<br>Safety reviews ☐ Yes ☐ No<br>Safety audits ☐ Yes ☐ No<br>Safety surveys ☐ Yes ☐No<br>Internal safety investigations ☐ Yes ☐ No | | |
| SMM (Doc 9859) Chapters 6 and 9 | Is the safety performance of the [organization] verified in reference to the safety performance indicators and safety performance targets of the SMS? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Are safety reports reviewed at the appropriate level of management? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a feedback process to notify contributors that their reports have been received and to share the results of the analysis? | ☐ Yes ☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 9 | Are corrective and preventive actions generated in response to hazard identification? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Are there procedures in place for the conduct of internal investigations? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a process to ensure that occurrences and deficiencies reported are analyzed to identify all associated hazards | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Does the service provider have a process for evaluating the effectiveness of the corrective/ preventive measures that have been developed? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Does the service provider have a system to monitor the internal reporting process and the associated corrective actions? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there an audit function with the independence and authority required to carry out effective internal evaluations? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Does the audit system cover all functions, activities and organizations within the service provider? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Are there selection/training processes to ensure the objectivity and competence of auditors as well as the impartiality of the audit process? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a procedure for reporting audit results and maintaining records? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a procedure outlining requirements for timely corrective and preventive action in response to audit results? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a procedure to record verification of action(s) taken and the reporting of verification results? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a process in place to monitor and analyze trends? | ☐ Yes ☐ No | |
| Element 3.2 – The management of change | | | |
| SMM (Doc 9859) Chapter 9 | Has the [organization] developed and maintains a formal process to identify changes within the organization which may affect established processes and services? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Does the formal process for the management of change analyze changes to operations or key personnel for safety risks? | ☐ Yes ☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 9 | Has the [organization] established arrangements to ensure safety performance prior to implementing changes? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Has the [organization] established a process to eliminate or modify safety risk controls that are no longer needed due to changes in the operational environment? | ☐ Yes ☐ No | |
| Element 3.3 – Continuous improvement of the SMS | | | |
| SMM (Doc 9859) Chapter 9 | Has the [organization] developed and maintains a formal process to identify the causes of sub-standard performance of the SMS? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Has the [organization] established a mechanism(s) to determine the implications of sub-standard performance of the SMS in operations? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Has the organization established a mechanism(s) to eliminate or mitigate the causes of substandard performance of the SMS? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Does the organization have a process for the proactive evaluation of facilities, equipment, documentation and procedures (through audits and surveys, etc.)? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Does the organization have a process for the proactive evaluation of the individuals' performance, to verify the fulfilment of their safety responsibilities? | ☐ Yes ☐ No | |
| Component 4 – SAFETY PROMOTION | | | |
| Element 4.1 – Training and education | | | |
| SMM (Doc 9859) Chapter 9 | Is there a documented process to identify training requirements so that personnel are trained and competent to perform the SMS duties? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is the safety training appropriate to the individual's involvement in the SMS? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is the safety training incorporated into indoctrination training upon employment? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there emergency response/contingency training for affected personnel? | ☐ Yes ☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a process that measures the effectiveness of training? | ☐ Yes ☐ No | |
| Element 4.2 – Safety communication | | | |
| SMM (Doc 9859) Chapter 9 | Are there communication processes in place within the [organization] that permit the safety management system to function effectively? | ☐ Yes ☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 9 | Are there communication processes (written, meetings, electronic, etc.) commensurate with the size and scope of the service provider? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 9 | Is safety critical information established and maintained in a suitable medium that provides direction regarding relevant SMS documents? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 9 | Is safety critical information disseminated throughout the [organization] and the effectiveness of safety communication monitored? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 9 | Is there a procedure that explains why particular safety actions are taken and why safety procedures are introduced or changed? | ☐ Yes<br>☐ No | |

- - - - - - - - - - - - - - -

# Chapter 8

# SMS PLANNING

## 8.1 OBJECTIVE AND CONTENTS

8.1.1 This chapter describes the requirements associated to the planning of an SMS, including the structure of an SMS implementation plan. These requirements are described using as reference the ICAO SMS framework. Although the ICAO SMS framework is introduced in full, the chapter discusses only the first component of the framework, safety policy and objectives, while the other three components of the ICAO SMS framework (Safety risk management, Safety assurance and Safety promotion) are discussed in chapter 9. The chapter includes the following:

- The components and the elements of SMS
- The ICAO SMS framework
- Management commitment and responsibility
- Safety accountabilities
- Appointment of key safety personnel
- Coordination of emergency response planning
- SMS documentation
- SMS implementation plan

## 8.2 THE COMPONENTS AND ELEMENTS OF SMS

8.2.1 There are four components in an SMS, that represent the two core operational processes underlying an SMS must undertake, as well as the organizational arrangements that are necessary to support the two core operational processes. The four components of an SMS are:

- Safety policy and objectives;
- Safety risk management;
- Safety assurance; and
- Safety promotion

8.2.2 The two core operational activities of an SMS are *safety risk management* and *safety assurance.* Safety risk management must be considered as an early system design activity, aimed at initial identification of hazards in the context in which operations related to the delivery of services will take place. Safety assurance must be considered as a continuous, on-going activity, aimed at ensuring that the initial identification of hazards and its assumptions in relation to the assessment of the consequences of safety risks and the defences that exist in the system as means of control remain valid and applicable as the system evolves over time, and/or to introduce changes in the defences as necessary. Thus, hazard identification can be considered as a one-stop or one-shot activity, that is conducted either during system design or when facing significant changes to the original system. Safety assurance, on the other hand, is a daily activity that is conducted non-stop to ensure that the operations that support the delivery of services are properly protected against hazards. Simply put, hazard identification provides the initial frame of reference against which assurance of safety is conducted on a daily basis.

8.2.3 These two core operational activities take place under the umbrella provided by *safety policy and objectives* and are supported by *safety promotion*. These two components of an SMS encompass the necessary organizational arrangements without which hazard identification and safety risk management would be impossible, or seriously flawed. It can therefore be considered that safety risk management and safety assurance are the actual "doing" of SMS; they are the operational activities underlying a performing SMS. Safety policies and objectives and safety promotion, on the other hand, provide the frame of reference as well as the support that allow the operational activities underlying safety risk management and safety assurance to be effectively conducted.

8.2.4 The four components discussed in the previous paragraphs constitute the basic building blocks of an SMS, in that they represent the four overarching safety management processes that underlie the actual management system (SMS). Each component is subdivided into elements, which encompass the specific sub-processes, specific tasks or specific tools that the actual management system must engage or utilise in order to conduct the management of safety as just any other core business function or organizational process.

8.2.5 The component ***Safety policy and objectives*** is composed of five elements:

- Management commitment and responsibility
- Safety accountabilities
- Appointment of key safety personnel
- Coordination of emergency response planning
- SMS documentation

8.2.6 The component ***Safety risk management*** is composed of two elements:

- Hazard identification
- Risk assessment and mitigation

8.2.7 The component ***Safety assurance*** is composed of three elements:

- Safety performance monitoring and measurement
- The management of change
- Continuous improvement of the SMS

8.2.8 The component ***Safety promotion*** is composed of two elements:

- Training and education
- Safety communication

## 8.3 THE ICAO SMS FRAMEWORK

***Note****. – A detail of the ICAO SMS framework is contained in Appendix 1 to this Chapter.*

8.3.1 The four components combined with the twelve elements discussed in section 8.2 conform the ICAO SMS framework, intended as a principled guide for the development and implementation of a service provider SMS, as follows:

**1. Safety policy and objectives**

1.1 – Management commitment and responsibility

1.2 – Safety accountabilities

1.3 – Appointment of key safety personnel

1.4 – Coordination of emergency response planning

1.5 – SMS documentation

**2. Safety risk management**

2.1 – Hazard identification

2.2 – Risk assessment and mitigation

| |
|---|
| **3. Safety assurance** |
| 3.1 – Safety performance monitoring and measurement |
| 3.2 – The management of change |
| 3.3 – Continuous improvement of the SMS |
| **4. Safety promotion** |
| 4.1 – Training and education |
| 4.2 – Safety communication |

## 8.4 MANAGEMENT COMMITMENT AND RESPONSIBILITY

8.4.1 In any organization, management is in control of the activities of personnel and of the use of resources that are directly related to, or necessary for, the delivery of services. The organization's exposure to safety hazards is a consequence of the activities directly related to the delivery of services. Through specific activities by personnel and the use of resources, management can actively control the safety risks related to the consequences of hazards. As examples of these activities, management hires, trains, and supervises employees, and procures equipment to support the service delivery related activities. Management must assure that the employees adhere to organizational safety directives and controls, and that their equipment remains in serviceable condition. Management's primary responsibly for managing safety is thus obvious, and this responsibility is discharged through the operation of a dedicated organizational system that incorporates the necessary safety risk controls. The service provider's SMS is management's means of fulfilling these responsibilities. An SMS is a management system for ensuring safe and efficient operations.

8.4.2 The starting point to ensure efficacy and efficiency of the organization's SMS is the safety policy of the organization. Senior management must develop the safety policy of the organization, signed by the Accountable Executive. An example of a safety policy is included in Figure 8-1. In general terms, the safety policy must include a commitment to:

- achieve the highest safety standards;
- observe all applicable legal requirements and international standards, and best effective practices;
- provide all appropriate resources;
- enforce safety as one primary responsibility of all managers; and
- ensure that the policy is understood, implemented and maintained at all levels.

**SAFETY POLICY STATEMENT**

Safety is one of our core business functions. We are committed to developing, implementing, maintaining and constantly improving strategies and processes to ensure that all our aviation activities take place under a balanced allocation of organizational resources, aimed at achieving the highest level of safety performance and meeting national and international standards.

All levels of management and all employees are accountable for the delivery of this highest level of safety performance, starting with the *[Chief Executive Officer (CEO)/Managing Director/ or as appropriate to the organization].*

**Our commitment is to:**

- **Support** the management of safety through the provision of all appropriate resources, that will result in an organizational culture that fosters safe practices, encourages effective safety reporting and communication, and actively manages safety with the same attention to results as the attention to the results of the other management systems of the organization;
- **Enforce** the management of safety among the primary responsibility of all managers and employees;
- **Clearly** define for all staff, managers and employees alike, their accountabilities and responsibilities for the delivery of the organization's safety performance and the performance of our safety management system;
- **Establish and operate** hazard identification and risk management processes, including a hazard reporting system, in order to eliminate or mitigate the safety risks of the consequences of hazards resulting from our operations or activities to a point which is As Low As Reasonably Practicable (ALARP);
- **Ensure** that no action will be taken against any employee who discloses a safety concern through the hazard reporting system, unless disclosure indicates, beyond any reasonable doubt, an illegal act, gross negligence, or a deliberate or wilful disregard of regulations or procedures;
- **Comply** with, and wherever possible exceed, legislative and regulatory requirements and standards;
- **Ensure** sufficient skilled and trained human resources are available to implement safety strategies and processes;
- **Ensure** that all staff are provided with adequate and appropriate aviation safety information and training, are competent in safety matters, and are allocated only tasks commensurate with their skills;
- **Establish and measure** our safety performance against realistic safety performance indicators and safety performance targets;
- **Continually improve** our safety performance through management processes that ensure that relevant safety action is taken and is effective; and
- **Ensure** externally supplied systems and services to support our operations are delivered meeting our safety performance standards.

(signed)

_____

CEO/Managing Director/or as appropriate

Figure 8-1 – Example of a safety policy

8.4.3 Once developed, senior management must communicate, with visible endorsement, the safety policy to all staff.

8.4.4 Senior management must also establish safety objectives, as well as the standards of safety performance for the SMS and, therefore, for the organization as a whole. The safety objectives must identify what the organization wants to achieve, in terms of the management of safety, and lay out the steps the organization needs to take to achieve the objectives. The standards of safety performance allow to measure organizational behaviour vis-à-vis safety performance and therefore regarding the management of safety. Both safety objectives and the standards of safety performance must be linked to the safety performance indicators, safety performance targets and safety requirements of the SMS, discussed in Chapter 6 *(ICAO safety management requirements)*.

8.4.5 The organization must identify the Accountable Executive, who must be a single, identifiable person having final responsibility for the effective and efficient performance of the organization's SMS. Depending on the size and complexity of the organization, the Accountable Executive may be:

- the Chief Executive Officer (CEO);
- the chairperson of the board of directors;
- a partner; or
- the proprietor
- ...

8.4.6. There is a tendency to identify *who* the Accountable Executive should be, from the perspective of the function assigned to the person within the organization. However, more important that *who* the Accountable Executive should be is *what* are the authorities and responsibilities the Accountable Executive should have in order to properly account for the safety performance of the SMS. These authorities and responsibilities include, but are not limited to:

- full authority for human resources issues;
- authority for major financial issues;
- direct responsibility for the conduct of the organization's affairs;
- final authority over operations under certificate; and
- final responsibility for all safety issues.

8.4.7 Chapter 2 *(Basic safety concepts)* discusses the allocation of resources as a fundamental organizational process. Allocation of resources is therefore one of the primordial functions of management. Paragraph 8.3.1 in this chapter further discusses the management function as one of control of the activities of personnel and of the use of resources that are directly related to the delivery of services, as a consequence of which the organization is exposed to safety hazards. The fore-mentioned underlies the justification for the responsibilities and authorities of the Accountable Executive in 8.4.6 above: such responsibilities and authorities refer to either allocation of resources or control of activities, exclusively. An organization that appoints an Accountable Executive who does not have these authorities and responsibilities would place the designated person in a position in which the person does not have the essential attributes to fulfil such role.

8.4.8 The Accountable Executive may assign the management of the SMS to another person, provided that such assignment is properly documented and described in the organization's Safety Management Systems Manual (SMSM) later discussed in this chapter. The accountability of the Accountable Executive is not, however, affected by the assignment of the management of the SMS to another person: the Accountable Executive retains final accountability for the performance of the organization's SMS.

## 8.5 SAFETY ACCOUNTABILITIES

8.5.1 Chapter 3 *(Introduction to safety management)* discusses the management of safety as a core business function that contributes to the analysis of an organization's resources and objectives. This analysis forms the basis for a balanced and realistic allocation of resources between protection and production goals that supports the overall service delivery needs of the organization. Paragraph 8.4.1 discusses SMS as management system for ensuring safe operations. Safe operations are unlikely unless a balanced and realistic allocation of resources between protection and production goals, that supports the overall service delivery needs of the organization, is achieved. In general terms, the *safety accountabilities* for ensuring safe operations, and the achievement of balance and realism in the allocation of resources, are materialised though the organization of the SMS itself, and particularly through one specific element of the SMS: the definition of safety accountabilities of all personnel, but most importantly, of *key* personnel.

8.5.2 The safety accountabilities of managers regarding the *organization of the SMS* refer to the definition of an architecture of the organization's SMS which corresponds to the size, nature and complexity of the operations, and to the hazards and safety risks associated with the activities necessary for the delivery of services. The safety accountabilities of

managers regarding the organization of the SMS furthermore include the allocation of human, technical, financial or any other necessary resources necessary for the effective and efficient performance of the SMS.

8.5.3 While the job descriptions of all employees, regardless of level, should include safety accountabilities and responsibilities, the safety accountabilities regarding the *definition of safety responsibilities and authorities of key personnel* refer to the inclusion in the job description of each senior manager (departmental head or responsible for a functional unit), of responsibilities regarding the operation of the SMS, to the appropriate extent, in addition to the specific responsibilities for the department/functional unit operation. Under the perspective of the management of safety as a core business function, every departmental head or responsible for a functional unit will have a degree of involvement in the operation of the SMS and its safety performance. This involvement will certainly be deeper for those responsible for operational departments or functional units directly involved in the delivery of the basic services of the organization (operations, maintenance, engineering, training and dispatch, hereafter referred to by the generic term "line managers") than for those responsible for supporting functions (human resources, administration, legal, and financial).

8.5.4 The safety accountabilities, responsibilities and authorities of all departmental heads and/or responsible for functional units, and in particular line managers, must be described in the organization's Safety Management Systems Manual (SMSM), discussed later in this chapter. Safety accountabilities, responsibilities and authorities must be graphically depicted in a functional chart showing interfaces and interrelationships in terms of the management of safety among the various sectors of the organization. Figure 8-2 is an example of a functional chart.

8.5.5 It is very important to note that Figure 8-2 depicts *functions* rather than *organization*. It is not intended to depict the *organization* of the management of safety in terms of departments and functional units and their relative hierarchical position within the enterprise, but rather the *functions* of each department and/or functional unit in terms of the delivery of safety as a core business process. The caveat is important because there will be as many organizational charts as organizations may exist in aviation. Therefore, for the purposes of this Manual, Figure 8-2 must be considered as a *functional chart*, not as an *organizational chart*. 8.5.6

8.5.6 The *Safety Services Office* is at the heart of the functional chart depicting safety accountabilities. The concept of a Safety Services Office is key to the notion of managing safety as a core business process, and to SMS as the system that management employs for such purpose. The Safety Services Office is independent and neutral from processes and decisions made regarding the delivery of services by line managers of operational units. Under an SMS environment, the Safety Services Office fulfils four essential corporate functions:

- manages and oversees the hazard identification system;
- monitors safety performance of operational units directly involved in service delivery;
- advises senior management on safety management matters; and
- assists line managers on safety management matters.


Figure 8-2 – Safety accountabilities

8.5.7 In the traditional perspective of safety discussed in Chapter 2, the safety office was the exclusive "owner" of the entire safety process within the organization. The safety officer, often known as accident prevention officer, was the person in change of identifying the safety concerns, proposing solutions, participating in the implementation of the solutions, and monitoring the effectiveness of the solutions. In recent years, the notion that "ownership" of the safety process was exclusive of the safety office was unwillingly reinforced by a widely-adopted industry practice establishing a direct reporting and communication link between the safety officer and the CEO of the organization. The intention behind this practice was providing unimpeded access by the safety officer to the CEO.

8.5.8 This widespread practice was propelled by a double justification. First, it aimed at raising the hierarchical level and conspicuousness of the safety office by establishing a direct link between the safety office and the CEO. Second, this direct link intended to generate neutrality in assessment of safety concerns and their resolution, by removing those in charge of managing operational activities directly related to service delivery (line managers) from safety assessment and resolution of concerns. The perspective was that there was a strong likelihood that line managers could be, to different degrees, interested parties, thus leading to potential conflict of interest in the assessment and resolution of safety concerns. The direct relationship between the safety officer and the CEO was established so as to defuse the potential for this perceived conflict of interest.

8.5.9 Clearly well-intentioned, this practice presented two serious downsides. First, by putting entire ownership of the safety process in the safety office, it gave a "free ride", safety-wise, to line managers. The direct link between the safety office and the CEO removed line managers from safety decision-making, and nurtured the perception that "safety problems are not my [line manager] problem, safety problems belong to the safety office and to the safety officer". The line of accountability thus shrank considerably, and was reduced to a two-party dialogue between the CEO and the safety officer. Given the workload associated to a CEO position, this dialogue had all the potential to become a monologue. Second and most important, it neglected and squandered the valuable input to the resolution of safety concerns, in terms of know-how, that the operational units could bring to the organizational safety decision-making process.

8.5.10 The SMS environment brings a different perspective. The name Safety Office is changed to Safety *Services* Office, to reflect that the office in question provides a service to the organization, to senior managers and line managers, in regard to the management of safety as a core business process. The axiom "one cannot manage what one cannot measure" discussed in Chapter 3 comes to fruition under SMS. The Safety Services Office is fundamentally a safety data collection and analysis unit. Through a combination of predictive, proactive and reactive methods (discussed in Chapter 3), the Safety Services Office captures what takes place within the operational drift (also discussed in Chapter 3), by continuously and routinely collecting safety data on hazards during service delivery activities.

8.5.11 Once hazards have been identified, their consequences evaluated and the safety risks of such consequences assessed *(i.e., once safety information has been extracted from the safety data)*, safety information is delivered to line managers for resolution of underlying safety concerns. Line managers are the true subject matter experts in their respective areas, and therefore those in the best position to design effective and efficient solutions and implement them. Furthermore, line managers can take the last step in safety data analysis, by turning safety information into safety intelligence, by providing context for the information on hazards distilled by the Safety Services Office.

8.5.12 As with the organization as a whole, the primary responsibility for safety management rests with those who "own" the production activities. It is during the production activities where hazards and the organization are directly confronted, where deficiencies in organizational processes contribute to unleash the damaging consequences of hazards, and where direct supervisory control and resource allocation can mitigate the safety risks to ALARP. Moreover, process owners are the domain technical experts in any organization and thus the most knowledgeable about the technical processes of production.

8.5.13 After the safety information is delivered to the appropriate line manager(s), the Safety Services Office resumes its routine safety data collection and analysis activities. At a time interval agreed between the Safety Services Office and the line manager(s) in question, the Safety Services Office presents a new set of safety information about the safety concern under consideration to the line manager(s) of the area(s) to which the safety concern pertains, and must therefore be involved in the resolution of the safety concern. The safety information will indicate if the mitigation solutions implemented by the line manager(s) addressed the safety concern, or if the safety concern persists. In the latter case, further mitigation solutions are deployed, a new time interval is agreed, safety data is collected and analysed, safety information is delivered, and this cycle is repeated as many times as necessary until safety data analysis substantiates that the safety concern has been solved. Throughout all this process, the line manager(s) of the area(s) in question do not report progress to the Safety Services Office, but to the Accountable Executive, as final responsible for the organization's SMS, through any of the organization's two formal safety bodies discussed in section 8.6 hereunder.

## 8.6 APPOINTMENT OF KEY SAFETY PERSONNEL

8.6.1 Key to the effective implementation and functioning of a Safety Services Office as discussed in the paragraphs above is the appointment of the person in charge of the daily operation of the Safety Services Office. This person

will be identified by different names in different organizations, and for the purposes of this Manual the generic term **Safety Manager** is retained.

8.6.2 The Safety Manager will be, in most organizations, the person whom the Accountable Executive has assigned the day-to-day management functions of the SMS. The Safety Manager is the responsible individual and focal point for the development and maintenance of an effective SMS. The Safety Manager also advises the Accountable Executive and line managers on matters regarding safety management, and is responsible for coordinating and communicating safety issues within the organization, as well as with external agencies, contractors and stakeholders as appropriate. The Safety Manager functions include, but are not necessarily limited to:

- management of the SMS implementation plan on behalf of the Accountable Executive;
- performing/facilitating hazard identification and safety risk analysis;
- monitoring corrective actions and evaluating their results;
- providing periodic reports on the organization's safety performance;
- maintaining records and safety documentation;
- planning and organizing staff safety training;
- providing independent advice on safety matters;
- monitoring safety concerns in the aviation industry and their perceived impact in the organization's operations aimed at service delivery;
- coordinating and communicating (on behalf of the Accountable Executive) on issues relating to safety with the State's oversight authority, and other State agencies as necessary; and
- coordinating and communicating (on behalf of the Accountable Executive) on issues relating to safety with international agencies.

8.6.3 The Safety Manager may be the only person running the Safety Services Office, or may be supported by additional staff, mostly safety data analysts. This will depend upon the size of the organization, and the nature and complexity of the operations supporting delivery of services. Regardless of the size of the Safety Services Office and its staffing level, its functionalities remain the same. The Safety Manager liaises directly with the line managers (operations, maintenance, engineering, training, etc.) This is depicted by the solid arrows in the functional chart in Figure 8.2. If, due to the size of the organization, the heads of operational units have a dedicated safety officer with subject matter expertise and delegated responsibility for the management of safety concerns in the particular area of activity, these dedicated safety officers become the first point of contact of their respective units for the Safety Manager, in the exchanges pertaining to safety information.

8.6.4 Under normal circumstances, the Safety Manager can access and/or communicate with the Accountable Executive through two channels: through the Safety Action Group, and through it through the Safety Review Board; or directly through the Safety Review Board. Both groups, their roles and interconnections, and the participation of the Safety Manager in these groups is discussed later in this chapter. Infrequently, specific and special circumstances may arise. These would be circumstances where the nature of the safety concern requiring communication with or access to the Accountable Executive by the Safety Manager is so exceptional and of such an urgency that going through the normal process of communication would expose the organization to extreme consequences. In these exceptional circumstances, the Safety Manager must have a direct emergency access to the Accountable Executive, as depicted by the dotted line connecting the respective boxes. This "backdoor" communication channel should rarely be used, and when it is, it should be properly justified and documented.

8.6.5 In an SMS environment, the Safety Manger will be the person responsible for the collection and analysis of safety data on hazards, and the distribution of safety information on hazards and the safety risks of the consequences of hazards among line managers. As such, the Safety Manager will likely be, more often than not, the bearer of bad news, safety-wise. For this reason the selection criteria of the Safety Manager acquires a special significance. The selection criteria of the Safety Manager include, but are not limited to, the following:

- operational management experience;
- technical background to understand the systems that support operations;
- people skills;
- analytical and problem-solving skills;

- project management skills; and
- oral and written communications skills.

***Note**. – A sample job description for the safety manager with detailed information concerning the key role, responsibilities and qualifications is contained in Appendix 2 to this Chapter.*

8.6.6 Distributing information on the safety risks of the consequences of hazards by the Safety Services Office is only the first step in the safety risk management process. This information must be acted upon by line managers. The mitigation of safety concerns inevitably requires resources. Sometimes such resources are available to line managers. Often times mitigation of safety concerns requires additional allocation of resources, and the authorities for such allocation may not be within the authorities of the line managers, and must be approved by senior levels of the organization. Likewise, there needs to be some formal organizational process to ensure a neutral assessment of the effectiveness and efficiency of the mitigation strategies in relation to the agreed safety performance of the organization. The Safety Review Board (SRB) provides the platform to achieve the objectives of resource allocation and neutral assessment of the effectiveness and efficiency of the mitigation strategies.

8.6.7 The SRB is a very high level committee, chaired by the Accountable Executive and composed by senior managers, including line managers responsible for functional areas. The Safety Manager participates of the SRB meeting in an advisory capacity only. The SRB is eminently strategic, deals with very high level issues in relation to policies, resource allocation and organizational performance monitoring, and meets infrequently, unless exceptional circumstances dictate otherwise. The SRB:

- monitors effectiveness of the SMS implementation plan;
- monitors that any necessary corrective action is taken in a timely manner;
- monitors safety performance against the organization's safety policy and objectives;
- monitors the effectiveness of the organisation's safety management processes which support the declared corporate priority of safety management as another core business process:
- monitors effectiveness of the safety supervision of sub-contracted operations;
- ensures that appropriate resources are allocated to achieve the established safety performance beyond that required by regulatory compliance alone; and
- gives strategic direction to the SAG.

8.6.8 Once strategic direction has been developed by the SRB, concerted implementation of strategies across the organization must take place, in a coordinated manner. The coordinated implementation of directive strategies is the primary role of the Safety Action Group (SAG). SAG is a high level committee chaired in turn by designated line managers, and composed by line managers and representatives of front-line personnel. The Safety Manager is the secretary of the SAG. The SAG is eminently tactical and, following strategic direction provided by the SRB, deals with implementation issues to satisfy the strategic directives of the SRB. While the SAG deals with "grass root" implementation issues pertaining to specific activities to ensure control of the safety risks of the consequences of hazards during line operations, the SRB deals with the coordination of "grass root" implementation issues, to ensure coordination of efforts and consistency with the strategic direction provided by the SRB. The SAG:

- oversees operational safety performance within the functional areas, ensuring that hazard identification and safety risk management are carried out as appropriate, with such involvement of staff as may be necessary to build up safety awareness;
- coordinates the resolution of mitigation strategies for the identified consequences of hazards, ensuring that satisfactory arrangements exist for safety data capture and securing employee feedback;
- assesses the impact on safety of operational changes;
- coordinates the implementation of corrective action plans, convening meetings or briefings as may be necessary to ensure that effective opportunities are available for all employees to participate fully in management for safety;
- ensures that corrective action is taken in a timely manner;

- reviews the effectiveness of previous safety recommendations; and
- oversees safety promotion and ensures that appropriate safety, emergency and technical training of personnel is carried out to meet or exceed minimum regulatory requirements.

## 8.7 COORDINATION OF EMERGENCY RESPONSE PLANNING

8.7.1 Emergency response planning (ERP) outlines in writing what should be done after an accident, and who is responsible for each action. The purpose of ERP is to ensure that there is orderly and efficient transition from normal to emergency operations, delegation of emergency authority, and assignment of emergency responsibilities. Authorization by key personnel for actions is also contained in the plan, as well as the coordination of efforts to cope with the emergency. The overall objective is the safe continuation of operations, or return to normal operations as soon as possible.

8.7.2 Airports must develop an Airport Emergency Plan (AEP), air traffic service providers must develop Contingency Plans, and airlines must develop an Emergency Response Plan. Since airport, ATC and airlines operations overlap, it stands to reason that the different plans should be compatible. The coordination of the different plans should be described in the SMS Manual.

## 8.8 SMS DOCUMENTATION

8.8.1 Chapter 7 introduces the features of an SMS, and discusses that one such feature is that an SMS is explicit, in that all safety management activities are documented and visible. It follows that documentation is an essential element of an SMS.

8.8.2 SMS documentation must include and make reference, as appropriate, to all relevant and applicable national and international regulations. It must also include SMS-specific records and documentation, such as hazards reporting forms, lines of accountability, responsibility and authority regarding the management of operational safety, the structure of the safety management organization, and so forth. It must furthermore document explicit guidelines for record management, including handling, storage, retrieval and preservation. But without doubt, the most important piece of documentation of an SMS is the SMS Manual (SMSM).

8.8.3 The SMSM is a key instrument for communicating the organization's approach to safety to the whole organization. It documents all aspects of the SMS, including the safety policy, objectives, procedures and individual safety accountabilities.

8.8.4 Typical contents of an SMSM include:

- Scope of the safety management system.
- The safety policy and objectives.
- Safety accountabilities.
- Key safety personnel.
- Documentation control procedures.
- Coordination of the emergency response planning.
- Hazard identification and risk management schemes.
- Safety assurance.
- Safety performance monitoring.
- Safety auditing.
- Management of change.
- Safety promotion.
- Contracted activities

## 8.9 SMS IMPLEMENTATION PLAN

8.9.1 The SMS implementation plan is a definition of the approach the organization will adopt for managing safety. As such, it becomes a realistic strategy for the implementation of an SMS that will meet the organization's safety objectives while supporting effective and efficient delivery of services. It describes how a organization will achieve its corporate safety objectives and how it will meet any new or revised safety requirements, regulatory or otherwise. Significant items in the plan will normally be included in the organization business plan. An SMS implementation plan, which may consist of more than one document, details the actions to be taken, by whom and in what time-scale.

8.9.2 Depending on the size of the organization and the complexity of the operations, the SMS implementation plan may be developed by one person, or by a planning group which comprises an appropriate experience base. The planning group should meet regularly with senior management to assess progress of the implementation plan, and receive resources (including time for meetings), commensurate with the task at hand.

8.9.3 Typical contents of an SMS implementation plan include:

- Safety policy and objectives
- System description
- Gap analysis
- SMS components
- Safety roles and responsibilities
- Safety reporting policy
- Means of employee involvement
- Safety performance measurement
- Safety communication
- Safety training
- Management review (of safety performance).

8.9.4 Once completed by the person or planning group, senior management endorses the plan. Typical implementation time frame for an SMS will be one to four years. SMS implementation, including a phased approach, is discussed in Chapter 10. Guidance on the methodology for developing an SMS implementation plan and associated timeframe is included in Appendix 2 to Chapter 10.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 1 to Chapter 8

# FRAMEWORK FOR SAFETY MANAGEMENT SYSTEMS (SMS)

## Introduction

Appendix 1 to Chapter 8 introduces a framework for the implementation and maintenance of a safety management system (SMS) by an organization. An SMS is a management tool for the management of safety by an organization. The framework includes four components and twelve elements representing the minimum requirements from SMS implementation. The implementation of the framework shall be commensurate with the size of the organization and the complexity of the services provided. This appendix also includes a brief description of each element of the framework.

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

## 1. SAFETY POLICY AND OBJECTIVES

### 1.1 Management commitment and responsibility

The [organization] shall define the organization's safety policy which shall be in accordance with international and national requirements, and which shall be signed by the Accountable Executive of the organization. The safety policy shall reflect organizational commitments regarding safety; shall include a clear statement about the provision of the necessary resources for the implementation of the safety policy; and shall be communicated, with visible endorsement, throughout the organization. The safety policy shall include the safety reporting procedures; shall clearly indicate which types of operational behaviours are unacceptable; and shall include the conditions under which exemption from disciplinary action would be applicable. The safety policy shall be periodically reviewed to ensure it remains relevant and appropriate to the organization.

### 1.2 Safety accountabilities

The [organization] shall identify the Accountable Executive who, irrespective of other functions, shall have ultimate responsibility and accountability, on behalf of the [organization], for the implementation and maintenance of the SMS. The [organization] shall also identify the accountabilities of all members of management, irrespective of other functions, as well as of employees, with respect to the safety performance of the SMS. Safety responsibilities, accountabilities and authorities shall be documented and communicated throughout the organization, and shall include a definition of the levels of management with authority to make decisions regarding safety risks tolerability.

### 1.3 Appointment of key safety personnel

The [organization] shall identify a safety manager to be the responsible individual and focal point for the implementation and maintenance of an effective SMS.

### 1.4 Coordination of emergency response planning

The [organization] shall ensure that an emergency response plan that provides for the orderly and efficient transition from normal to emergency operations and the return to normal operations is properly coordinated with the emergency response plans of those organizations it must interface with during the provision of its services.

### 1.5 SMS documentation

The [organization] shall develop an SMS implementation plan, endorsed by senior management of the organization, that defines the organization's approach to the management of safety in a manner that meets the organization's safety objectives, and maintain SMS documentation to describe the safety policy and objectives, the SMS requirements, the SMS processes and procedures, the accountabilities, responsibilities and authorities for processes and procedures, and the SMS outputs. Also as part of the SMS documentation, the [organization] shall develop and maintain a safety management systems manual (SMSM), to communicate its approach to the management of safety throughout the organization.

## 2. SAFETY RISK MANAGEMENT

### 2.1 Hazard identification

The [organization] shall develop and maintain a formal process that ensures that hazards in operations are identified. Hazard identification shall be based on a combination of reactive, proactive and predictive methods of safety data collection.

### 2.2 Safety risk assessment and mitigation

The [organization] shall develop and maintain a formal process that ensures analysis, assessment and control of the safety risks in [organization] operations.

## 3. SAFETY ASSURANCE

### 3.1 Safety performance monitoring and measurement

The [organization] shall develop and maintain the means to verify the safety performance of the organization and to validate the effectiveness of safety risks controls. The safety performance of the organization shall be verified in reference to the safety performance indicators and safety performance targets of the SMS.

### 3.2 The management of change

The [organization] shall develop and maintain a formal process to identify changes within the organization which may affect established processes and services; to describe the arrangements to ensure safety performance before implementing changes; and to eliminate or modify safety risk controls that are no longer needed or effective due to changes in the operational environment.

### 3.3 Continuous improvement of the SMS

The [organization] shall develop and maintain a formal process to identify the causes of sub-standard performance of the SMS, determine the implications of sub-standard performance of the SMS in operations, and eliminate or mitigate such causes.

## 4. SAFETY PROMOTION

### 4.1 Training and education

The [organization] shall develop and maintain a safety training programme that ensures that personnel are trained and competent to perform the SMS duties. The scope of the safety training shall be appropriate to each individual's involvement in the SMS.

### 4.2 Safety communication

The [organization] shall develop and maintain formal means for safety communication, that ensures that all personnel are fully aware of the SMS, conveys safety critical information, and explains why particular safety actions are taken and why safety procedures are introduced or changed.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 2 to Chapter 8

# SAMPLE JOB DESCRIPTION FOR SAFETY MANAGER

## 1. OVERALL PURPOSE

The safety manager is responsible for providing guidance and direction for the planning, implementation and operation of the organization's safety management system (SMS).

## 2. KEY ROLES

*Safety advocate*

- Demonstrates an excellent safety behaviour and attitude, follows regulatory practices and rules, recognizes and reports hazards and promotes an effective safety reporting.

*Leader*

- Models and promotes an organizational culture that fosters safety practices through effective leadership.

*Communicator*

- Acts as an information conduit to bring safety issues to the attention of management and to deliver safety information to the organization staff, contractors and stakeholders.
- Provides and articulates information regarding safety issues within the organization.

*Developer*

- Assists in the continuous improvement of the hazard identification and safety risk assessment schemes and the organization's SMS.

*Relationship builder*

- Builds and maintains an excellent working relationship with the organizations Safety Action Groups (SAG) and within the Safety Services Office (SSO).

*Ambassador*

- Represents the organization on government, international organizations and industry committees (e.g., ICAO, IATA, CAA, AIB, etc.)

*Analyst*

- Analyzes technical data related to hazards, events and occurrences for trends.

*Process management*

- Effectively utilizes applicable processes and procedures to complete roles and responsibilities.
- Investigates opportunities to increase process efficiency.
- Measures the effectiveness and seeks to continually improve the quality of processes.

## 3. RESPONSIBILITIES

3.1 The position requires the ability to cope with changing circumstances and situations with little supervision. The safety manager acts independently of other managers within the organization.

3.2 The safety manager is responsible for providing information and advice to senior management and to the Accountable Executive on matters relating to safe operations. Tact, diplomacy and a high degree of integrity are prerequisites.

3.3 The job requires flexibility as assignments may be undertaken with little or no notice and outside normal work hours.

## 4. NATURE AND SCOPE

The safety manager must interact with operational personnel, senior managers and departmental heads throughout the organization. The safety manager should also foster positive relationships with regulatory authorities, agencies and service providers outside the organization. Other contacts will be established at a working level as appropriate.

## 5. QUALIFICATIONS

The attributes and qualifications include:

a) broad operational knowledge and experience in the functions of the organization (e.g. training management, aircraft operations, air traffic management, aerodrome operations, and maintenance organization management);

b) sound knowledge of safety management principles and practices;

c) good written and verbal communication skills;

d) well-developed interpersonal skills;

e) computer literacy;

f) the ability to relate to all levels, both inside and outside the organization;

g) organizational ability;

h) capable of working unsupervised;

i) good analytical skills;

j) leadership skills and an authoritative approach; and

k) worthy of respect among peers and management.

## 6. AUTHORITY

6.1 Regarding safety matters, the safety manager has direct access to the Accountable Executive and appropriate senior and middle management.

6.2 The safety manager is authorized to conduct safety audits, surveys and inspections of any aspect of the operation.

6.3 The safety manager has the authority to conduct investigations on internal safety events in accordance with the procedures specified in the safety management systems manual (SMSM) of the organization.

- - - - - - - - - - - - - - -

# Chapter 9

# SMS OPERATION

## 9.1 OBJECTIVE AND CONTENTS

9.1.1 This chapter describes the requirements associated with the operation of an SMS. The requirements associated with the operation of an SMS are discussed using as reference the ICAO SMS framework. While Chapter 8 discussed the requirements associated with the planning of an SMS using as a reference the first component of the ICAO SMS framework, this chapter discusses the operation of an SMS, using as references the three remaining components of the framework. The chapter includes the following:

- Safety risk management - General
- Hazard identification
- Risk assessment and mitigation
- Safety assurance - General
- Safety performance monitoring and measurement
- Protection of sources of safety information
- The management of change
- Continuous improvement of the SMS
- The relationship between safety risk management and safety assurance
- Safety promotion – Training and education
- Safety promotion – Safety communication

## 9.2 SAFETY RISK MANAGEMENT - GENERAL

9.2.1 Organizations manage safety by ensuring that, through its safety management process, the safety risks of the consequences of hazards in critical activities related to the provision of services are controlled to a level as low as reasonably practicable (ALARP). This is known as *safety risk management*, a generic term that encompasses two distinct activities: hazard identification and safety risk assessment and mitigation.

9.2.2 Safety risk management builds upon a system design into which appropriate controls to the safety risks of the consequences of anticipated hazards are embedded in the system. This is true whether the "system" in question is a physical system such as an aircraft, or an organizational system, such as an airline, an aerodrome or a traffic service provider. In terms of this Manual, the latter – organizational system – is the "system" more commonly referred to. An organization is a system consisting of the structures, processes, and procedures, as well as the people, equipment and facilities that are necessary to accomplish the system's mission.

## 9.3 HAZARD IDENTIFICATION

9.3.1 Safety risk management starts with a description of system's functions as the basis for hazard identification (system description is discussed in Chapter 7). In the system description, the system components and their interfaces with the system's operational environment are analyzed for the presence of hazards, as well as to identify those safety risk controls already existing in the system or their absence thereof (a process known as gap analysis, also discussed in Chapter 7). Hazards are analyzed within the context of the described system, their potentially damaging consequences identified, and such consequences assessed in terms of safety risks (the probability and resulting severity of the damaging potential of the identified consequences, discussed in Chapter 5). Where the safety risks of the consequences of hazards are assessed to be too high to be acceptable, additional safety risk controls must be built into the system. Assessment of system design and verification that it adequately controls the consequences of hazards is, therefore, a fundamental element of safety management.

9.3.2 Hazard identification is therefore the first step in a formal process of collecting, recording, acting on and generating feedback about hazards and safety risks in operations. In a properly deployed SMS, sources of hazard identification

must include the three methods discussed in Chapter 3: reactive, proactive and predictive methods. The hazard identification process itself is discussed in Chapter 4.

9.3.3 A structured approach to the identification of hazards ensures that, as much as possible, most hazards in the system's operational environment are identified. Suitable techniques for ensuring such a structured approach might include:

a) *Checklists*: Review experience and available data from similar systems and draw up a hazard checklist. Potentially hazardous areas will require further evaluation.

b) *Group review*: Group sessions may be used to review the hazard checklist, to brainstorm hazards more broadly, or to conduct a detailed scenario analysis.

9.3.4 Hazard identification sessions require a range of experienced operational and technical personnel, and are usually done through a form of managed group discussion. A facilitator who is familiar with brainstorming techniques should manage the group sessions. A safety manager, if appointed, would normally fill this role. While the use of group sessions is addressed here in the context of hazard identification, the same group would also address the assessment of the probability and severity of the safety risks of the consequences of the hazards they have identified.

9.3.5 The assessment of hazards should take into consideration all possibilities, from the least to the most likely. It has to make adequate allowance for "worst case" conditions, but it is also important that the hazards to be included in the final analysis be "credible" hazards. It is often difficult to define the boundary between a worst credible case and one so dependent on coincidence that it should not be taken into account. The following definitions can be used as a guide in making such decisions:

- *Worst case*: The most unfavourable conditions expected, e.g. extremely high levels of traffic, and extreme weather disruption.
- *Credible case*: This implies that it is not unreasonable to expect that the assumed combination of extreme conditions will occur within the operational life cycle of the system.

9.3.6 All identified hazards should be assigned a hazard number, and be recorded in a hazard log (examples of hazard logs can be found in the appendixes to Chapter 5). The hazard log should contain a description of each hazard, its consequences, the assessed likelihood and severity of the safety risks of the consequences, and required safety risk controls, most usually, mitigation measures. The hazard log should be updated as new hazards are identified, and proposals for further safety risk controls (i.e., further mitigation measures) are introduced.

## 9.4 RISK ASSESSMENT AND MITIGATION

9.4.1 Once hazards have been identified, the safety risks of their potential consequences must be assessed (Chapter 5). Safety risk assessment is the analysis of the safety risks of the consequences of the hazards that have been determined as threatening the capabilities of an organization. Safety risk analyses use a conventional breakdown of risk in two components – probability of occurrence of a damaging event or condition, and severity of the event or condition, should it occur. Safety risk decision making and acceptance is specified through use of a risk tolerability matrix. While a matrix is required, discretion is also required. The definitions and final construction of the matrix should be left to the service provider's organization to design, subject to approval of its oversight organization. This is to ensure that each organization's safety decision tools are relevant to its operations and operational environment, recognizing the extensive diversity in this area.

9.4.2 After safety risks have been assessed though the preceding step, elimination and/or mitigation to ALARP must take place. This is known as safety risk mitigation. Safety risk controls must be designed and implemented. These may be additional or changed procedures, new supervisory controls, changes to training, additional or modified equipment, or any of a number of other elimination/mitigation alternatives. Almost invariably these alternatives will involve deployment or re-deployment of any of the three traditional aviation defences (technology, training and regulations), or combinations of them. After the safety risk controls are designed but before the system is placed "on line," an assessment must be made of whether the controls are considered effective and/or if they introduce new hazards to the system.

9.4.3 At this point, the system is ready for operational deployment/re-deployment, assuming that the safety risk controls are deemed to be acceptable. The next component of an SMS, safety assurance, utilises auditing, analysis, review and similar techniques, in line with those utilised by quality management systems. These techniques are used to monitor the safety risk controls to ensure that they continue to be implemented as designed and that they continue to be effective in the dynamic operational environment.

## 9.5 SAFETY ASSURANCE - GENERAL

9.5.1 Safety risk management requires feedback on safety performance to complete the safety management cycle. Through monitoring and feedback, SMS performance can be evaluated and any necessary changes to the system effected. In addition, safety assurance provides stakeholders an indication of the level of safety performance of the system.

9.5.2 Assurance can simply be defined as "something that gives confidence". The safety risk management process in the SMS starts with the organization's obtaining a good understanding of its operational processes and the environments in which it operates; progresses through hazard identification, safety risk assessment and safety risk mitigation, and culminates in development and implementation of appropriate safety risk controls. After controls for the safety risks of the consequences of hazards are designed, deemed to be capable of controlling safety risks, and put into operation, safety assurance takes over safety risk management.

9.5.3 Once safety risk controls are developed and implemented, it is the organization's responsibility to assure that they continue to be in place and that they work as intended. Under the above definition of "assurance," this consists of processes and activities undertaken by the organization to provide confidence as to the performance and effectiveness of the controls. The organization must continually monitor its operations and the environment to assure that it recognizes changes in the operational environment that could signal the emergence of new and unmitigated hazards, and for degradation in operational processes, facilities, equipment conditions, or human performance that could reduce the effectiveness of existing safety risk controls. This would signal the need to return to the safety risk management process to review and, if necessary, revise existing safety risk controls or develop new ones.

9.5.4 A process of permanent examination, analysis, and assessment of these controls must continue throughout the daily operation of the system. The safety assurance process mirrors those found in quality assurance, with requirements regarding analysis, documentation, auditing, and management reviews of the effectiveness of the safety risk controls. The difference is that the emphasis in safety assurance is in assuring that the safety risk controls are in place, being practiced, and remain effective. The traditional emphasis in quality assurance is typically on customer satisfaction, which, unless the proper perspectives are respected, may or may not fully parallel safety satisfaction. A brief discussion follows.

9.5.5 Quality assurance in aviation has traditionally been associated with maintenance and manufacturing operations and less often used in flight operations, except for limited use in training and checking. Some earlier regulations called for quality assurance programmes, although the requirements were often not comprehensive or well defined across all functions of the organization. The fact remains, however, that quality assurance is a familiar term although often associated with customer satisfaction and achievement of commercial objectives rather than safety. Nevertheless, as a means of assuring attainment of organizational objectives, quality assurance techniques are applicable to safety assurance. In order to use these techniques for safety assurance, the organization must be careful in setting and measuring objectives with respect to safety.

9.5.6 The most important aspect is for the organization to design and implement all operational processes in such a manner as to incorporate safety risk controls based on a sound application of safety risk management principles and to provide assurance of those controls. The choice of title – "quality" or "safety" – for the assurance process on the part organization is of lesser importance as long as a focus on safety is maintained in the SMS.

9.5.7 Chapter 6 discusses compliance and performance based approaches to safety management. One aspect that might be overlooked in assuring performance, unless a proper perspective is observed, is the inclusion of assurance of regulatory compliance. Chapter 6 introduces the notion of regulations as safety risk controls. As such, regulations are an integral part of the safety risk management process. In a properly deployed SMS, there should be no conflict between safety risk assurance and regulatory compliance assurance. Regulations should be part of the system design, and regulatory compliance and safety risk management are parts of the same whole. Compliance with regulations is still an expectation, and should be within the purview of safety assurance, as an activity aimed at "giving confidence" of the performance of the SMS.

9.5.8 In conclusion, senior management must ensure that safety satisfaction and customer satisfaction objectives are balanced in order to maintain business viability while maintaining safety of operations. While integration of SMS and QMS objectives might result in economy of resources, the possibility of mismatches between safety satisfaction objectives and customer satisfaction objectives means that the two are not automatically interchangeable or even aligned. It is up to the organization's management to provide for this type of integration. Assessment of system performance and verification that the system's performance continues to control safety risk in its current operational environment remains the fundamental concern, from the perspective of safety management.

9.5.9 Lastly, the safety assurance activities should include procedures that ensure that corrective actions are developed in response to findings of reports, studies, surveys, audits, evaluations and so forth, and to verify their timely and effective implementation. Organizational responsibility for the development and implementation of corrective actions should reside with the operational departments cited in findings. If new hazards are discovered, the safety risk management process should be employed to determine if new safety risk controls should be developed.

## 9.6 SAFETY PERFORMANCE MONITORING AND MEASUREMENT

9.6.1 The primary task of safety assurance is control. This is achieved through safety performance monitoring and measurement, process by which the safety performance of the organization is verified in comparison with the safety policy and approved safety objectives. The safety assurance control is conducted by monitoring and measuring the outcomes of activities the operational personnel must engage into for the delivery of services by the organization.

9.6.2 The international quality management standard, ISO-9000, supplies the following definition of process: *"…an interrelated set of activities that transform inputs into outputs."* The emphasis on *"activities"* as basically *"the things people do"* is the reason why so much discussion about human error takes place, and so much emphasis is placed on workplace conditions, in the discussions on safety and safety management in Chapters 2 and 3, and eventually carried over to safety risk management. It is these conditions that are at the root of most hazards, and it is these conditions that are the focus of most safety risk controls. Thus, most assurance activities under safety performance and monitoring are focused on conditions in the workplace that affect how people perform necessary activities from delivery of services. It is for this reason also that the SHEL(L) model – a model of the systems that support accomplishment of the operational activities that make up the delivery of services – is proposed as the guide for system description and the gap analyses.

9.6.3 The following provides a list of generic aspects or areas to be considered to "assure safety" through safety performance monitoring and measurement:

- ***Responsibility***: Who is accountable for management of the operational activities (planning, organizing, directing, controlling) and its ultimate accomplishment.
- ***Authority***: Who can direct, control, or change the procedures and who cannot as well as who can make key decisions such as safety risk acceptance decisions.
- ***Procedures.*** These are specified ways to carry out operational activities, and that translate the "what" (objectives) into "how" (practical activities).
- ***Controls***: These are elements of the system, including, hardware, software, special procedures or procedural steps, and supervisory practices designed to keep operational activities on track.
- ***Interfaces.*** This aspect includes an examination of such things as lines of authority between departments, lines of communication between employees, consistency of procedures, and clear delineation of responsibility between organizations, work units, and employees.
- ***Process measures.*** Means of providing feedback to responsible parties that required actions are taking place, required outputs are being produced and expected outcomes are being achieved.

9.6.4 Information for safety performance and monitoring comes from a variety of sources, including formal auditing and evaluation, investigations of safety-related events, continuous monitoring of day-to-day activities related to the delivery of services, and inputs from employees through hazard reporting systems. Each of these types of information sources may exist to some degree in every organization. However, specifications about what these sources be or how they should "look like" should be are left for the operational level, allowing individual organizations to tailor them to the scope and scale appropriate for their size and type of organization. Information sources for safety performance monitoring and measurement include:

- hazard reporting;
- safety studies;
- safety reviews;
- audits;
- safety surveys; and
- internal safety investigations

9.6.5 **Hazard reporting** and hazard reporting systems are essential elements in hazard identification. Nobody knows better actual system performance than operational personnel. An organization who wishes to know how it really operates daily, as opposed as to how it should operate as per "the book", should ask operational personnel. Hence the importance of reporting systems. There are three types of reporting systems:

- mandatory reporting systems;
- voluntary reporting systems; and
- confidential reporting systems.

9.6.6 In mandatory reporting systems, people are required to report certain types of events or hazards. This necessitates detailed regulations outlining who shall report and what shall be reported. Since mandatory systems deal mainly with "hardware" matters, they tend to collect more information on technical failures than on other aspects of operational activities. To help overcome this bias, voluntary reporting systems aim at acquiring more information on those other aspects.

9.6.7 In voluntary reporting systems the reporter, without any legal or administrative requirement to do so, submits voluntary event or hazard information. In these systems, regulatory agencies may offer an incentive to report. For example, enforcement action may be waived for unintentional violations that are reported. The reported information should not be used against the reporters, i.e. such systems must be non-punitive and afford protection to the sources of the information to encourage the reporting of such information.

9.6.8 Confidential reporting systems aim to protect the identity of the reporter. This is one way of ensuring that voluntary reporting systems are non-punitive. Confidentiality is usually achieved by de-identification, often by not recording any identifying information of the reporter. Confidential incident reporting systems facilitate the disclosure of hazards leading to human error, without fear of retribution or embarrassment, and enable broader acquisition of information on hazards.

9.6.9 While the basic processes underlying reporting system are standardised, the actual reporting requirements may vary among States and organizations. It is also important to note, in order to ensure success of the reporting system(s), that there is a normal reluctance by operational personnel to report. This statement is valid for all types of reporting, and particularly applicable where self-reporting of errors is involved. There are reasons for this reluctance: retaliation, self-incrimination and embarrassment just to mention the topmost three. Education in terms of the importance of safety reporting as hazard identification systems, discussed in Chapter 2, and the protection of the sources of safety information (discussed in Section 9.7) are essential strategies to circumvent reluctance to report and ensure an effective safety reporting environment. Typical qualities of successful safety reporting systems include:

- the reports are easy to make;
- there is no disciplinary actions as result of the reports;
- the reports are confidential; and
- feedback is rapid, accessible and informative.

9.6.10 **Safety studies** are rather large analyses encompassing broad safety concerns. Some pervasive safety issues can best be understood through an examination in the broadest possible context. An organization might experience a safety concern which is of a global nature, and which may have been addressed on an industry or State-wide scale. For example, an airline may experience an increase in approach and landing related events (unstable approaches, deep landings, landings with excessive airspeed and so forth). At a global level, the industry has been concerned with the frequency and severity of approach and landing accidents (ALA) and has undertaken major studies, produced many safety recommendations and implemented global measures to reduce events during the critical approach and landing phases of flight. Thus, the airline in question can find in these global recommendations and studies convincing arguments for its own, in-house safety analysis. Such arguments are necessary to achieve large-scale changes requiring significant data, appropriate analysis, and effective communication. Safety arguments based on isolated occurrences and anecdotal information may not be enough. Because of their nature, safety studies are more appropriate to address system safety deficiencies rather than identify specific, individual hazards.

9.6.11 **Safety reviews** are conducted during introduction and deployment of new technologies, change or implementation of procedures, or in situations of structural change in operations. Safety reviews are a fundamental component of the management of change, discussed in Section 9.8. They have a clearly a defined objective that is linked to the change under consideration. For example, an airport is considering implementing Airport Surface Detection Equipment (ASDE). Therefore, the objective of the safety review would be to assess the safety risks associated with implementing an ASDE in XYZ airport by evaluating the appropriateness and effectiveness of the safety management activities related to the project. Safety reviews are conducted by Safety Action Groups (SAG), which look for effective performance of the following safety management activities under the proposed changes:

- hazard identification and safety risk assessment/mitigation;
- safety measurement;
- management accountabilities;
- operational personnel skills;
- technical systems; and
- abnormal operations.

9.6.12 Once performance of each safety management activity under the proposed changes is reviewed, the SAG produces a list of hazards concerns for each activity, the response/mitigation proposed by the line manager, and an assessment of the appropriateness and effectiveness of the mitigations to address the hazards. The mitigation will be appropriate if it actually addresses the hazard. The mitigation will be effective if it consistently manages the safety risks under normal operating conditions in order to reduce the safety risks to ALARP. The SAG also proposes a prioritization of the responses/mitigations, by allocating importance and urgency to each hazard. Safety reviews thus ensure safety performance during periods of change, by providing a roadmap to safe and effective change.

9.6.13 **Audits** focus in the integrity of the organization's SMS, and periodically assess the status of safety risk controls. As with other requirements, the auditing requirements are left at a functional level, allowing for a broad range of complexity, commensurate with the complexity of the organization. While audits are "external" to the units involved in activities directly related with the provision of services, they are still "internal" to the organization as a whole. Audits are not intended to be in-depth audits of the technical processes but rather they are intended to provide assurance of the line units' safety management functions, activities and resources. Audits are used to ensure that the structure of the SMS is sound in terms of levels of staff, compliance with approved procedures and instructions, level of competency and training to operate equipment and facilities and maintain their levels of performance, etc.

9.6.14 **Safety surveys** examine particular elements or procedures of a specific operation, such as problem areas or bottlenecks in daily operations, perceptions and opinions of operational personnel and areas of dissent or confusion. Safety surveys may involve the use of checklists, questionnaires and informal confidential interviews. Since surveys information is subjective, verification may be needed before corrective action. Surveys may provide an inexpensive source of significant safety information.

9.6.15 **Internal safety investigations** include occurrences or events that are not required to be investigated or reported to State, although in some instances organizations may conduct internal investigations notwithstanding the fact that the event in question is investigated by the State. Examples of occurrences or events that fall within the scope of internal safety investigations include: in-flight turbulence (flight operations); frequency congestion (ATC); material failure (maintenance), and ramp vehicle operations (aerodrome).

9.6.16 In conclusion, the contribution of the sources of information for safety performance and monitoring to an organization SMS can be summarised as follows;

- hazard reporting is a primary source of information on hazards in operations;
- safety studies are a source of information on generic safety concerns and/or systemic safety deficiencies;
- safety reviews are linked to the management of change and ensure safety performance under changing operational conditions;
- audits ensure integrity of the SMS structures and processes;
- safety surveys sample expert opinion and perceptions on specific problem areas in daily operations; and
- internal safety investigations address outcomes of minor magnitude that are not required to be investigated by the State.

## 9.7 PROTECTION OF SOURCES OF SAFETY INFORMATION

9.7.1 International civil aviation's outstanding safety record is among others, due to two key factors: a continuous learning process, based on the development and free exchange of safety information; and the ability to turn errors into preventive actions. It has long been recognized that endeavours aimed at improving contemporary civil aviation safety must build upon empirical data. There are several sources of such data available to civil aviation. In combination, they provide the basis for a solid understanding of the strengths and weaknesses of aviation operations.

9.7.2 For years, information from accident and incident investigations formed the backbone of activities aimed at improvements in equipment design, maintenance procedures, flight crew training, air traffic control systems, aerodrome design and functions, weather support services, and other safety-critical aspects of the air transportation system. In recent years, the availability of technological means has led to an accelerated development of safety data collection, processing and exchange systems (hereafter referred to, in combination with accident and incident investigation and reporting, as Safety Data Collection and Processing Systems or SDCPS). SDCPS, as discussed in Chapter 3, form the pillars of an SMS, and generate information that is used to implement corrective safety actions and ongoing-term strategies.

9.7.3 SDCPS have allowed civil aviation to gain a deeper understanding of operational errors: why they happen, what can be done to minimize their occurrence, and how to contain their negative impact on safety. It remains undisputed

that hazards lead to operational errors in aviation that in their vast majority are inadvertent: well-trained, well-intentioned people make errors while maintaining, operating, or controlling well-designed equipment. For those rare situations where errors are a result of wilful acts, substance abuse, sabotage or violations, enforcement systems in place ensure that the chain of accountability remains unbroken. This dual approach, combining enhanced understanding of inadvertent operational errors with appropriate enforcement of rules in cases of misconduct, has served civil aviation well in terms of safety, while ensuring that there are no harbours for violators.

9.7.4 Recent years, however, have shown a trend in civil aviation when dealing with operational errors leading to occurrences, in that information from SDCPS has been used for disciplinary and enforcement purposes, as well as admitted as evidence in judicial proceedings. These proceedings have also resulted in criminal charges being brought against individuals involved in such occurrences. Bringing criminal charges into aviation occurrences resulting from inadvertent operational errors may hinder the development and free exchange of safety information which is essential to improve aviation safety, with a potential adverse effect on it.

9.7.5 A number of initiatives within the international civil aviation community have attempted to address the protection of SDCPS. However, given the sensitivity of the question at hand, a framework that provides unity of purpose and consistency among civil aviation's efforts is essential. Efforts to ensure the protection of safety information must strike a very delicate balance of interests between the need to protect safety information, and the responsibility to administer justice. A cautious approach should be taken in this regard to avoid making proposals which might be incompatible with laws pertaining to the administration of justice in Contracting States.

9.7.6 The 35th Session of the ICAO Assembly considered the subject of the protection of sources and free flow of safety information and adopted Resolution A35-17 – *Protecting information from safety data collection and processing systems in order to improve aviation safety.* This Resolution instructed the ICAO Council "to develop appropriate legal guidance that will assist States to enact national laws and regulations to protect information gathered from all relevant safety data collection and processing systems, while allowing for the proper administration of justice in the State."

9.7.7 As a first step in developing the legal guidance called for in Assembly Resolution A35-17, ICAO requested some States to provide examples of their relevant laws and regulations relating to the protection of information from SDCPS. Subsequently, ICAO conducted an analysis of the material received from States, seeking common threads and conceptual points from the laws and regulations provided. The legal guidance that resulted takes the form of a series of principles that have been distilled from such laws and regulations.

9.7.8 The guidance (contained in Attachment E to Annex 13 — *Aircraft Accident and Incident Investigation)* is aimed at assisting States enact national laws and regulations to protect information gathered from SDCPS, while allowing for the proper administration of justice. The objective is to prevent the inappropriate use of information collected solely for the purpose of improving aviation safety. Bearing in mind that States should be allowed the flexibility to draft their laws and regulations in accordance with their national policies and practices, the legal guidance takes the form of a series of principles that can be adapted to meet the particular needs of the State enacting laws and regulations to protect safety information. A brief outline of the guidance follows.

9.7.9 The legal guidance includes general principles stating that:

- The sole purpose of protecting safety information from inappropriate use is to ensure its continued availability so that proper and timely preventive actions can be taken and aviation safety improved;
- It is not the purpose of protecting safety information to interfere with the proper administration of justice in States;
- National laws and regulations protecting safety information should ensure that a balance is struck between the need for the protection of safety information in order to improve aviation safety, and the need for the proper administration of justice;
- National laws and regulations protecting safety information should prevent its inappropriate use, and
- Providing protection to qualified safety information under specified conditions is part of a State's safety responsibilities.

9.7.10 The guidance includes principles of protection, as follows:

- Safety information should qualify for protection from inappropriate use according to specified conditions that should include, but not necessarily be limited to: the collection of information was for explicit safety purposes and the disclosure of the information would inhibit its continued availability;
- The protection should be specific for each SDCPS, based upon the nature of the safety information it contains;

- A formal procedure should be established to provide protection to qualified safety information, in accordance with specified conditions;
- Safety information should not be used in a way different from the purposes for which it was collected; and
- The use of safety information in disciplinary, civil, administrative and criminal proceedings should be carried out only under suitable safeguards provided by national law.

9.7.11 The guidance provides that exceptions to the protection of safety information should only be granted by national laws and regulations when:

- there is evidence that the occurrence was caused by an act considered, in accordance with the law, to be conduct with intent to cause damage, or conduct with knowledge that damage would probably result, equivalent to reckless conduct, gross negligence or wilful misconduct;
- an appropriate authority considers that circumstances reasonably indicate that the occurrence may have been caused by conduct with intent to cause damage, or conduct with knowledge that damage would probably result, equivalent to reckless conduct, gross negligence or wilful misconduct; or
- a review by an appropriate authority determines that the release of the safety information is necessary for the proper administration of justice, and that its release outweighs the adverse domestic and international impact such release may have on the future availability of safety information.

9.7.12 The guidance also addresses the subject of public disclosure, proposing that, subject to the principles of protection and exception outlined above, and any person seeking disclosure of safety information should justify its release. Formal criteria for disclosure of safety information should be established and should include, but not necessarily be limited to, the following:

- disclosure of the safety information is necessary to correct conditions that compromise safety and/or to change policies and regulations;
- disclosure of the safety information does not inhibit its future availability in order to improve safety;
- disclosure of relevant personal information included in the safety information complies with applicable privacy laws; and
- disclosure of the safety information is made in a de-identified, summarized or aggregate form.

9.7.13 The guidance discusses the responsibility of the custodian of safety information, proposing that each SDCPS should have a designated custodian. It is the responsibility of the custodian of safety information to apply all possible protection regarding the disclosure of the information, unless:

- the custodian of the safety information has the consent of the originator of the information for disclosure; or
- the custodian of the safety information is satisfied that the release of the safety information is in accordance with the principles of exception.

9.7.14 Lastly, the guidance discusses the protection of recorded information, and considering that ambient workplace recordings required by legislation, such as cockpit voice recorders (CVRs), may be perceived as constituting an invasion of privacy for operational personnel that other professions are not exposed to, proposes that:

- subject to the principles of protection and exception above, national laws and regulations should consider ambient workplace recordings required by legislation as privileged protected information, i.e. information deserving enhanced protection; and national laws and regulations should provide specific measures of protection to such recordings as to their confidentiality and access by the public. Such specific measures of protection of workplace recordings required by legislation may include the issuance of orders of non-public disclosure.

## 9.8 THE MANAGEMENT OF CHANGE

9.8.1 Aviation organizations experience permanent change due to expansion, contraction, changes to existing systems, equipment, programmes, products and services, and introduction of new equipment or procedures. Hazards may inadvertently be introduced into an operation whenever change occurs. Safety management practices require that hazards

that are a by-product of change be systematically and proactively identified and those strategies to manage the safety risks of the consequences of hazards be developed, implemented and subsequently evaluated. Safety reviews, discussed in paragraph 9.6.11, are a valuable source of information and decision making under circumstances of change.

9.8.2 Change can introduce new hazards; impact the appropriateness of existing safety risk mitigation strategies, and/or impact the effectiveness of existing safety risk mitigation strategies. Changes may be external to the organization, or internal. Examples of external changes include changes of regulatory requirements, changes in security requirements, and reorganization of air traffic control. Examples of internal changes include management changes, new equipment and new procedures.

9.8.3 A formal process for the management of change should take into account the following three considerations:

- ***Criticality of systems and activities.*** Criticality is closely related to safety risk. Criticality relates to the potential consequences of equipment being improperly operated or an activity incorrectly executed – essentially answering the question, "how important is this equipment/activity to safe system operations?" While this is a consideration that should be made during the system design process, it becomes relevant during a situation of change. Clearly, some activities are more essential for safe delivery of services than others. For example, the changes in activities or procedures related to aircraft return to service after major maintenance in an organization that has first implemented its own maintenance organization after previously subcontracting third-party maintenance might be considered to be more safety critical than a similar scenario regarding changes in meal catering activities. Those equipments and activities that have higher safety criticality should be reviewed following change to make sure that corrective actions can be taken to control potentially emerging safety risks.

- ***Stability of systems and operational environments.*** Changes may be the result of programmed change such as growth, operations to new destinations, changes in fleets, changes in contracted services, or other changes directly under the control of the organization. Changes in the operational environment are also important, such as economic or financial status, labour unrest, changes in political or regulatory environments, or changes in the physical environment such as cyclical changes in weather patterns. While these factors are not under direct control of the organization, they must take action to respond to them. Frequent changes in either systems or operational environments dictate that managers need to update key information more frequently than in more stable situations. This is an essential consideration in management of change.

- ***Past performance.*** Past performance of critical systems is a proven indicator of future performance. This is where the closed-loop nature of safety assurance comes into play. Trend analyses in the safety assurance process should be employed to track safety performance measures over time and to factor this information into planning of future activities under situations of change. Moreover, where deficiencies have been found and corrected as a result of past audits, evaluations, investigations, or reports, it is essential that such information is considered to assure the effectiveness of corrective actions.

9.8.4 A formal management of change process should then identify changes within the organization which may affect established processes, procedures, products and services. Prior to implementing changes, a formal management of change process should describe the arrangements to ensure safety performance. The result of this process is the reduction in the safety risks resulting from changes in the provision of services by the organization to ALARP.

9.8.5 Chapter 7 discusses the importance of describing the system (system description) as one of the fundamental preliminary activities in the planning of an SMS. The objective of the system description is to determine a baseline hazard analysis for the baseline system. As system life evolves, seemingly small, incremental changes can accumulate over time in the system (or the environment which provides the context for the system operation), that will make the initial system description inaccurate. Therefore, as part of a formal process of the management of change, the system description and the baseline hazard analysis should be reviewed periodically, even if circumstances of change are not present, to determine their continued validity. When changes to the system are made, and periodically thereafter, an organization should go over its system, its anticipated, and its actual operational environment, to make sure it continues to hold a clear picture of the circumstances under which the provision of service takes place.

## 9.9 CONTINUOUS IMPROVEMENT OF THE SMS

9.9.1 Assurance builds on the principle of the continuous improvement cycle. In much the same way that quality assurance facilitates continuous improvements in quality, safety assurance ensures control of safety performance – including regulatory compliance – through constant verification and upgrading of the operational system. These objectives are achieved through the application of similar tools: internal evaluations and independent audits (both internal and external), strict document controls and on-going monitoring of safety controls and mitigation actions.

9.9.2 **Internal evaluations** involve the evaluation of the operational activities of the organization as well as the SMS-specific functions. Evaluations conducted for the purpose of this requirement must be conducted by persons or organizations that are functionally independent of the technical process being evaluated. A specialist safety or quality assurance department or another sub-organization as directed by senior management may accomplish it. The internal evaluation function also requires auditing and evaluation of the safety management functions, policymaking, safety risk management, safety assurance, and safety promotion. These audits provide the management officials designated responsibility for the SMS to inventory the processes of the SMS itself.

9.9.3 **Internal audits** are an important tool for managers to use to obtain information with which to make decisions and to keep operational activities on track. The primary responsibility for safety management rests with those who "own" the organization's technical activities supporting delivery of services. It is here where hazards are most directly encountered, where deficiencies in activities contribute to safety risk, and where direct supervisory control and resource allocation can mitigate the safety risk to ALARP. While internal audits are often thought of as tests or "grading" of an organization's activities, they are an essential tool for safety assurance, to help managers in charge of activities supporting delivery of services to control that, once safety risk controls they have been implemented, they continue to perform and that they are effective in maintaining continuing operational safety.

9.9.4 **External audits** of the SMS may be conducted by the regulator, code-share partners, customer organizations, or other third parties selected by the organization. These audits not only provide a strong interface with the oversight system but also a secondary assurance system.

9.9.5 Continuous improvement of the SMS thus aims at determining the immediate causes of below standard performance and their implications in the operation of the SMS, and rectifying situations involving below standard performance identified through safety assurance activities. Continuing improvement is achieved through internal evaluations, internal and external audits and it applies to:

- proactive evaluation of facilities, equipment, documentation and procedures, for example, through internal evaluations;
- proactive evaluation of the individuals' performance, to verify the fulfilment of their safety responsibilities, for example, through periodic competency checks ( form of evaluation/audit); and
- reactive evaluations in order to verify the effectiveness of the system for control and mitigation of safety risks, for example, through internal and external audits.

9.9.6 As conclusion, continuous improvement can only occur when the organization displays constant vigilance regarding the effectiveness of its technical operations and its corrective actions. Indeed, without on-going monitoring of safety controls and mitigation actions, there is no way of telling whether the safety management processes achieves its objectives. Similarly, there is no way of measuring if an SMS is fulfilling its purpose with efficiency.

## 9.10 THE RELATIONSHIP BETWEEN SAFETY RISK MANAGEMENT (SRM) AND SAFETY ASSURANCE (SA)

9.10.1 The subtleties related to the interrelationship between safety risk management and safety assurance are frequently a source of confusion. One of the first tasks in effective safety risk management and safety assurance is for both the service provider and the civil aviation oversight authority to have a thorough understanding of the configuration and structure of the organizational system and its activities. A significant number of hazards and safety risks exist from improper design of these activities or a poor fit between the system and its operational environment. In these cases, hazards to operational safety may be poorly understood and, therefore, inadequately controlled.

9.10.2 The safety risk management function of an SMS provides for initial identification of hazards and assessment of safety risks. Organizational safety risk controls are developed and, once they are determined to be capable of bringing the safety risk to ALARP, they are employed in daily operations. The safety assurance function takes over at this point to ensure that the safety risk controls are being practiced as intended and they continue to achieve their intended objectives. The safety assurance function also provides for the identification of the need for new safety risk controls because of changes in the operational environment.

9.10.3 In an SMS, the system's safety requirements are developed from, and based upon, an objective assessment of safety risks in the organization's activities supporting service delivery. The assurance side of the system concentrates upon the organization's proving (to itself and to appropriate external parties) that those requirements have been met, through collection and analysis of objective evidence.

9.10.4 The safety risk management function of an SMS, therefore, provides for the assessment of safety risks in operations supporting service delivery, as well as development of controls to bring the assessed risk to ALARP. It also supports safety decisions supporting relation to these activities. Once put into place, the safety assurance function of the SMS operates in a manner very similar to the quality assurance function in a QMS. In fact, the safety assurance functions of SMS

were derived almost directly from ISO 9001-2000, the international quality management standard. As already discussed, there is one significant difference: while typical QMS requirements are customer requirements and are based upon customer satisfaction, SMS requirements are safety requirements and are based upon safety satisfaction.

9.10.5 It is important to reiterate the roles of the two functions within the integrated processes of an SMS. The safety risk management (SRM) process provides for initial identification of hazards and assessment of risk. Safety risk controls are developed and, once they are determined to be capable of bringing the safety risk to ALARP, these controls are employed in daily operations. It is at this point that the safety assurance (SA) function takes over. Safety assurance ensures (i.e., give confidence) that organizational controls are being practiced and that all types of controls continue to achieve their intended objectives. This system also provides for assessment of the need for new controls due to changes in the operational environment. Figure 9-1 presents this discussion in visual format.

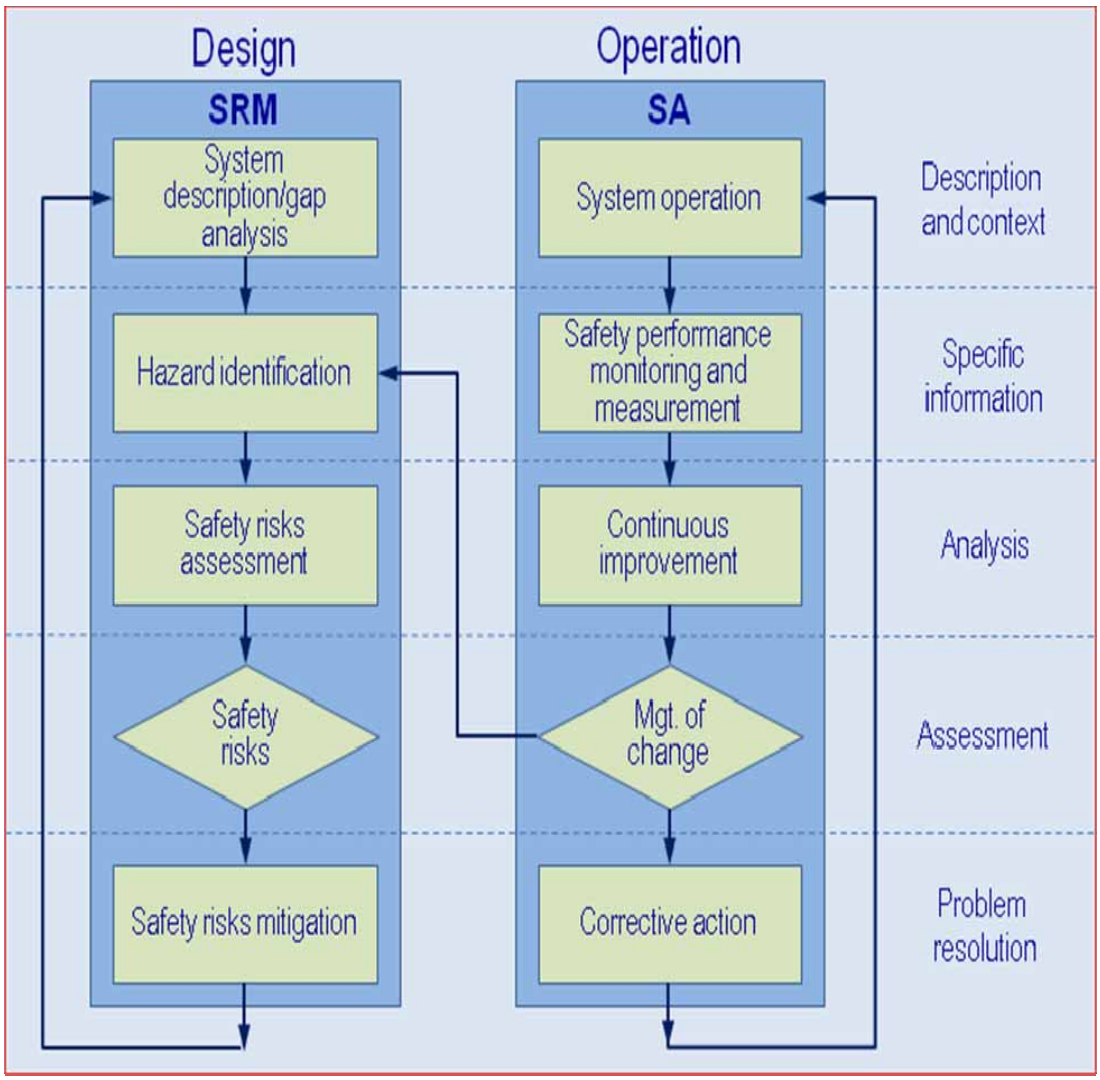



Figure 9-1 – Safety risk management process

## 9.11 SAFETY PROMOTION – TRAINING AND EDUCATION

9.11.1 An organizational safety effort cannot succeed by mandate or strictly though mechanistic implementation of policies. Safety promotion sets the tone that predisposes both individual and organizational behaviour, and fills in the blank spaces in the organization's policies, procedures, and processes, providing a sense of purpose to safety efforts.

9.11.2 Many of the processes and procedures specified in the safety policy and objectives, and safety risk management and safety assurance components of the SMS provide the structural building blocks of an SMS. However, the organization must also set in place processes and procedures that allow for communication among operational personnel and

with the organization's management. Organizations must make every effort to communicate their objectives, as well as the current status of the organization's activities and significant events. Likewise, organizations must supply a means of upward communication in an environment of openness.

9.11.3 Safety promotion includes:

- training and education, including safety competency; and
- safety communication

9.11.4 The Safety Manager provides current information and training related to safety issues relevant to the specific operations and operational units of the organization. The provision of appropriate training to all staff, regardless of their level in the organization, is an indication of management's commitment to an effective SMS. Safety training and education should consist of the following:

- a documented process to identify training requirements;
- a validation process that measures the effectiveness of training;
- initial (general safety) job-specific training;
- indoctrination/initial training incorporating SMS, including Human Factors and organizational factors; and
- recurrent safety training.

9.11.5 Training requirements and activities should be documented for each area of activity within the organization. A training file should be developed for each employee, including management, to assist in identifying and tracking employee training requirements and verifying that the personnel have received the planned training. Training programmes should be adapted to fit the needs and complexity of the organization.

9.11.6 Safety training within an organization must ensure that personnel are trained and competent to perform their safety management duties. The SMS Manual (SMSM) should specify initial and recurrent safety training standards for operational personnel, managers and supervisors, senior managers and the Accountable Executive. The amount of safety training should be appropriate to the individual's responsibility and involvement in the SMS. The SMSM should also specify responsibilities for the safety training, contents and frequency, validation and safety training records management.

9.11.7 Safety training should follow a building block approach. Safety training for operational personnel should address safety responsibilities, including following all operating and safety procedures, and recognizing and reporting hazards. The training objectives include the organization's safety policy and SMS fundamentals and overview. The contents include the definition of hazards, consequences and risks, the safety risk management process, including roles and responsibilities and, quite fundamentally, safety reporting and the organization's safety reporting system(s).

9.11.8 Safety training for managers and supervisors should address safety responsibilities, including promoting the SMS and engaging operational personnel in hazard reporting. In addition to the training objectives established for operational personnel, training objectives for managers and supervisors should add a detailed knowledge of the safety process, hazard identification and safety risk assessment and mitigation, and change management. In addition to the contents specified for operational personnel, the training contents for supervisors and managers should include safety data analysis.

9.11.9 Safety training for senior managers should include safety responsibilities including compliance with national and organizational safety requirements, allocation of resources, ensuring effective inter-departmental safety communication and active promotion of the SMS. In addition to the objectives of the two previous employee groups, safety training for senior managers should add safety assurance and safety promotion, safety roles and responsibilities, and establishing acceptable level(s) of safety. (Figure 9-2)

9.11.10 Lastly, safety training should include a special safety training for the Accountable Executive. This training session should be reasonably brief (it should not exceed one-half day), and it should intended to provide the Accountable Executive with a general awareness of the organization's SMS, including SMS roles and responsibilities, safety policy and objectives, safety risk management and safety assurance.

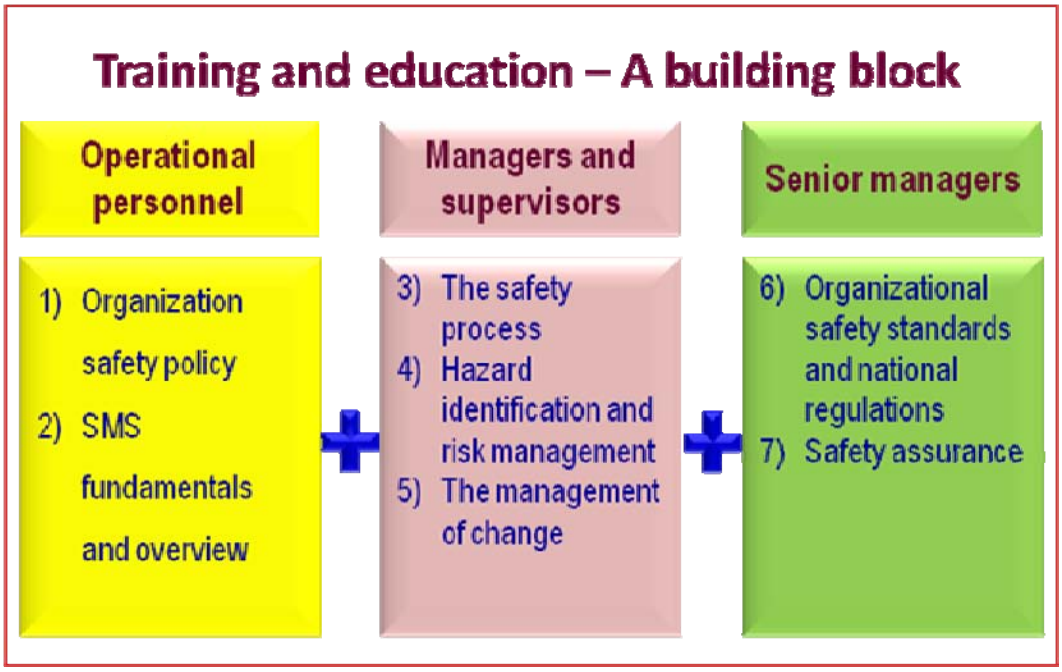



**Figure 9-2 – safety training**

## 9.12 SAFETY PROMOTION – SAFETY COMMUNICATION

9.12.1 The organization should communicate SMS objectives and procedures to all operational personnel, and the SMS should be visible in all aspects of the organization's operations supporting delivery of services. The Safety Manager should communicate the performance of the organization's SMS programme through bulletins and briefings. The Safety Manager should also ensure that lessons learned from investigations and case histories or experiences, both internally and from other organizations, are distributed widely. The communication should flow between the Safety Manager and operational personnel throughout the organization. Safety performance will be more efficient if operational personnel are actively encouraged to identify and report hazards. Safety communication therefore aims to:

- ensure that all staff are fully aware of the SMS;
- convey safety critical information;
- explain why particular actions are taken;
- explain why safety procedures are introduced or changed; and
- convey "nice-to-know" information.

9.12.2 Examples of organizational communication include:

- Safety Management System Manual (SMSM)
- safety processes and procedures;
- safety newsletters, notices and bulletins; and
- Web sites or email.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Chapter 10

# PHASED APPROACH TO SMS IMPLEMENTATION

## 10.1 OBJECTIVE AND CONTENTS

10.1.1 The objective of this chapter is to introduce a proposal for an implementation in phases of an SMS. The chapter includes the following:

- Why a phased approach to SMS?
- Phase I – Planning SMS implementation
- Phase II – Reactive safety management processes
- Phase III – Proactive and predictive safety management processes
- Phase IV – Operational safety assurance

## 10.2 WHY A PHASED IMPLEMENTATION?

10.2.1 The implementation of an SMS is a straightforward process. Nevertheless, depending on a number of factors, such as availability of guidance material published by the civil aviation oversight authority, knowledge regarding SMS within the service providers and resources for implementation, this straightforward process may turn into a daunting task.

10.2.2 It is axiomatic in project management that complex projects are best progressed by breaking down the overall complexity of the task at hand into smaller, manageable subcomponents of the overall task. In this way, overwhelming and sometimes confusing complexity, and its underlying workload, may be turned into simpler and transparent subsets of activities that only require a manageable workload. Likewise, the necessary resources to implement SMS "in one shot" might simply be unavailable to the organization. Thus, breaking down the overall complexity into smaller subsets of activities allows for a partial, smaller allocations of resources to complete subsets of activities. This partial allocation of resources may be more commensurate with the requirements of each activity as well as the resources available to the organization. Therefore, the first two reasons that justify why a phased approach to SMS implementation is proposed can be expressed as (a) providing a manageable series of steps to follow in implementing an SMS, including allocation of resources; and (b) effectively managing the workload associated with SMS implementation.

10.2.3 A third reason, quite distinct from the previous two reasons, but equally important, is avoiding "cosmetic compliance". An organization should set as its objective the realistic implementation of an effective SMS, not the tokens of it. It would be quite appealing for an organization unduly burdened with requirements, and without the resources to fully implement an SMS in its entirety in an insufficient period of time, to produce all the paperwork that would conform the demands and requirements of a civil aviation oversight authority. In other words, a situation referred to by the parochial expression "ticking boxes" might develop, as result of unreasonably demanding implementation requirements. Should such be the case, the resulting SMS, although complete and compliant in paper, would be nothing more than an empty shell. By providing a series of small, incremental and, most important, measurable steps, cosmetic compliance and "ticking boxes" is discouraged. Full SMS implementation will certainly take longer, but the robustness of the resulting SMS will be enhanced as each implementation phase is completed and simpler safety management processes are started before moving on into successive phases involving safety management processes of greater complexity.

10.2.4 In summary, the proposal for a phased implementation of SMS aims at:

- providing a manageable series of steps to follow in implementing an SMS, including allocation of resources;
- effectively managing the workload associated with SMS implementation; and
- pre-empting a "ticking boxes" exercise.

10.2.5 Four implementation phases are proposed for an SMS. Each phase is associated to a component of the ICAO SMS framework introduced in Chapter 8. The implementation of each phase is based upon the introduction of specific elements of each component of the ICAO SMS framework during the phase in question.

## 10.3 PHASE I – PLANNING SMS IMPLEMENTATION

10.3.1 The objectives of Phase I of SMS implementation are to provide a blueprint on how the SMS requirements will be met and integrated to the organization's work activities, as well as an accountability framework for the implementation of the SMS.

10.3.2 During Phase I, basic planning and assignment of responsibilities are established. Central to the Phase I is the gap analysis. From this gap analysis, an organization can determine the current status of its safety management processes. From here, detailed planning for the development of further safety management processes can be done. One significant output of Phase I is the SMS implementation plan.

10.3.3 At the completion of Phase I, the following activities should be finalised in such a manner that meets the expectations of the civil aviation oversight authority, as set forth in relevant requirements and guidance material:

- Identify the Accountable Executive and the safety accountabilities of managers. This activity is based upon Elements 1.1 and 1.2 of the ICAO SMS framework, and discussed in Chapter 8 of this Manual.

- Identify the person (or planning group) within the organization responsible for implementing the SMS. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapter 8 of this Manual.

- Describe the system (Approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes). This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapter 7 of this Manual. Guidance on a system description is also included as in Appendix 1 to Chapter 7 of this Manual.

- Conduct a gap analysis of the organization's existing resources compared with the national and international requirements for establishing a SMS. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapter 7 of this Manual. Guidance on an SMS gap analysis for a service provider is also included as in Appendix 2 to Chapter 7of this Manual.

- Develop an SMS implementation plan that explains how the organization will implement the SMS on the basis of national requirements and international SARPs, the system description and the results of the gap analysis. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapter 8 of this Manual.

- Develop documentation relevant to safety policy and objectives. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapter 8 of this Manual, including an example of a safety policy statement.

- Develop and establish means for safety communication. This activity is based upon Element 4.2 of the ICAO SMS framework, and discussed in Chapter 9 of this Manual.

## 10.4 PHASE II – REACTIVE SAFETY MANAGEMENT PROCESSES

10.4.1 The objective of Phase II is to implement essential safety management processes, while at the same time correcting potential deficiencies in existing safety management processes. Most organizations will have some basic safety management activities in place, at different levels of implementation and with different degrees of effectiveness. These activities may include inspections and audits reports, analysis of information from accident reports and incident investigations, and employee reports. This phase aims at solidifying existing activities, and developing those which do not exist yet. However, because forward looking systems have yet to be developed and implemented, this phase is considered reactive. Towards the end of Phase I, the organization will be ready to perform coordinated safety analyses based on information obtained through reactive methods of safety data collection.

10.4.2 At the completion of Phase II, the following activities should be finalised in such a manner that meets the expectations of the civil aviation oversight authority as set forth in relevant requirements and guidance material:

- Implement those aspects of the SMS implementation plan that refer to the safety risk management based on reactive processes. This activity is based upon Elements 2.1 and 2.2 of the ICAO SMS framework, and discussed in Chapters 3 and 8 of this Manual.

- Deliver training relevant the SMS implementation plan components and to safety risk management based on reactive processes. This activity is based upon Element 4.1 of the ICAO SMS framework, and discussed in Chapters 3, 8 and 9 of this Manual.

- Develop documentation relevant to the SMS implementation plan components and to safety risk management based on reactive processes. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapters 3, 8 and 9 of this Manual.

- Maintain means for safety communication. This activity is based upon Element 4.2 of the ICAO SMS framework, and discussed in Chapter 9 of this Manual.

## 10.5 PHASE III – PROACTIVE AND PREDICTIVE SAFETY MANAGEMENT PROCESSES

10.5.1 The objective of Phase III is to structure forward looking safety management processes. Safety information management and analytical processes are refined. Towards the end of Phase II, the organization will be ready to perform coordinated safety analyses based on information obtained through reactive, proactive and predictive methods of safety data collection.

10.5.2 At the completion of Phase III, the following activities should be finalised in such a manner that meets the expectations of the civil aviation oversight authority as set forth in relevant requirements and guidance material:

- Implement those aspects of the SMS implementation plan that refer to the safety risk management based on proactive and predictive processes. This activity is based upon Elements 2.1 and 2.2 of the ICAO SMS framework, and discussed in Chapters 3 and 8 of this Manual.

- Develop training relevant the SMS implementation plan components and to safety risk management based on proactive and predictive processes. This activity is based upon Element 4.1 of the ICAO SMS framework, and discussed in Chapters 3, 8 and 9 of this Manual.

- Develop documentation relevant to the SMS implementation plan components and to safety risk management based on proactive and predictive processes. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapters 3, 8 and 9 of this Manual.

- Maintain means for safety communication. This activity is based upon Element 4.2 of the ICAO SMS framework, and discussed in Chapter 9 of this Manual.

## 10.6 PHASE IV– OPERATIONAL SAFETY ASSURANCE

10.6.1 Phase IV is the final mature phase of the SMS. In this Phase operational safety assurance is assessed through the implementation of periodic auditing, feedback and continuous corrective action to maintain the effectiveness of safety risk controls under changing operational demands. At the end of Phase IV, safety information management and analytical processes ensure sustenance of safe organizational processes over time and changes in the operational environment.

10.6.2 At the completion of Phase IV, the following activities should be finalised in such a manner that meets the expectations of the civil aviation oversight authority as set forth in relevant requirements and guidance material:

- Development and agreement on safety performance indicators and safety performance targets, and SMS continuous improvement. This activity is based upon Elements 1.1, 3.1, 3.2 and 3.3 of the ICAO SMS framework, and discussed in Chapters 6 and 9 of this Manual.

- Develop training relevant to operational safety assurance. This activity is based upon Element 4.1 of the ICAO SMS framework, and discussed in Chapter 9 of this Manual.

- Develop documentation relevant to operational safety assurance. This activity is based upon Element 1.5 of the ICAO SMS framework, and discussed in Chapter 9 of this Manual.

- Maintain means for safety communication. This activity is based upon Element 4.2 of the ICAO SMS framework, and discussed in Chapter 9 of this Manual.

10.6.3 A summary of the different phases of the SMS implementation and corresponding elements is shown in Figure 10-1 hereunder.

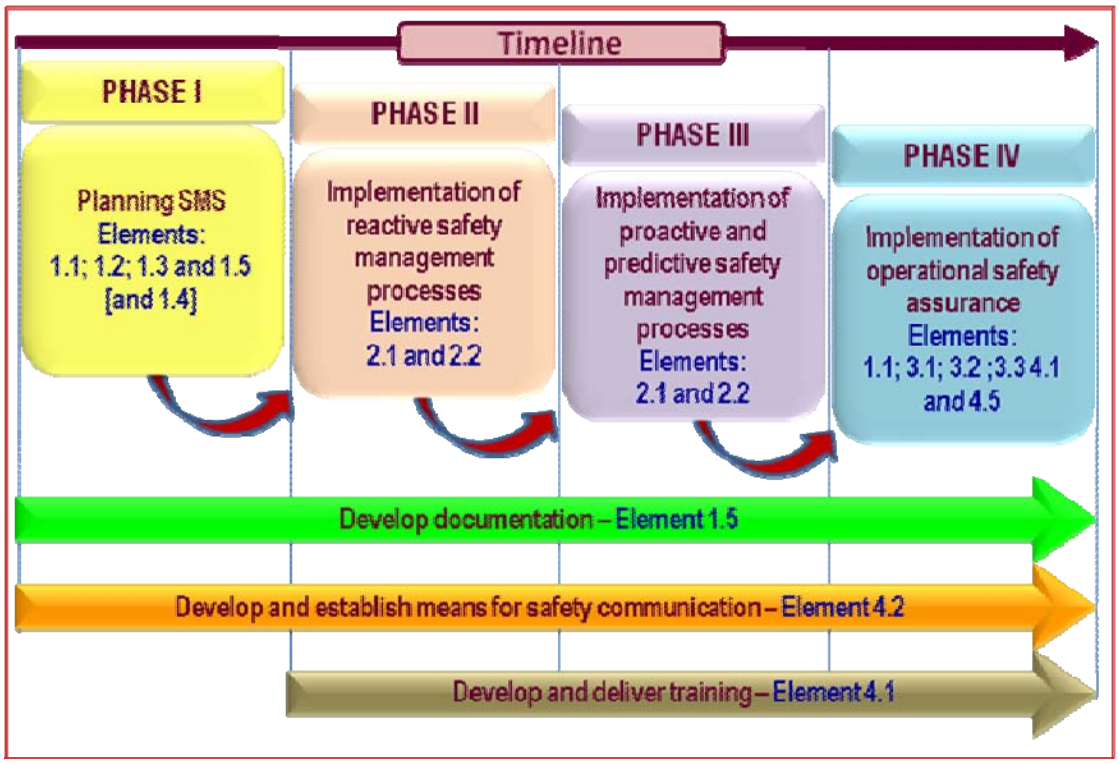



Figure 10-1 – SMS implementation phases – Summary

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 1 to Chapter 10

# GUIDANCE ON THE DEVELOPMENT OF A STATE'S REGULATION ON SMS

## 1. STATUTORY BASIS

This regulation is promulgated under the statutory authority in *[State's applicable civil aviation regulation(s), air navigation order(s) or regulatory standard(s)]*

## 2. SCOPE AND APPLICABILITY

### 2.1 Scope

2.1.1 This regulation specifies the requirements for a service provider safety management system (SMS) operating in accordance with *Annex 1 — Personnel Licensing, Annex 6 — Operation of Aircraft, Part I — International Commercial Air Transport — Aeroplanes and Part III — International Operations — Helicopters, Annex 8 — Airworthiness of Aircraft, Annex 11 — Air Traffic Services, and Annex 14 — Aerodromes, Volume I — Aerodrome Design and Operation,*

2.1.2 Within the context of this guidance the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to operational safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.

2.1.3 This regulation addresses aviation safety related processes, procedures and activities rather than occupational safety, environmental protection, or customer service or product quality.

2.1.4 The service provider is responsible for the safety of services or products contracted or sub-contracted to or purchased from other organizations.

2.1.5 This regulation establishes the minimum acceptable requirements; the service provider can establish more stringent requirements.

### 2.2 Applicability and acceptance

2.2.1 Effective *[date(s)],* a service provider shall have in place a safety management system (SMS) acceptable to *[State]* that, as a minimum:

2.2.1.1 identifies safety hazards;

2.2.1.2 ensures the implementation of remedial action necessary to maintain agreed safety performance;

2.2.1.3 provides for continuous monitoring and regular assessment of the safety performance; and

2.2.1.4 aims at a continuous improvement of the overall performance of the safety management system.

2.2.2 In order to be acceptable to the State, a service provider SMS shall meet the requirements set forth in this regulation.

*Information note. – A regulation on SMS should include information regarding the acceptance process for the SMS. The acceptance process should include, as applicable, the application for SMS acceptance, the procedure(s) to submit the application, the duration of the acceptance, the renewal of the acceptance, and the suspension and/or revocation of the acceptance.*

## 3. REFERENCES

3.1 This regulation is in accordance with *Annex 1 — Personnel Licensing, Annex 6 — Operation of Aircraft, Part I — International Commercial Air Transport — Aeroplanes and Part III — International Operations — Helicopters, Annex 8 — Airworthiness of Aircraft, Annex 11 — Air Traffic Services, and Annex 14 — Aerodromes, Volume I — Aerodrome Design and Operation,* and the ICAO Safety Management Manual (Doc 9859).

3.2 This regulation is in accordance with *[applicable regulatory and/or guidance material by the State]*.

## 4. DEFINITIONS

***Note**. – List intended as guidance only.*

- Accident
- Acceptable Level of Safety (ALoS)
- Accountable Executive
- Consequence
- Continuous monitoring
- Gap analysis
- Hazard
- Incident
- Internal safety investigations
- Mitigation
- Occurrence
- Oversight
- Predictive
- Proactive
- Probability
- Procedure
- Process
- Reactive
- Risk
- Safety
- Safety assessment
- Safety assurance
- Safety audit
- Safety Manager
- Safety performance
- Safety performance indicator
- Safety performance target
- Safety policy
- Safety requirement
- Safety risk
- Safety survey
- Safety management system (SMS)
- State Safety programme (SSP)
- Severity
- System description

## 5. GENERAL

5.1 A service provider shall develop, establish, maintain and adhere to a safety management system (SMS) that is appropriate to the size, nature and complexity of the operations authorized to be conducted under its operations certificate and the hazards and safety risks related to the operations.

## 6. SAFETY POLICY AND OBJECTIVES

### 6.1 General requirements

6.1.1 A service provider shall define the organization's safety policy.

6.1.2 The safety policy shall be signed by the Accountable Executive of the organization.

6.1.3 The safety policy shall include the responsibilities of management and employees with respect to the safety performance of the SMS.

6.1.4 The safety policy shall include a clear statement about the provision of the necessary resources for its implementation.

6.1.5 The safety policy shall be communicated, with visible endorsement, throughout the organization.

6.1.6 The safety policy shall also include, *inter alia*:

6.1.6.1 a commitment to continual improvement in the level of safety;

6.1.6.2 the hazard reporting procedures; and

6.1.6.3 the conditions under which disciplinary action would be not be applicable following hazard reporting by employees.

6.1.7. The safety policy shall be in accordance with all applicable legal requirements and international standards, best industry practices and shall reflect organizational commitments regarding safety.

6.1.8 The safety policy shall be reviewed periodically to ensure it remains relevant and appropriate to the organization.

6.1.8 A service provider shall establish safety objectives for the SMS.

6.1.9 The safety objectives should be linked to the safety performance indicators, safety performance targets and safety requirements of the service provider's SMS.

### 6.2 SMS organizational arrangements and safety accountabilities and responsibilities

6.2.1 A service provider shall identify an Accountable Executive to be responsible and accountable on behalf of the service provider for meeting the requirements of this regulation, and shall notify *[State]* the name of the person.

6.2.2 The Accountable Executive shall be a single, identifiable person who, irrespective of other functions, shall have ultimate responsibility and accountability, on behalf of the [organization], for the implementation and maintenance of the SMS

6.2.3 The Accountable Executive shall have:

6.2.3.1 full control of the human resources required for the operations authorized to be conducted under the operations certificate;

6.2.3.2 full control of the financial resources required for the operations authorized to be conducted under the operations certificate;

6.2.3.3 final authority over operations authorized to be conducted under the operations certificate;

6.2.3.4 direct responsibility for the conduct of the organization's affairs; and

6.2.3.5 final responsibility for all safety issues.

6.2.4 A service provider shall establish the necessary organizational arrangements for the implementation, adherence and maintenance of the organization's SMS.

6.2.5 A service provider shall identify the safety accountabilities, responsibilities and authorities of all members of management as well as of all employees, irrespective of other responsibilities.

6.2.6 Safety-related accountabilities, responsibilities and authorities shall be defined, documented and communicated throughout the organization.

6.2.7 A service provider shall identify a safety manager to be the member of management to be the responsible individual and focal point for the implementation and maintenance of an effective SMS.

6.2.8 The Safety Manager shall *inter alia*.

6.2.8.1 ensure that processes needed for the SMS are developed, implemented adhered to and maintained;

6.2.8.2 report to the Accountable Executive on the performance of the SMS and on any need for improvement; and

6.2.8.3 ensure safety promotion throughout the organization.

## 6.3 Coordination of emergency response planning

6.3.1 A service provider shall ensure its emergency response plan is properly coordinated with the emergency response plans of those organizations it must interface with during the provision of its services.

6.3.2 The coordination of the emergency response planning shall ensure the orderly and efficient transition from normal to emergency operations and the return to normal operations

6.3.2 The coordination of emergency response plan shall include, *inter alia*.

6.3.1.1 the designation of emergency authority;

6.3.1.2 the assignment of emergency responsibilities during the coordinated activities;

6.3.1.3 the coordination of efforts to cope with the emergency; and

6.3.1.4 the compatibility with other emergency response plans of other organizations.

## 6.4 Documentation

6.4.1 A service provider shall develop and maintain SMS documentation to describe:

6.4.1.1 the safety policy and objectives;

6.4.1.2 the SMS requirements;

6.4.1.3 the SMS processes and procedures;

6.4.1.4 the accountabilities, responsibilities and authorities for processes and procedures; and

6.4.1.5 the SMS outputs.

6.5.6 A service provider shall, as part of the SMS documentation, complete a system description.

6.5.7 The system description shall include the following:

6.3.6.1 the system interactions with other systems in the air transportation system;

6.3.6.2 the system functions;

6.3.6.3 required human performance considerations of the system operation;

6.3.6.4 hardware components of the system;

6.3.6.5 software components of the system;

6.3.6.6 related procedures that define guidance for the operation and use of the system;

6.3.3.7 operational environment; and

6.3.3.8 contracted, sub-contracted and purchased products and/or services.

6.3.7 A service provider shall, as part of the SMS documentation, complete a gap analysis, in order to:

6.3.7.1 identify the safety arrangements and structures that may be already exist throughout an organization; and

6.3.7.2 determine additional safety arrangements required to implement and maintain the organization's SMS.

6.5.2 A service provider shall, as part of the SMS documentation, develop, adhere to and maintain an SMS implementation plan.

6.5.3 The SMS implementation plan shall be the definition of the approach the organization will adopt for managing safety in a manner that will meet the organization's safety objectives.

6.3.8 The SMS implementation plan shall explicitly address the coordination between the SMS of the service provider and the SMS of other organizations the service provider must interface with during the provision of services

6.5.4 The SMS implementation plan shall include the following:

6.5.4.1 safety policy and objectives;

6.5.4.2 system description;

6.5.4.3 gap analysis;

6.5.4.4 SMS components;

6.5.4.5 safety roles and responsibilities;

6.5.4.6 hazard reporting policy:

6.5.4.7 means of employee involvement;

6.5.4.8 safety performance measurement

6.5.4.9 safety training;

6.5.4.10 safety communication; and

6.5.4.11 management review of safety performance.

6.5.5 The SMS implementation plan shall be endorsed by senior management of the organization.

6.5.3 A service provider shall, as part of the SMS documentation, develop and maintain a safety management system manual (SMSM), to communicate the organization's approach to safety throughout the organization.

6.5.4 The SMSM shall document all aspects of the SMS, and its contents shall include the following:

6.5.4.1 scope of the safety management system;

6.5.4.2 safety policy and objectives;

6.5.4.3 safety accountabilities;

6.5.4.4 key safety personnel;

6.5.4.5 documentation control procedures;

6.5.4.6 coordination of emergency response planning;

6.5.4.7 hazard identification and risk management schemes;

6.5.4.8 safety performance monitoring;

6.5.4.9 safety auditing;

6.5.4.10 procedures for the management of change;

6.5.4.11 safety promotion; and

6.5.4.12 control of contracted activities.

***Information note.*** *– Generic guidelines for SMS documentation development and maintenance can be found in Attachment H to ICAO Annex 6, Part I, and Attachment G to ICAO Annex 6, Part III, Operator's Flight Safety Documents System.*

## 7. SAFETY RISK MANAGEMENT

### 7.1 General

7.1.1 A service provider shall develop and maintain a formal process that ensures that hazards in operations are identified

7.1.2 A service provider shall develop and maintain safety data collection and processing systems (SDCPS) that provide for the identification of hazards and the analysis, assessment and mitigation of safety risks.

7.1.3 A service provider's SDCPS shall include reactive, proactive and predictive methods of safety data collection.

### 7.2 Hazard identification

7.2.1 A service provider shall develop and maintain formal means for effectively collecting, recording, acting on and generating feedback about hazards in operations, which combine reactive, proactive and predictive methods of safety data collection. Formal means of safety data collection shall include mandatory, voluntary and confidential reporting systems.

7.2.2 The hazard identification process shall include the following steps:

7.2.2.1 reporting of hazards, events or safety concerns;

7.2.2.2 collection and storing the safety data;

7.2.2.3 analysis of the safety data; and

7.2.2.4 distribution of the safety information distilled from the safety data.

### 7.3 Safety risk assessment and mitigation

7.3.1 A service provider shall develop and maintain a formal process that ensures analysis, assessment and control of the safety risks of the consequences of hazards during the provision of its services

7.3.2 The safety risks of the consequences of each hazard identified through the hazard identification processes described in section 7.2 of this regulation shall be analysed in terms of probability and severity of occurrence, and assessed for their tolerability.

7.3.3 The organization shall define the levels of management with authority to make safety risk tolerability decisions.

7.3.4 The organization shall define safety controls for each safety risk assessed as tolerable.

## 8. SAFETY ASSURANCE

### 8.1 General

8.1.1 A service provider shall develop and maintain safety assurance processes to ensure that the safety risks controls developed as a consequence of the hazard identification and safety risk management activities under paragraph 7 achieve their intended objectives.

8.1.2 Safety assurance processes shall apply to an SMS whether the activities and/or operations are accomplished internally or outsourced.

### 8.2 Safety performance monitoring and measurement

8.2.1 A service provider shall, as part of the SMS safety assurance activities, develop and maintain the necessary means to verify safety performance of the organization in reference to the safety performance indicators and safety performance targets of the SMS, and to validate the effectiveness of safety risk controls.

8.2.2 Safety performance monitoring and measurement means shall include the following:

8.2.2.1 hazard reporting systems;

8.2.2.2 safety audits;

8.2.2.3 safety surveys;

8.2.2.4 safety reviews;

8.2.2.5 safety studies; and

8.2.2.6 internal safety investigations

8.2.3 The hazard reporting procedures shall set out the conditions to ensure effective reporting, including the conditions under which disciplinary / administrative action shall not apply.

### 8.3 Management of change

8.3.1 A service provider shall, as part of the SMS safety assurance activities, develop and maintain a formal process for the management of change.

8.3.2 The formal process for the management of change shall:

8.3.2.1 identify changes within the organization which may affect established processes and services;

8.3.2.2 describe the arrangements to ensure safety performance before implementing changes; and

8.3.3.3 eliminate or modify safety risk controls that are no longer needed due to changes in the operational environment.

### 8.4 Continuous improvement of the safety system

8.4.1 A service provider shall, as part of the SMS safety assurance activities, develop and maintain formal processes to identify the causes of below standard performance of the SMS, determine the implications in its operation, and rectify situations involving below standard performance in order to ensure the continual improvement of the SMS.

8.4.2 Continuous improvement of the service provider SMS shall include:

8.4.2.1 proactive and reactive evaluations of facilities, equipment, documentation and procedures, to verify the effectiveness of strategies for control of safety risks; and

8.4.2.2 proactive evaluation of the individuals' performance, to verify the fulfilment of safety responsibilities.

## 9. SAFETY PROMOTION

### 9.1 General

9.1.1 Service providers shall develop and maintain formal safety training and safety communication activities to create an environment where the safety objectives of the organization can be achieved.

### 9.2 Safety training

9.2.1 A service provider shall, as part of its safety promotion activities, develop and maintain a safety training programme that ensures that personnel are trained and competent to perform the SMS duties.

9.2.2 The scope of the safety training shall be appropriate to the individual's involvement in the SMS.

9.2.3 The Accountable Executive shall receive safety awareness training regarding:

9.2.3.1 safety policy and objectives;

9.2.3.2 SMS roles and responsibilities;

9.2.3.3 SMS standards; and

9.2.3.4 safety assurance.

### 9.3 Safety communication

9.3.1 A service provider shall, as part of its safety promotion activities, develop and maintain formal means for safety communication, to:

9.3.1.1 ensure that all staff is fully aware of the SMS;

9.3.1.2 convey safety critical information;

9.3.1.3 explain why particular safety actions are taken;

9.3.1.4 explain why safety procedures are introduced or changed; and

9.3.1.5 convey generic safety information.

9.3.2 Formal means of safety communication shall include *inter alia*.

9.3.2.1 safety policies and procedures;

9.3.2.2 newsletters

9.3.2.3 bulletins; and

9.3.2.4 websites

## 10. QUALITY POLICY

10.1 A service provider shall ensure that the organization quality policy is consistent with, and supports the fulfilment of the activities of the SMS.

## 11. IMPLEMENTATION OF THE SMS

11.1 This regulation proposes, but does not mandate, a phased implementation of a service provider SMS, which encompasses four phases as described in paragraph 11.2 through paragraph 11.5 hereunder.

11.2 **Phase 1** – *Planning* should provide a blueprint on how the SMS requirements will be met and integrated to the organization's work activities, and an accountability framework for the implementation of the SMS:

11.2.1 Identify the Accountable Executive and the safety accountabilities of managers;

11.2.2 Identify the person (or planning group) within the organization responsible for implementing the SMS;

11.2.3 Describe the system (ATO, Air operators, AMO, organizations responsible for design and/or manufacture of aircraft, ATC services providers, certified aerodromes);

11.2.4 Conduct a gap analysis of the organization's existing resources compared with the national and international requirements for establishing an SMS;

11.2.5 Develop an SMS implementation plan that explains how the organization will implement the SMS on the basis of national requirements and international SARPs, the system description and the results of the gap analysis;

11.2.6 Develop documentation relevant to safety policy and objectives; and

11.2.7 Develop and establish means for safety communication.

11.3 **Phase 2** – *Reactive processes* should put into practice those elements of the SMS implementation plan that refer to safety risk management based on reactive processes:

11.3.1 hazard identification and risk management using reactive processes;

11.3.2 training relevant to:

11.3.2.1 SMS implementation plan components; and

11.3.2.2 safety risk management (reactive processes).

11.3.4 documentation relevant to:

11.3.4.1 SMS implementation plan components; and

11.3.4.2 safety risk management (reactive processes).

11.4 **Phase 3** – *Proactive and predictive processes* should put into practice those elements of the SMS implementation plan that refer to safety risk management based on proactive and predictive processes:

11.4.1 hazard identification and risk management using proactive and predictive processes

11.4.2 training relevant to:

11.4.2.1 SMS implementation plan components; and

11.4.2.2 safety risk management (proactive and predictive processes).

11.4.3 documentation relevant to:

11.4.4.1 SMS implementation plan components; and

11.4.4.2 safety risk management (proactive and predictive processes).

11.5 **Phase 4** – *Operational safety assurance* should put into practice operational safety assurance:

11.5.1 development and agreement on safety performance indicators and safety performance targets;

11.5.2 SMS continuous improvement;

11.5.3 training relevant to operational safety assurance; and;

11.5.4 documentation relevant to operational safety assurance.

11.5.5 maintain means for safety communication

- - - - - - - - - - - - - - -

# Appendix 2 to Chapter 10

# GUIDANCE ON AN SMS IMPLEMENTATION PLAN FOR SERVICE PROVIDERS

## 1. Background

This appendix provides guidance to assist service providers in developing an SMS implementation plan that defines the organization's approach to the management of safety. The SMS implementation plan shall be endorsed by senior management of the organization and developed on the basis of national regulations, International Standards and Recommended Practices (SARPs), the system description and the results of a gap analysis.

The development of an SMS implementation plan will also:

- assist service providers in preparing a realistic strategy for the implementation of an SMS that will meet the organization's safety objectives;
- provide a manageable series of steps to follow in implementing an SMS; and
- provide an accountability framework for the implementation of the SMS.

A phased approach is proposed to assist in effectively manage the workload associated with SMS implementation. Each phase is based upon the introduction of specific elements of the ICAO SMS framework.

The timeline for the implementation of each phase shall be commensurate with the size of the organization and complexity of the services provided.

*Note 1. – A model Gantt chart for the development of the SMS implementation plan is included in this Appendix. This guidance is intended as a reference only, and it may need to be tailored to meet the needs of individual service providers. A Project Management file of the model Gantt chart can be downloaded from www.icao.int/fsix or www.icao.int/anb/safetymanagement.*

*Note 2. – Within the context of this Appendix the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.*

## 2. PHASE 1 – PLANNING SMS IMPLEMENTATION

2.1 Identify the Accountable Executive and the person or planning group to develop the SMS implementation plan (discussed in Chapter 8 of this Manual).

2.2 Perform the system description and gap analysis (discussed in Chapter 7 of this Manual)

### System description

The system description is the first prerequisite activity for the development of an SMS in an organization. It should include the interfaces both within the system, as well as with other systems in the air transportation system.

Guidance on a system description is also included as in Appendix 1 to Chapter 7 of this Manual.

### Gap analysis

Perform a gap analysis to identify the safety arrangements existing within the organization and those missing, against the four components and twelve elements of the ICAO SMS framework.

Guidance on the development of an SMS gap analysis is contained in Appendix 2 to Chapter 7 of this Manual.

Based upon the results of the gap analysis, the person or planning group should be able to develop the SMS implementation plan taking into consideration:

- The identification of potential gaps that may hinder SMS implementation; and
- The development of strategies to address such gaps.

2.3 Safety policy and objectives *(discussed in Chapter 8 of this Manual)*

**Safety policy**

- Develop a safety policy.
- The Accountable Executive signs the safety policy.
- The safety policy is communicated with visible endorsement, throughout the organization.
- Establish a review schedule for the safety policy, to ensure it remains relevant and appropriate to the organization.
- An example of a safety policy statement is found in Chapter 8 of this Manual.

**Safety objectives**

Establish safety objectives for the SMS, by developing safety performance standards in terms of:

- Safety performance indicators;
- Safety performance targets; and
- Safety requirements.

Establish the SMS requirements for sub-contractors:

- Establish a procedure to write SMS requirements into the contracting process; and
- Establish the SMS requirements in the bidding documentation.

2.4 Safety accountabilities and appointment of key safety personnel *(discussed in Chapter 8 of this Manual)*

**SMS organizational structure**

Establish the safety service office.

- Appoint a safety manager as the responsible individual and focal point for the development and maintenance of an effective SMS.
- Assess and establish lines of communication between the safety service office and the Accountable Executive, the Safety Action Group (SAG) and the Safety Review Board (SRB).
- The assessment of functional lines of communication should commensurate with the size of the organization and complexity of the services provided.
- Establish the Safety Review Board (SRB) chaired by the Accountable Executive.
- Appoint senior managers, including line managers responsible for functional areas to the SRB.
- Assign the SRB appropriate strategic functions.
- Establish the Safety Action Group(s) (SAG).
- Appoint line managers and representatives of front-line personnel to the SAG.
- Assign the SRB appropriate tactical functions.
- Document all safety responsibilities, accountabilities and authorities and communicate those throughout the organization, including a definition of the levels of management with authority to make decisions regarding safety risks tolerability.
- Develop a schedule of meetings among the safety service office with the SRB and SAG as needed.

2.5 Coordination of emergency response planning (ERP) (discussed in Chapter 8 of this Manual)

**Internal coordination**

- Review the outline of the ERP related to the delegation of authority and assignment of emergency responsibilities; and
- Establish coordination procedures for key personnel for actions during the emergency and the return to normal operations;

**External coordination:**

- Identify external entities that will interact with the organization during emergency situations;
- Assess their respective ERPs;
- Establish coordination between the different ERPs; and
- Incorporate the coordination among different ERPs in the organization's Safety Management Systems Manual (SMSM).

2.6 SMS documentation *(discussed in Chapter 8 of this Manual)*

**SMS documentation**

- Establish the mechanism to collect and store the SMS-specific records and documentation.
- Refer to all relevant and applicable national regulations and international standards.
- Develop guidelines for record management that includes:

**SMS implementation plan**

- Appoint the person or establish the planning group responsible for the development of the SMS implementation plan.
- Collect all applicable documents that form the SMS implementation plan.
- Conduct regular meetings with senior management to assess progress.
- Allocate resources (including time for meetings) commensurate with tasks.
- Include significant items of the SMS implementation plan in the business plan of the organization.
- Identify the costs associated for training and planning of the implementation.
- Establish allocation of time for the development and deployment of SMS implementation plan among the different management layers of the organization.
- Draft budget for SMS implementation.
- Approve initial budget for SMS implementation.
- Submit the SMS implementation plan for endorsement by senior management.

**Safety Management Systems Manual (SMSM)**

- Draft the SMSM to communicate the organization's approach to safety to the whole organization.
- SMSM is a living document and its contents may be expanded, reviewed and amended as the phased approach of the SMS evolves.

2.7 Safety promotion – Training *(discussed in Chapter 9 of this Manual)*

**Safety training**

Develop

- A documented process to identify training requirements.
- A validation process that measures the effectiveness of training.

Develop safety training considering

- Initial (general safety) job-specific training.
- Indoctrination/initial training incorporating SMS, including Human Factors and organizational factors.
- Recurrent training.

Identify the costs associated for training.

Organize and set up schedules for appropriate training to all staff according to the individual responsibilities and involvement in the SMS.

Training files to be developed for each employee, including management.

2.8 Safety promotion – Safety communication *(discussed in Chapter 9 of this Manual)*

Establish means to convey organizational information for Phase 1, including:

- Safety newsletters, notices and bulletins.
- Websites.
- E-mail.

2.9 Time frame for implementation and deliverables

The estimated time frame for implementation of Phase 1 could take from 1 to 6 months, depending on the size of the organization and complexity of the services provided.

### Deliverables

1) Safety policy signed by the Accountable Executive.
2) Safety policy communicated to all staff.
3) System description completed.
4) Gap analysis completed.
5) SMS organizational structure in place.
6) SMS implementation plan approved.
7) Training on SMS planning phase delivered.
8) Initial draft of SMSM published.
9) Means to communicate safety issues established.

## 3 PHASE 2 – REACTIVE SAFETY MANAGEMENT PROCESSES

3.1 Hazard identification and analysis based on reactive processes *(discussed in Chapters 3, 4 and 9 of this Manual)*

### Hazard identification

Identify the internal and external sources to be used in collecting reactive information on hazards.

Implement a structured approach to the reactive identification of hazards.

3.2 Safety risk management based on reactive processes *(discussed in Chapters 5 and 9 of this Manual)*

### Risk assessment

Develop/adopt a risk matrix relevant to own operational environment.

Develop risk matrix instructions and include them to the training programme.

3.3 Training *(discussed in Chapter 9 of this Manual)*

Develop a safety training programme for front line personnel, managers and supervisors on:

- The relevant SMS implementation plan components.
- Hazard identification and risk management on reactive processes.
  - ✓ Front line personnel is trained on identification and reporting hazards from triggering events; and
  - ✓ Supervisors are trained on hazard and risk management
- The safety reporting form/template.

3.4 Documentation on reactive processes (discussed in Chapters 4 and 9 of this Manual)

**Establish a safety library.**

Information on reactive safety risk management processes added to SMSM.

Information on reactive process to be used at a later phase to establish safety performance indicators and targets.

Write requirements on hazard identification and risk management on reactive processes into the bid documentation for contractors, if necessary and notify contractors and sub-contractors in writing.

3.5 Safety promotion – Safety communication (discussed in Chapter 9 of this Manual)

Establish means to convey organizational information for Phase 2:

- Safety newsletters, notices and bulletins.
- Websites.
- E-mail.

3.6 Time frame for implementation and deliverables

The estimated time frame for implementation of Phase 2 could take from 9 to 12 months, depending on the size of the organization and complexity of the services provided.

**Deliverables**

1) Safety library established.
2) Reactive safety management processes implemented.
3) Training relevant to SMS implementation plan components and safety risk management on reactive processes completed.
4) Safety critical information to the organization related to reactive processes distributed.

## 4. PHASE 3 – PROACTIVE AND PREDICTIVE SAFETY MANAGEMENT PROCESSES

4.1 Hazard identification and analysis based on proactive and predictive processes *(discussed in Chapters 3, 4 and 9 of this Manual)*

**Hazard identification**

Identify the internal and external sources to be used in collecting proactive and predictive information on hazards.

Implement a structured approach to the proactive and predictive identification of hazards.

4.2 Safety risk management based on proactive and predictive processes *(discussed in Chapters 5 and 9 of this Manual) (As per 3.2)*

4.3 Training *(discussed in Chapter 9 of this Manual)*

Safety service office staff trained on specific proactive and predictive means to collect safety-related data.

Brief supervisors and frontline personnel on proactive and predictive processes.

Develop a safety training programme for front line personnel, managers and supervisors on:

- The relevant SMS implementation plan components.
- Hazard identification and risk management on proactive and predictive processes.
  - ✓ Front line personnel are trained on identification and reporting hazards from less serious triggering events or during real-time normal operations.
  - ✓ Supervisors are trained on hazard and risk management of proactive and predictive processes.

4.4 Documentation on proactive and predictive processes *(discussed in Chapters 4 and 9 of this Manual)*

Information from the safety risk management based on proactive and predictive processes stored in the safety library.

Information on proactive and predictive safety risk management processes added to SMSM.

Develop safety performance indicators and safety performance targets.

Write requirements on hazard identification and risk management on proactive and predictive processes into the bid documentation for contractors, if necessary and notify contractors and sub-contractors in writing.

4.5 Safety promotion - Safety communication *(discussed in Chapter 9 of this Manual)*

Establish means to convey organizational information for Phase 3:

- Safety newsletters, notices and bulletins.
- Websites.
- E-mail.

4.6 Time frame for implementation and deliverables

The estimated time frame for implementation of Phase 3 could take from 12 to 16 months, depending on the size of the organization and complexity of the services provided.

**Deliverables**

1) Initial testing period for proactive and predictive means to collect hazard identification established.
2) Proactive and predictive safety management processes implemented.
3) Training relevant to SMS implementation plan components and safety risk management on proactive and predictive processes completed.
4) Safety performance indicators and safety performance targets developed.
5) Critical safety information based on safety data captured by reactive, proactive and predictive processes distributed to the organization.

## 5. PHASE 4 – OPERATIONAL SAFETY ASSURANCE

5.1 Safety performance or the SMS *(discussed in Chapter 9 of this Manual)*

Establish safety performance indicators.

Establish safety performance targets.

Establish safety requirements.

Define measures of reliability, availability and/or accuracy related to safety requirements.

Agree on safety performance measurement with the State oversight authority.

5.2 Safety performance monitoring and measurement *(discussed in Chapter 9 of this Manual)*

Define and develop sources of information for safety performance and monitoring to the organization SMS.

5.3 The management of change *(discussed in Chapter 9 of this Manual)*

Establish a formal process for the management of change that considers:

- Criticality of systems and activities.
- Stability of systems and operational environments.
- Past performance.
- Identify changes that might affect established processes, procedures, products and services.
- Prior to implement changes; define arrangements to ensure safety performance.

5.4 SMS continuous improvement *(discussed in Chapter 9 of this Manual)*

- Develop forms for internal evaluations and ensure independence from technical process being evaluated.
- Define an internal audit process.
- Define an external audit process.
- Define a schedule proactive evaluation of facilities, equipment, documentation and procedures, to be completed through audits and surveys.
- Define a schedule proactive evaluation of the individuals' performance.
- Develop documentation relevant to operational safety assurance.

5.5 Training *(discussed in Chapter 9 of this Manual)*

Develop training relevant to operational safety assurance to staff involved in the safety assurance phase.

5.6 Safety promotion - safety communication (discussed in Chapter 9 of this Manual)

Establish means to convey organizational information for Phase 4:

- Safety newsletters, notices and bulletins.
- Websites.
- E-mail.

5.7 Time frame for implementation and deliverables

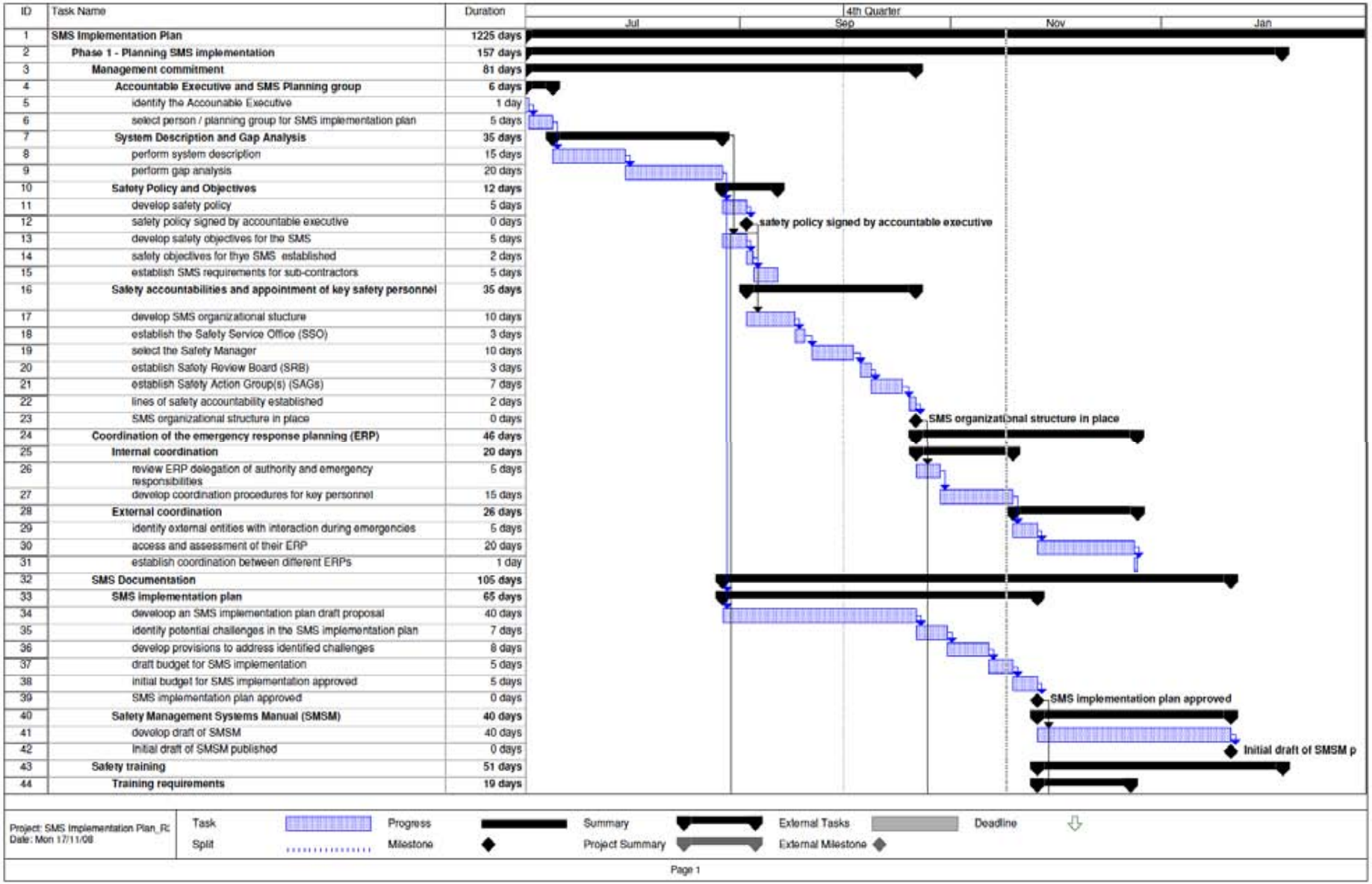
The estimated time frame for implementation of Phase 4 could take from 9 to 12 months, depending on the size of the organization and complexity of the services provided.

**Deliverables**

1) Agreement with the State oversight authority on safety performance indicators and safety performance targets.
2) Training on safety assurance for operational personnel, managers and supervisors completed.
3) Documentation relevant to operational safety assurance place in safety library.

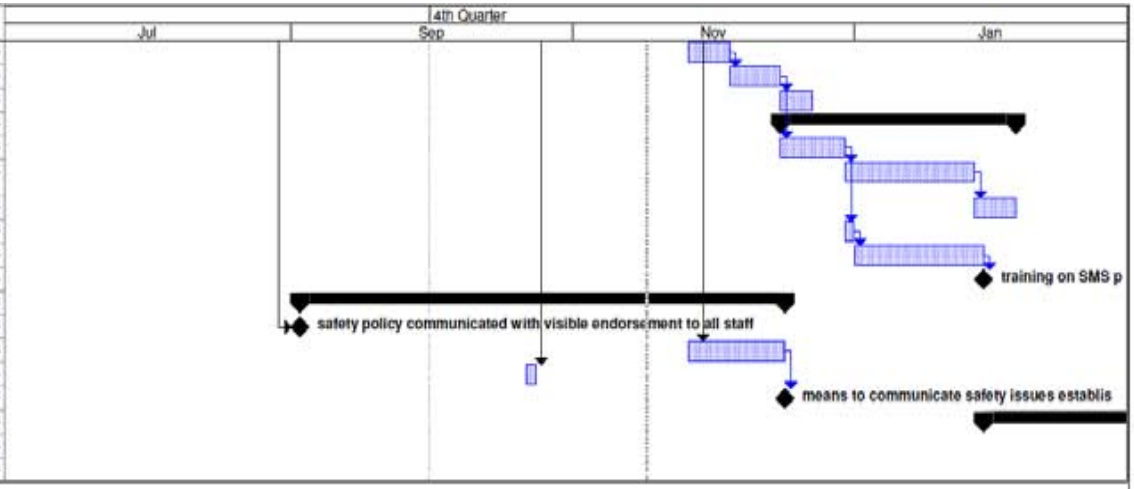
- - - - - - - - - - - - - - -

Gantt chart – SMS implementation plan




| ID | Task Name | Duration |
|---|---|---|
| 1 | **SMS Implementation Plan** | **1225 days** |
| 2 | **Phase 1 - Planning SMS implementation** | **157 days** |
| 3 | **Management commitment** | **81 days** |
| 4 | **Accountable Executive and SMS Planning group** | **6 days** |
| 5 | identify the Accountable Executive | 1 day |
| 6 | select person / planning group for SMS implementation plan | 5 days |
| 7 | **System Description and Gap Analysis** | **35 days** |
| 8 | perform system description | 15 days |
| 9 | perform gap analysis | 20 days |
| 10 | **Safety Policy and Objectives** | **12 days** |
| 11 | develop safety policy | 5 days |
| 12 | safety policy signed by accountable executive | 0 days |
| 13 | develop safety objectives for the SMS | 5 days |
| 14 | safety objectives for thye SMS established | 2 days |
| 15 | establish SMS requirements for sub-contractors | 5 days |
| 16 | **Safety accountabilities and appointment of key safety personnel** | **35 days** |
| 17 | develop SMS organizational stucture | 10 days |
| 18 | establish the Safety Service Office (SSO) | 3 days |
| 19 | select the Safety Manager | 10 days |
| 20 | establish Safety Review Board (SRB) | 3 days |
| 21 | establish Safety Action Group(s) (SAGs) | 7 days |
| 22 | lines of safety accountability established | 2 days |
| 23 | SMS organizational structure in place | 0 days |
| 24 | **Coordination of the emergency response planning (ERP)** | **46 days** |
| 25 | **Internal coordination** | **20 days** |
| 26 | review ERP delegation of authority and emergency responsibilities | 5 days |
| 27 | develop coordination procedures for key personnel | 15 days |
| 28 | **External coordination** | **26 days** |
| 29 | identify external entities with interaction during emergencies | 5 days |
| 30 | access and assessment of their ERP | 20 days |
| 31 | establish coordination between different ERPs | 1 day |
| 32 | **SMS Documentation** | **105 days** |
| 33 | **SMS implementation plan** | **65 days** |
| 34 | develoop an SMS implementation plan draft proposal | 40 days |
| 35 | identify potential challenges in the SMS implementation plan | 7 days |
| 36 | develop provisions to address identified challenges | 8 days |
| 37 | draft budget for SMS implementation | 5 days |
| 38 | initial budget for SMS implementation approved | 5 days |
| 39 | SMS implementation plan approved | 0 days |
| 40 | **Safety Management Systems Manual (SMSM)** | **40 days** |
| 41 | dovelop draft of SMSM | 40 days |
| 42 | Initial draft of SMSM published | 0 days |
| 43 | **Safety training** | **51 days** |
| 44 | **Training requirements** | **19 days** |

| ID | Task Name | Duration |
|---|---|---|
| 45 | develop a documented process to identify training requirements | 7 days |
| 46 | develop a validation process to measure effectiveness of training | 7 days |
| 47 | identify costs associated for training | 5 days |
| 48 | **Training programme** | **37 days** |
| 49 | develop initial (general safety) job-specific | 10 days |
| 50 | indoctrination/initial on SMS, human factors and organizational factors | 20 days |
| 51 | develop recurrent training syllabus | 7 days |
| 52 | schedule initial (general safety) training job-wise for all staff | 2 days |
| 53 | deliver initial (general safety) training | 20 days |
| 54 | training on SMS planning phase delivered | 0 days |
| 55 | **Safety Promotion-Communication** | **75 days** |
| 56 | safety policy communicated with visible endorsement to all staff | 0 days |
| 57 | identify and develop means to convey safety related issues | 15 days |
| 58 | convey to all staff information related to SMS organizational structure | 2 days |
| 59 | means to communicate safety issues established | 0 days |
| 60 | **Phase 2- Reactive safety management processes** | **287 days** |
| 86 | **Phase 3- Proactive and predictive safety mangement processes** | **445 days** |
| 109 | **Phase 4- Operational safety assurance** | **341 days** |



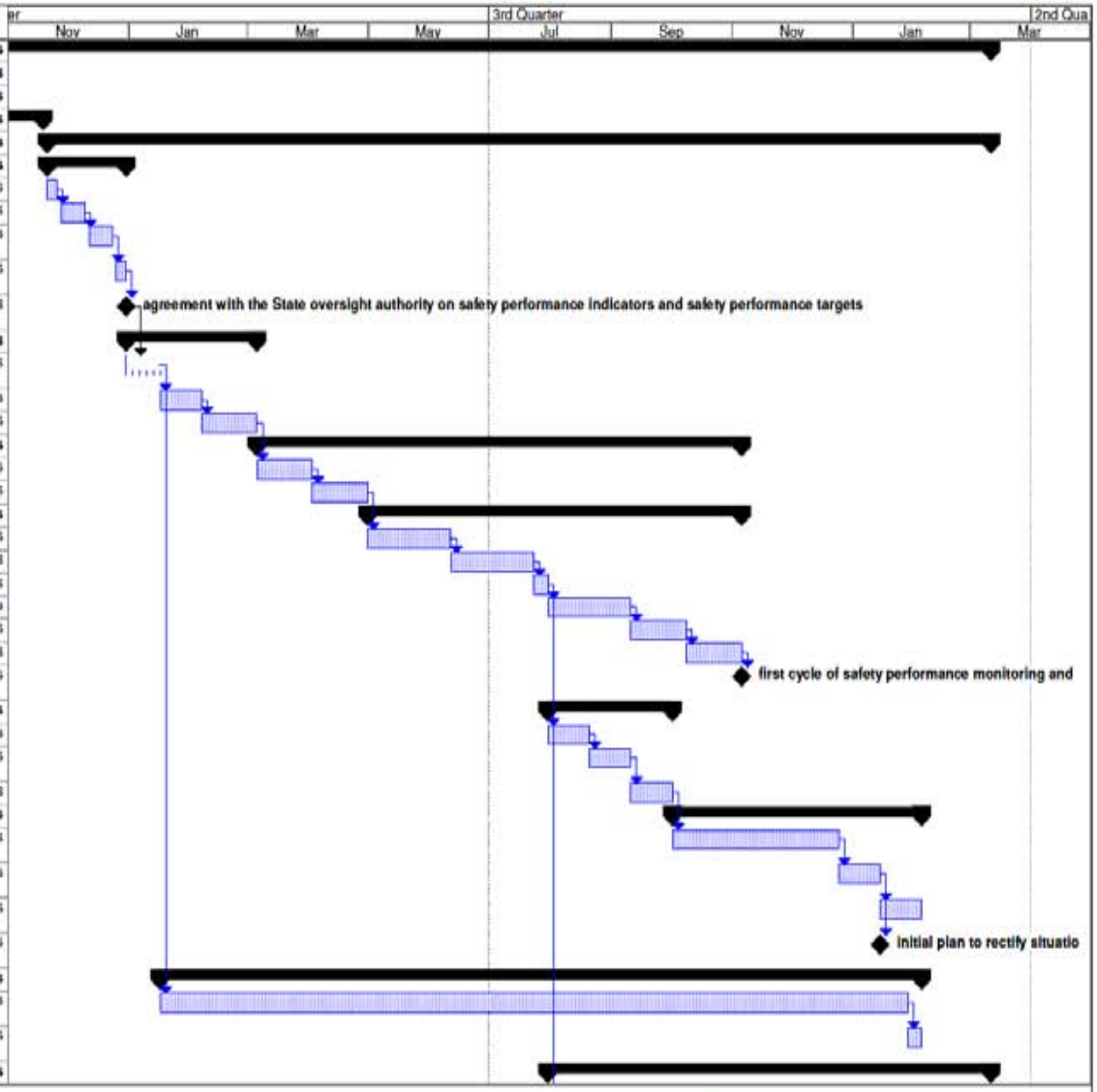

Project: SMS Implementation Plan_R
Date: Mon 17/11/08

Task | Progress | Summary | External Tasks | Deadline
Split | Milestone | Project Summary | External Milestone


ID
Task Name
Duration
3rd Quarter
2nd Qua
Nov
Jan
Mar
May
Jul
Sep
Nov
Jan
Mar
1 SMS Implementation Plan 1225 days
2 Phase 1 - Planning SMS Implementation 157 days
60 Phase 2- Reactive safety management processes 207 days
61 Develop reactive safety management processes 50 days
62 Hazard identification 30 days
63 identify int/ext sources to collect reactive info on hazards 10 days
64 develop a structured approach to reactive identification of hazards 20 days
65 Safety risk management 20 days
66 develop/adopt risk matrix 15 days
67 develop risk matrix instructions 5 days
68 training 52 days
69 develop training on SMS/safety risk management on reactive processes 20 days
70 schedule Develop training on SMS/safety risk management on reactive processes 2 days
71 deliver training on SMS/safety risk management on reactive processes 30 days
72 training on SMS/safety risk management on reactive processes delivered 0 days
73 test reactive safety management processes 180 days
74 test period 180 days
75 reactive safety management processes implemented 0 days
76 SMS documentation on reactive processes 184 days
77 develop the safety library 20 days
78 safety library established 0 days
79 Information from the development of safety mangement process and test period store in safety library 160 days
80 Information on reactive safety risk management process added to SMSM 3 days
81 Information on reactive processes store for later use on the safety performance indicators and targets 1 day
82 develop requirements on hazard identification and risk management on reactive processes for sub-contractors 3 days
83 Safety Promotion-Communication 165 days
84 establish means to convey organizational information for Phase 2 15 days
85 safety critical information to the organization related to reactive process distributed 150 days
86 Phase 3- Proactive and predictive safety mangement processes 445 days
109 Phase 4- Operational safety assurance 341 days
training on SMS/safety risk management on reactive processes delivered
reactive safety
safety library established
Project: SMS Implementation Plan_R
Date: Mon 17/11/08
Task
Split
Progress
Milestone
Summary
Project Summary
External Tasks
External Milestone
Deadline
Page 1


| ID | Task Name | Duration |
|---|---|---|
| 1 | **SMS Implementation Plan** | **1225 days** |
| 2 | **Phase 1 - Planning SMS implementation** | **157 days** |
| 60 | **Phase 2- Reactive safety management processes** | **287 days** |
| 86 | **Phase 3- Proactive and predictive safety mangement processes** | **445 days** |
| 87 | **Develop proactive/predictive safety management processes** | **40 days** |
| 88 | **hazard identification** | **40 days** |
| 89 | identify int/ext sources to collect proactive and predictive information on hazards | 15 days |
| 90 | develop a structured approach to proactive and predictive identification of hazards | 20 days |
| 91 | **Safety risk management** | **5 days** |
| 92 | review risk matrix for proactive and predictive safety management processes | 5 days |
| 93 | **Training** | **70 days** |
| 94 | develop training programme for specific proactive and predictive processes | 30 days |
| 95 | training on proactive and predictive proceses developed | 40 days |
| 96 | training on SMS/safety risk management on proactive and predictive processes delivered | 0 days |
| 97 | **test proactive/predictive safety management processes** | **300 days** |
| 98 | **hazard identification and risk analysis** | **300 days** |
| 99 | test period | 300 days |
| 100 | proactive / predictive safety management processes implemented | 0 days |
| 101 | **SMS documentation on proactive / predictive processes** | **335 days** |
| 102 | Information from the safety risk management based on proactive and predictive processes stored in the safety library | 300 days |
| 103 | add proactive / predictive risk management processes information to SMSM | 5 days |
| 104 | development of safety performance indicators and targets | 30 days |
| 105 | safety performance indicators and safety performance targets established | 0 days |
| 106 | **Safety promotion-safety communication** | **265 days** |
| 107 | establish means to convey organizational information for Phase 3 | 5 days |
| 108 | safety critical information to the organization related to proactive and predictive process distributed | 260 days |
| 109 | **Phase 4- Operational safety assurance** | **341 days** |

| ID | Task Name | Duration |
|---|---|---|
| 1 | **SMS Implementation Plan** | **1225 days** |
| 2 | **Phase 1 - Planning SMS implementation** | **157 days** |
| 60 | **Phase 2- Reactive safety management processes** | **287 days** |
| 86 | **Phase 3- Proactive and predictive safety mangement processes** | **445 days** |
| 109 | **Phase 4- Operational safety assurance** | **341 days** |
| 110 | **Safety performance of the SMS** | **30 days** |
| 111 | establish safety performance indicators and targets | 5 days |
| 112 | establish safety requirements | 10 days |
| 113 | define measures of reliability,availability / accuracy related to safety requirements | 10 days |
| 114 | meetings with State oversight authority to agree on safety performance measurement | 5 days |
| 115 | agreement with the State oversight authority on safety performance indicators and safety performance targets | 0 days |
| 116 | **Safety performance monitoring and measurement** | **46 days** |
| 117 | define sources of information for safety performance and monitoring | 10 days |
| 118 | collect information from safety studies and reviews | 15 days |
| 119 | develop protocols for safety audits | 20 days |
| 120 | **Training** | **175 days** |
| 121 | develop training programme for operational safety assurance | 20 days |
| 122 | training relevant to operational safety assurance completed | 20 days |
| 123 | **Test tools to measure safety performance** | **135 days** |
| 124 | conduct first cycle of safety audits | 30 days |
| 125 | information of first cycle of audits reviewed | 30 days |
| 126 | information distilled from the audits distributed | 5 days |
| 127 | checklists and questionaries for safety surveys | 30 days |
| 128 | safety surveys completed | 20 days |
| 129 | internal safety investigations procedures developed | 20 days |
| 130 | first cycle of safety performance monitoring and measurement completed | 0 days |
| 131 | **Management of change** | **45 days** |
| 132 | Establish a formal process for the management of change | 15 days |
| 133 | identify changes within the organization which may affect established processes and services | 15 days |
| 134 | description of arrangements to ensure safety performance | 15 days |
| 135 | **SMS continuous improvement** | **90 days** |
| 136 | first cycle of proactive evaluation of facilities, equipment, documentation and individual performance completed | 60 days |
| 137 | first cycle of identification of immediate causes of below standard performance identified and their implications in the operation | 15 days |
| 138 | initial plan to rectify situations involving below standard performance developed | 15 days |
| 139 | initial plan to rectify situations involving below standard performance approved | 0 days |
| 140 | **SMS documentation on operational safety assurance** | **275 days** |
| 141 | documentation relevant to operational safety assurance added to safety library | 270 days |
| 142 | documentation relevant to operational safety assurance added to the SMSM | 5 days |
| 143 | **Safety promotion-safety communication** | **160 days** |




Project: SMS Implementation Plan_R;
Date: Mon 17/11/08

Task | Progress | Summary | External Tasks | Deadline
Split | Milestone | Project Summary | External Milestone


ID
Task Name
Duration
er
Nov
Jan
Mar
May
3rd Quarter
Jul
Sep
Nov
Jan
2nd Qua
Mar
144
establish means to convey organizational information for Phase 4
10 days
145
safety critical information to the organization related to operational safety assurance distributed
150 days
Project: SMS Implementation Plan_R
Date: Mon 17/11/08
Task
Split
Progress
Milestone
Summary
Project Summary
External Tasks
External Milestone
Deadline
Page 2

*Page left blank intentionally*

# Chapter 11

# STATE SAFETY PROGRAMME (SSP)

## 11.1 OBJECTIVES AND CONTENTS

11.1.1 This chapter introduces a framework for development and implementation of a State safety programme (SSP) which combines elements of both prescriptive and performance-based approaches to the management of safety. The chapter also discussed the importance of a realistic implementation of an SSP as prerequisite for the implementation of an SMS by service providers. The chapter includes the following:

- The components and elements of an SSP
- The ICAO SSP framework
- SSP – Development
- SSP – Implementation
- SSP – The role of the SSP in SMS implementation

## 11.2 THE COMPONENTS AND ELEMENTS OF AN SSP

11.2.1 An SSP is a management system for the management of safety by the State. The implementation of an SSP must be commensurate with the size and complexity of the State's aviation system, and may require coordination among multiple authorities responsible for individual element functions of civil aviation in the State.

11.2.2 There are four components in an SSP, that represent the two core operational activities an SSP must undertake, as well as the organizational arrangements that are necessary to support such core operational activities. The four components of an SSP are:

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

11.2.3 From a point of view of safety performance, the two core operational activities of an SSP are the *State safety risk management* and *State safety assurance.* These two core operational activities take place under the umbrella provided by the *State safety policy and objectives* and are supported by the *State safety*

*promotion*. The discussion on the subject presented in Chapter 8, paragraphs 8.2 and 8.3 regarding the equivalent components of an SMS are mostly applicable for the SSP. There is, however, one difference: under the SSP, the accident and serious incident investigation process, although formally considered as an element of the State policy and objectives, is also a core operational activity that contributes to safety data collection analysis and exchange, as well as to the targeting of oversight on areas of greater concern (State safety assurance).

11.2.4 The four components discussed in paragraph 11.2.2 constitute the basic building blocks of an SSP, in that they represent the four overarching safety management processes that underlie the actual management system (SSP). Each component is subdivided into elements, which encompass the specific sub-processes, specific activities or specific tools that the actual State management system must engage or utilise in order to conduct the management of safety in a manner that combines prescription and performance based approaches and supports the implementation of SMS by service providers.

11.2.5 The component ***State safety policy and objectives*** is composed of four elements:

- State safety legislative framework
- State safety responsibilities and accountabilities
- Accident and incident investigation
- Enforcement policy

11.2.6 The component ***State safety risk management*** is composed of two elements:

- Safety requirements for service providers SMS
- Agreement on service providers safety performance

11.2.7 The component ***State safety assurance*** is composed of three elements:

- Safety oversight
- Safety data collection, analysis and exchange
- Safety data driven targeting of oversight on areas of greater concern or need

11.2.8 The component ***State safety promotion*** is composed of two elements:

- Internal training, communication and dissemination of safety information
- External training, communication and dissemination of safety information

*Note.— Within the context of the SSP, the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.*

## 11.3 THE ICAO SSP FRAMEWORK

***Note***. *– Detailed information on the ICAO SSP framework is contained in Appendix 1 to this Chapter.*

11.3.1 The four components combined with the elements discussed in section 11.2 conform the ICAO SSP framework, which is intended as a principled guide for the development, implementation and maintenance of an SSP, as follows:

**1. State safety policy and objectives**

1.1. State safety legislative framework

1.2 State safety responsibilities and accountabilities

1.3 Accident and incident investigation

1.4 Enforcement policy

**2. State safety risk management**

2.1 Safety requirements for service providers SMS

2.2 Agreement on service providers safety performance

**3. State safety assurance**

3.1 Safety oversight

3.2 Safety data collection, analysis and exchange

3.3 Safety data driven targeting of oversight on areas of greater concern or need

**4. State safety promotion**

4.1 Internal training, communication and dissemination of safety information

4.2 External training, communication and dissemination of safety information

11.3.2 The SSP framework introduced in this Chapter, and the safety management system (SMS) framework specified in Chapter 8 must be viewed as complementary, yet distinct frameworks.

## 11.4 SSP DEVELOPMENT

11.4.1 It is proposed that States develop their SSP around the four components and eleven elements of the ICAO SSP framework.

11.4.2 **State safety policy and objectives** – A description of how the State will oversee the management of safety in the aviation activities of the State. This includes a definition of the different State organizations requirements, responsibilities and accountabilities regarding the SSP, as well as of the Acceptable Level of Safety (ALoS) to be achieved by the SSP.

11.4.3 The three SSP components discussed in the following paragraphs can only be effectively implemented as part of an overall framework of accountabilities, responsibilities and liabilities. This overall framework becomes a "protective umbrella", under which safety risk management, safety assurance and safety promotion by the State take place. The component Safety policy and objectives provides management and personnel explicit policies, procedures, management controls, documentation, and corrective action processes that keep the State civil aviation authorities safety management efforts on track. This component is also essential in generating confidence in the State's ability to provide safety leadership to an increasingly complex and constantly changing air transportation system. A central activity under this component is the development of a State safety policy. Appendix 2 to this chapter includes guidance on the development of a State's safety policy statement.

11.4.4 **State safety risk management** – A description oh how the State will identify hazards and assess the safety risks of the consequences of hazards in the State's aviation operations. This includes the establishment of controls (rules and/or regulations) which govern how the State will manage safety, the rules and/or regulations which govern how the service providers' SMS operate, as well as the agreement of the safety performance of the service providers SMS.

11.4.5 Safety management principles affect most activities of a State civil aviation authorities, starting with rulemaking and policy development. Rather than only pursuing the causes of the most recent accident, the SSP rulemaking is based on comprehensive analyses of the State's aviation system. Regulations are based on identified hazards and analysis of the safety risks of the consequences of hazards. The regulations themselves provide frameworks for risk control, when integrated into service providers SMS.

11.4.6 **State safety assurance** – A description of how the State will ensure that safety management within the State and the operation of the service providers' SMS follow established controls (regulatory compliance), how the actual performance of the SSP (ALoS) will be demonstrated, though a combination of safety measurement and safety performance measurement, and how the actual performance of service providers SMS (safety performance) will be demonstrated (safety performance measurement). This includes the establishment of the necessary arrangements (oversight, inspections, audits, safety data analysis and so forth) necessary to verify compliance and measure performance.

11.4.7 SSP oversight activities beyond rulemaking are supported by analysis, with States aviation authorities' resource allocation priorities being based on the safety risks of the consequences of the hazards identified through analysis. Certification and continuing operational safety decisions are based on assessments of performance of service providers' processes, products and/or services. Flowing forward from the regulations that address defined hazards, compliance decisions are based on whether a service provider's SMS addresses the hazard addressed through in regulations within the service provider specific operational environment. The State safety assurance processes are used to obtain confidence in service providers' safety management capability as demonstrated in assessments of their SMS.

11.4.8 **State's safety promotion** – A description of the arrangements by the State to ensure that safety training, communication and dissemination of safety information takes place. Under an SSP, this is a dual-track promotion; both within the State aviation organizations as well as among the service providers it oversees. This includes the establishment of the necessary means to provide training and communicate safety information.

11.4.9 None of the above changes the role of the State and its aviation organizations regarding the establishment of State's regulations and standards, or the requirement for State civil aviation personnel to possess high levels of knowledge and skills. Quite the contrary, it requires additional skills in areas such as safety risk analysis, system evaluation, and management system assessment, as well as in the many new technologies essential for the aviation industry to achieve its production objectives. This makes it incumbent on the State to provide for these competencies through training, recruitment, and human resource management.

11.4.10 In developing the SSP, safety management principles provide a conceptual platform for parallel development between the SSP by the State and the SMS by service providers. An SSP developed from, and based upon safety management principles becomes the bridge that closes a gap that would otherwise inevitably develop between the internal and external safety processes within the State civil aviation organizations and the internal safety processes of service providers. As part of the SSP, the State promulgates SMS requirements for service providers requiring providers to demonstrate their safety management capability up front, rather than waiting for accidents, incidents, or non-compliance with safety standards. This allows both the State and service providers to get ahead of safety risks. SMS requirements under the SSP also provide a structured framework allowing the State and service providers to interact more effectively in the resolution of safety concerns. In this way the shared, interactive nature of the SSP and the SMS comes to fruition.


Figure 11-1 – A bridge

## 11.5 SSP IMPLEMENTATION

11.5.1 SSP implementation is facilitated by identifying the processes involved in each of the four components of an SSP discussed in the previous paragraphs. These processes can then be turned into discrete elements of each component of an SSP and, similar to the SMS framework discussed in Chapter 8, the combination of elements and components becomes the framework for an SSP. The availability of such a framework provides a principled guide for SSP implementation. ICAO has developed guidance for the development of an SSP framework in order to facilitate SSP implementation, and the ICAO SSP framework is included in Appendix 2 to this chapter. Appendix 5 to this chapter presents guidance on an SSP implementation plan.

11.5.2 An example of an SSP by one State, the State safety programme for the United Kingdom, published through the UK Civil Aviation Publication (CAP) 784, can be accessed through the UKCAA website: www.caa.co.uk.

## 11.6 THE ROLE OF THE SSP IN SUPPORTING SMS IMPLEMENTATION

11.6.1 One of the objectives of an SSP is to generate a context that supports the implementation of SMS by service providers. The service providers' SMS cannot effectively perform either in a regulatory vacuum, or in an exclusively compliance-oriented environment. In such environments, service providers will only implement and demonstrate, and the State authorities will only assess, the tokens of an SMS. In such environments, service providers will not be able to implement, or the State authorities will be not able to assess, effectively performing SMS. Effectively performing SMS by service providers can only flourish under the enabling umbrella provided by an SSP. The SSP is therefore a fundamental enabler for the implementation of effective SMS by service providers. For this reason, within the scope of the overall implementation of an SSP presented by Appendix 5, four steps – two globally and two specifically – aim at supporting SMS implementation by service providers.

11.6.2 The first step – overall – to be taken by the State in implementing its SSP is to conduct a gap analysis of the SSP, in order to ascertain the status of maturity and existence within the State of the elements of an SSP. An example of a gap analysis for an SSP is included in Appendix 3 to this Chapter. Following the gap analysis, the State is in a position to draft the national legislation and operating regulations governing the functioning of the SSP. Included among these will be the SMS requirements for service providers.

11.6.3 An early step in implementing an SSP is to develop a training programme for the State authorities personnel. The training programme should aim at two basic objectives. The first objective is to provide knowledge of safety management concepts and ICAO SARPs on safety management in Annexes 1, 6, 8, 11, 13 and 14, and related guidance material. This aspect of the training applies to the SSP, overall. The second objective is to develop knowledge to accept and oversee the implementation of key components of an SMS, in compliance with the national regulations and relevant ICAO SARPs. This aspect of the training aims at supporting SMS implementation.

11.6.4 The first step in implementing an SSP specifically aimed at supporting SMS implementation is the development of SMS requirements for service providers, as well as of guidance material for the implementation of SMS. Guidance on the development of a State's regulation on SMS is included in Attachment 1 to Chapter 10. Such guidance uses as reference the components and elements of the ICAO SMS framework, discussed in Chapter 8. This Manual and the ICAO SMS training and SSP training courses are sources of information for the development of guidance material.

11.6.5 The second step in implementing an SSP specifically aimed at supporting SMS implementation is the revision of the civil aviation oversight authority's enforcement policy. This step deserves a special mention.

11.6.6 The essence of both the SSP and the SMS is to get ahead of safety risks through the development of safety management capabilities within the State as well as the industry, rather than waiting for accidents, incidents or events of non-compliance. One essence of management, as discussed in various parts of this Manual, is

measurement, since it is not possible to manage what cannot be measured. Measurement, in turn, requires data. It follows that safety data collection, analysis and exchange is at the heart of the interactive nature of the SSP and the SMS discussed in paragraph 11.4.10.

11.6.7 During the course of normal safety management activities under the respective SSP and SMS, the State and the service providers will exchange safety data. The service provider's safety data received by the State will be property data, a part of which the State will convert into aggregate data. A significant amount of all these data will reasonably refer to safety concerns identified through the normal course of the service providers SMS processes. If the response to this data by the civil aviation oversight authority is enforcement action, the safety management process in the State will grind to a halt. It is therefore essential that, as part of the SSP, the civil aviation oversight authority revises its enforcement policy to ensure continuing flow and exchange of proactive and predictive safety management data with service providers who operate under an SMS environment. The following guidelines are proposed for such revision:

- service providers should be allowed to deal with certain safety concerns internally, within the context of their SMS;
- service providers should provide the State with a clear definition of the safety concern, including deviations and/or minor violations, and a mitigation plan for its resolution, that satisfies the State;
- the mitigation plan should include time lines, so that the State can monitor satisfactory progress of mitigation activities; and
- gross negligence, reckless conduct and wilful deviations should be dealt through established enforcement procedures.

Appendix 4 to this chapter presents an example of the development of a State's enforcement policy and enforcement procedures in an SMS environment.

11.6.8 A summary the role of the SSP in supporting SMS implementation and proposed actions is shown in Figure 11-2 hereunder.

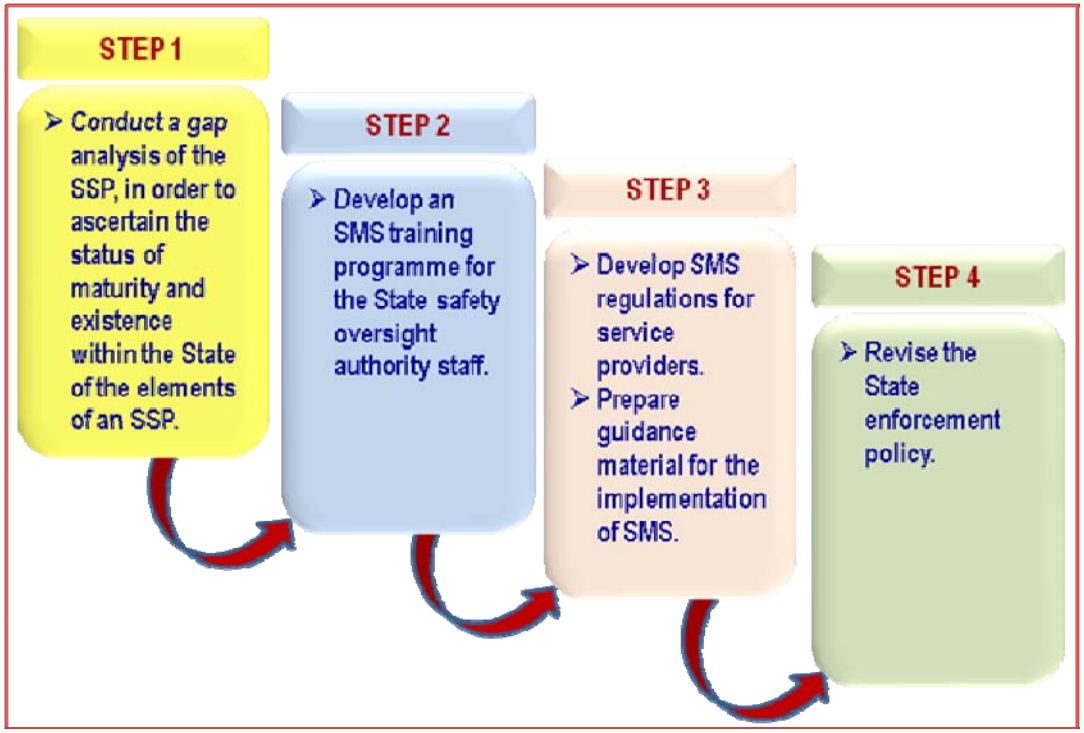



Figure 11-2 – The role of the SSP in supporting SMS implementation – Summary

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 1 to Chapter 11

# FRAMEWORK FOR THE STATE SAFETY PROGRAMME (SSP)

## INTRODUCTION

Appendix 2 to Chapter 11 introduces a framework for the implementation and maintenance of a State safety programme (SSP) by a State. The framework consists of four components and eleven elements, outlined hereunder. A brief description of each element is presented.

1. State safety policy and objectives

    1.1 – State safety legislative framework

    1.2 – State safety responsibilities and accountabilities

    1.3 – Accident and incident investigation

    1.4 – Enforcement policy

2. State's safety risk management

    2.1 – Safety requirements for service providers SMS

    2.2 – Agreement on service providers safety performance

3. State's safety assurance

    3.1 – Safety oversight

    3.2 – Safety data collection, analysis and exchange

    3.3 – Safety data driven targeting of oversight on areas of greater concern or need

4. State's safety promotion

    4.1 – Internal training, communication and dissemination of safety information

    4.2 – External training, communication and dissemination of safety information

***Note**.– Within the context of this attachment the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.*

## 1. STATE SAFETY POLICY AND OBJECTIVES

### 1.1 State safety legislative framework

The State has promulgated a national safety legislative framework and specific regulations in compliance with international and national standards that define how the State will conduct the management of safety in the State. This includes the participation of the State aviation organizations in specific activities related to the management of

safety in the State, and the establishment of the roles, responsibilities, and relationships of such organizations. The safety legislative framework and specific regulations are periodically reviewed to ensure they remain relevant and appropriate to the State.

### 1.2 State safety responsibilities and accountabilities

The State has identified, defined and documented the requirements, responsibilities and accountabilities regarding the establishment and maintenance of the SSP. This includes the directives to plan, organize, develop, maintain, control and continuously improve the SSP in a manner that meets the State's safety objectives. It also includes a clear statement about the provision of the necessary resources for the implementation of the SSP.

### 1.3 Accident and incident investigation

The State has established an independent accident and incident investigation process, the sole objective of which is the prevention of accidents and incidents, and not the apportioning of blame or liability. Such investigations are in support of the management of safety in the State. In the operation of the SSP, the State maintains the independence of the accident and incident investigation organization from other State aviation organizations.

### 1.4 Enforcement policy

The State has promulgated an enforcement policy that establishes the conditions and circumstances under which service providers are allowed to deal with, and resolve, events involving certain safety deviations internally, within the context of the service provider safety management system (SMS), and to the satisfaction of the appropriate State authority. The enforcement policy also establishes the conditions and circumstances under which to deal with safety deviations through established enforcement procedures.

## 2. STATE SAFETY RISK MANAGEMENT

### 2.1 Safety requirements for service providers SMS

The State has established the controls which govern how service providers will identify hazards and manage safety risks. These include the requirements, specific operating regulations and implementation policies for service providers SMS. The requirements specific operating regulations and implementation policies are periodically reviewed to ensure they remain relevant and appropriate to the service providers.

### 2.2 Agreement on service providers safety performance

The State has agreed with individual service providers on the safety performance of their SMS. The agreed safety performance of individual service providers SMS is periodically reviewed to ensure it remains relevant and appropriate to the service providers.

## 3. STATE SAFETY ASSURANCE

### 3.1 Safety oversight

The State has established mechanisms to ensure an effective monitoring of the eight critical elements of the safety oversight function. The State has also established mechanisms to ensure that the identification of hazards and the management of safety risks by service providers follow established regulatory controls (requirements, specific

operating regulations and implementation policies). These mechanisms include inspections, audits and surveys to ensure that regulatory safety risk controls are appropriately integrated into the service providers SMS, that they are being practiced as designed, and that the regulatory controls have the intended effect on safety risks.

### 3.2 Safety data collection, analysis and exchange

The State has established mechanisms to ensure the capture and storage of data on hazards and safety risks at both an individual and aggregate State's level. The State has also established mechanisms to develop information from the stored data, and to actively exchange safety information with service providers and/or other States as appropriate.

### 3.3 Safety data driven targeting of oversight on areas of greater concern or need

The State has established procedures to prioritize inspections, audits and surveys towards those areas of greater safety concern or need, as identified by the analysis of data on hazards, their consequences in operations, and the assessed safety risks.

## 4. STATE SAFETY PROMOTION

### 4.1 Internal training, communication and dissemination of safety information

The State provides training and fosters awareness and two-way communication of safety relevant information to support, within the State aviation organizations, the development of an organizational culture that fosters an effective and efficient SSP.

### 4.2 External training, communication and dissemination of safety information

The State provides education and promotes awareness of safety risks and two-way communication of safety relevant information, to support among services providers the development of an organizational culture that fosters an effective and efficient SMS.

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 2 to Chapter 11

# GUIDANCE ON THE DEVELOPMENT OF A STATE'S SAFETY POLICY STATEMENT

The management of civil aviation safety is one of major responsibilities of [State]. [State] is committed to developing, implementing, maintaining and constantly improving strategies and processes to ensure that all aviation activities that take place under its oversight will achieve the highest level of safety performance, while meeting both national and international standards.

The holders of [State] aviation certificates shall require demonstrating that their management systems adequately reflect an SMS approach. The expected result of this approach is improved safety management, safety practices, including safety reporting within the civil aviation industry.

At the [State], all levels of management are accountable for the delivery of the highest level of safety performance within [State], starting with the Accountable Executive [as appropriate to the organization].

[State's] commitment is to:

a) Develop general rulemaking and specific operational policies that build upon safety management principles, based on a comprehensive analysis of the State's aviation system;

b) Consult with all segments of the aviation industry on issues regarding regulatory development;

c) Support the management of safety in the State through an effective safety reporting and communication system;

d) Interact effectively with service providers in the resolution of safety concerns;

e) Ensure that within the [State safety oversight authority], sufficient resources are allocated, personnel have the proper skills and are trained for discharging their responsibilities, both safety-related and otherwise;

f) Conduct both, performance-based as well as compliance-oriented oversight activities, supported by analyses and prioritized resource allocation based on safety risks;

g) Comply with, and wherever possible, exceed international safety requirements and standards;

h) Promote and educate the aviation industry on safety management concepts and principles;

i) Oversee the implementation of SMS within aviation organizations;

j) Ensure that all activities under oversight achieve the highest safety standards;

k) Establish provisions for the protection of safety data, collection and processing systems (SDCPS), so that people where people are encouraged to provide essential safety-related information on hazards, a continuous flow and exchange of safety management data between [State] and service providers;

l) Establish and measure our safety performance against safety performance indicators and safety performance targets which are clearly identified; and

m) Promulgate an enforcement policy that ensures that no information derived from any SDPCS established under the SSP or SMS will be used as the basis for enforcement action, unless gross negligence or wilful deviation.

This policy must be understood, implemented and observed by all staff involved in activities related to the [State safety oversight authority].

(Signed)

_____

Accountable Executive

- - - - - - - - - - - - - - -

# Appendix 3 to Chapter 11

# GUIDANCE ON THE DEVELOPMENT OF A STATE SAFETY PROGRAMME (SSP) GAP ANALYSIS

## GAP ANALYSIS

The implementation of an SSP requires that the State conduct an analysis of its safety system to determine which components and elements of an SSP are currently in place and which components and elements must be added or modified to meet the implementation requirements. This analysis is known as gap analysis, and it involves comparing the SSP requirements against the existing resources in the State.

This guidance provides, in checklist format, information to assist in the evaluation of the components and elements that comprise the ICAO SSP framework and to identify the components and elements that need to be developed. Once the gap analysis is complete and documented, it forms one basis of the SSP implementation plan.

The gap analysis form included in this guide can be used as a template to conduct a gap analysis. Each question is designed for a "Yes" or "No" response. A "Yes" answer indicates that the State already has component or element of the ICAO SSP framework in question incorporated into its safety system, and that it matches or exceeds the requirement. A "No" answer indicates that a gap exists between the component/element of the ICAO SSP framework and the safety system in the State.

***Note**. – Within the context of this guidance the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to operational safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.*

## ICAO SSP FRAMEWORK

The ICAO SSP framework comprises four components and eleven elements, outlined hereunder:

1. **State safety policy and objectives**
   - 1.1 State safety legislative framework
   - 1.2 State safety responsibilities and accountabilities
   - 1.3 Accident and incident investigation
   - 1.4 Enforcement policy
2. **State safety risk management**
   - 2.1 Safety requirements for service providers SMS
   - 2.2 Agreement on service providers safety performance
3. **State safety assurance**
   - 3.1 Safety oversight
   - 3.2 Safety data collection, analysis and exchange

3.3 Safety data driven targeting of oversight on areas of greater concern or need

**4. State safety promotion**

4.1 Internal training, communication and dissemination of safety information

4.2 External training, communication and dissemination of safety information

## STATE SAFETY PROGRAMME (SSP) GAP ANALYSIS

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| Component 1 – STATE SAFETY POLICIES AND OBJECTIVES | | | |
| Element 1.1 – State safety legislative framework | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] promulgated a national safety legislative framework and specific regulations that define the management of safety in the State? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] defined the specific activities related to the management of safety in the State that each [State] aviation organization must participate? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] established requirements, responsibilities and accountabilities regarding the management of safety in [State] by its aviation organizations? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are the legislative framework and specific regulations periodically reviewed to ensure they remain relevant and appropriate to the State? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are [State] legislative framework and specific regulations periodically reviewed to ensure that they are up-to-date with respect to international standards? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] established a safety policy? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) | Is [State] safety policy signed by the [State] SSP accountable manager or a high authority within | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| Chapter 11 | [State]? | | |
| SMM (Doc 9859) Chapter 11 | Is [State] safety policy reviewed periodically? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is [State] safety policy communicated with visible endorsement to all employees in all [State] aviation organizations with the intent that they are made aware of their individual safety responsibilities? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] developed documentation that describes the SSP, including the interrelationship between its components and elements? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does [State] have a record system that ensures the generation and retention of all records necessary to document and support the SSP activities? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the record system provide the control processes necessary to ensure appropriate identification, legibility, storage, protection, archiving, retrieval, retention time, and disposition of records? | ☐ Yes<br>☐ No | |
| Element 1.2 – State safety responsibilities and accountabilities | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] identified and defined the State requirements, responsibilities and accountabilities regarding the establishment and maintenance of the SSP? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do the requirements include directives and activities to plan, organize, develop, control and continuously improve the SSP in a manner that meet [State] safety objectives? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do the requirements include a clear statement about the provision of the necessary resources for the implementation and maintenance of the SSP? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) | Has [State] identified and appointed an accountable manager as the qualified person having direct | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| Chapter 11 | responsibility for the SSP implementation, operation and supervision? | | |
| SMM (Doc 9859) Chapter 11 | Does the [State] SSP accountable manager fulfil the required job functions and responsibilities? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the [State] SSP accountable manager ensure that the [State] SSP is performing to requirements in all [State] aviation organizations involved? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the [State] SSP accountable manager have control of the necessary resources required for the proper execution of the SSP? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the [State] SSP accountable manager verify that all [State] aviation organizations personnel understand their authorities, responsibilities and accountabilities in regards of the SSP and all safety management processes, decisions and actions? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are safety responsibilities and accountabilities, at all levels, defined and documented? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] developed an Acceptable Level of Safety (ALoS) for its SSP? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does [State] ALoS for the SSP combine elements of safety measurement and safety performance measurement? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is [State] ALoS commensurate to the complexity of aviation activities within [State]? | ☐ Yes<br>☐ No | |
| Element 1.3 – Accident and incident investigation | | | |
| SMM (Doc 9859) | Has [State] established, as part of the management of | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| Chapter 11 | safety, an independent accident and incident investigation process, the sole objective of which is the prevention of accidents and incidents, and not the apportioning of blame or liability? | | |
| SMM (Doc 9859) Chapter 11 | Does [State] maintain the independence of the accident and incident investigation organization from other State aviation organizations? | ☐ Yes<br>☐ No | |
| Element 1.4 – Enforcement policy | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] promulgated an enforcement policy? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the enforcement policy establish the conditions and circumstances under which service providers are allowed to deal with, and resolve, events involving certain safety deviations internally, within the context of the service provider safety management system (SMS), and to the satisfaction of the appropriate State authority? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the enforcement policy establish the conditions and circumstances under which to deal with safety deviations through established enforcement procedures? | ☐ Yes<br>☐ No | |
| Component 2 – STATE SAFETY RISK MANAGEMENT | | | |
| Element 2.1 – Safety requirements for service providers SMS | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] established the controls which govern how service providers will identify hazards and manage safety risks? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do those controls include requirements, specific operating regulations and implementation policies for service providers SMS? | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 11 | Are requirements, specific operating regulations and implementation policies based on identified hazards and analysis of the safety risks of the consequences of hazards? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are requirements, specific operating regulations and implementation policies periodically reviewed to ensure they remain relevant and appropriate to the service providers? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is there a structured process within [State] to assess how the service providers will manage the safety risks associated with identified hazards, expressed in terms of probability and severity of occurrence? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is there a [State] policy in place that ensures effective safety reporting of safety deficiencies, hazards or occurrences including the conditions under which protection from disciplinary and /or administrative action applies? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does [State] policy on reporting of safety deficiencies, hazards or occurrences include the conditions under which protection from disciplinary and /or administrative action applies? | ☐ Yes<br>☐ No | |
| Element 2.2 – Agreement on service providers safety performance | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] individually agreed with service providers on the safety performance of their SMS? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is the agreed safety performance commensurate to the complexity of individual service providers specific operational contexts? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Does the agreed safety performance consider individual service provider resources to address safety risks? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is the agreed safety performance expressed by multiple safety indicators and safety targets, as opposed to a | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| | single one, as well as by safety requirements? | | |
| SMM (Doc 9859) Chapter 11 | Is the agreed safety performance periodically reviewed to ensure it remains relevant and appropriate to the service providers? | ☐ Yes<br>☐ No | |
| Component 3 – STATE SAFETY ASSURANCE | | | |
| Element 3.1 – Safety oversight | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] has established mechanisms to ensure an effective monitoring of the eight critical elements of the safety oversight function? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] established mechanisms to ensure that the identification of hazards and the management of safety risks by service providers follow established regulatory controls? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do established mechanisms include inspections, audits and surveys to ensure that regulatory safety risk controls are appropriately integrated into the SMS service providers? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do established mechanisms ensure that regulatory safety risk controls are practised as designed? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do established mechanisms ensure that regulatory safety risk controls have the intended effect on safety risks? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are regular and periodic reviews conducted regarding [State] AIoS? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Do reviews consider changes that could affect [State] SSP and its ALoS, recommendations for improvement and sharing of best practices across the State? | ☐ Yes<br>☐ No | |
| SMM | Are regular and periodic reviews conducted to assess if | ☐ Yes | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| (Doc 9859) Chapter 11 | [State] SSP and its ALoS remain appropriate to the scope and complexity of the aviation operations in the State? | ☐ No | |
| SMM (Doc 9859) Chapter 11 | Is there a process to evaluate the effectiveness of changes related to the SSP? | ☐ Yes<br>☐ No | |
| Element 3.2 – Safety data collection, analysis and exchange | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] established mechanisms to ensure the capture and storage of data on hazards and safety risks at both the individual and aggregate State level? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Has [State] established mechanisms to develop information from the stored data, and to promote the exchange of safety information with service providers and/or other States as appropriate? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is there a formal process within [State] to develop and maintain a set of performance parameters to measure the safety performance of the SSP, beyond ALoS? | ☐ Yes<br>☐ No | |
| Element 3.3 – Safety data driven targeting of oversight on areas of greater concern or need | | | |
| SMM (Doc 9859) Chapter 11 | Has [State] developed procedures to prioritize inspections, audits and surveys towards those areas of greater safety concern or need? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is the prioritization of inspections and audits the result of the analysis of data on hazards, their consequences in operations, and the assessed safety risks? | ☐ Yes<br>☐ No | |
| Component 4 – STATE SAFETY PROMOTION | | | |
| Element 4.1 – Internal training, communication and dissemination of safety information | | | |
| SMM (Doc 9859) Chapter 11 | Does [State] provide internal training, awareness, and two-way communication of safety-relevant information within the State aviation organizations? | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 11 | Are there communication processes in place within [State] to ensure that information about the SSP functions and products is timely available to [State] aviation organizations? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is there a process for the dissemination of safety information throughout [State] aviation organizations and a means of monitoring the effectiveness of this process? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are communication processes (written, meetings, electronic, etc.) commensurate with the size and scope of the [State] aviation organizations? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is safety information and information about the SSP functions and products maintained in a suitable medium? | ☐ Yes<br>☐ No | |
| Element 4.2 – External training, communication and dissemination of safety information | | | |
| SMM (Doc 9859) Chapter 11 | Does the [State] provide external education, awareness of safety risks and two-way communication of safety-relevant information? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are there communication processes in place within [State] that allow the SSP to be nationally and internationally promoted? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is there a formal process for the external dissemination of safety information throughout the [State] service providers, and means of monitoring the effectiveness of this process? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Are there communication processes in place within [State] to ensure that information about the SSP functions and products is timely available to [State] service providers? | ☐ Yes<br>☐ No | |

| ICAO reference | Aspects to be analyzed or question to be answered | Answer | Status of implementation |
|---|---|---|---|
| SMM (Doc 9859) Chapter 11 | Are communication processes (written, meetings, electronic, etc.) commensurate with the size and scope of [State] service providers? | ☐ Yes<br>☐ No | |
| SMM (Doc 9859) Chapter 11 | Is safety information and information about the SSP functions and products established and maintained in a suitable medium? | ☐ Yes<br>☐ No | |

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 4 to Chapter 11

# Guidance on the development of a State's enforcement policy and enforcement procedures in an SMS environment

## Enforcement policy

### 1.1 Introduction

This enforcement policy is promulgated under the statutory authority in [State's applicable civil aviation regulation(s), air navigation order(s) or regulatory standard(s)].

### 1.2 Principles

This enforcement policy is the culmination of a comprehensive review by [State's CAA] of its capacity and regulations for evaluating safety activities by service providers.

The implementation of safety management systems (SMS) requires that [State's CAA], develop a flexible enforcement approach to this evolving safety framework while at the same time carrying out enforcement functions in an equitable, practical and consistent manner. A flexible enforcement approach in an SMS environment should be based in two general principles.

The first general principle is to develop enforcement procedures that allow service providers to deal with, and resolve, certain events involving safety deviations internally, within the context of the service provider SMS, and to the satisfaction of the authority. Intentional contraventions of the [State's Civil Aviation Act] and the [State's Civil Aviation Regulations] will be investigated and may be subject to conventional enforcement action if appropriate.

The second general principle is that no information derived from a safety data, collection and processing systems (SDCPS) established under SMS shall be used as the basis for enforcement action.

### 2. Scope

The principles underlying this enforcement policy statement and associated enforcement procedures apply to service providers operating in accordance with ICAO Annex 1 — Personnel Licensing, Annex 6 — Operation of Aircraft, Part I — International Commercial Air Transport — Aeroplanes, and Part III — International Operations — Helicopters, Annex 8 — Airworthiness of Aircraft, ICAO Annex 11 — Air Traffic Services, and ICAO Annex 14 — Aerodromes, Volume I — Aerodrome Design and Operations.

Within the context of this guidance the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.

### 3. General

[Service provider] will establish, maintain and adhere to an SMS that is commensurate to the size, nature and complexity of the operations authorized to be conducted under their operations certificate and to the hazards and safety risks related to these operations.

In order to develop an enforcement policy that supports the implementation of SMS, [State's CAA] inspectors will maintain an open communication with service providers.

When a service provider operating under an SMS unintentional contravenes [Civil Aviation act or Civil Aviation regulations], specific review procedures will be used. These procedures will allow the [State's CAA] inspector responsible for the oversight of the service provider the opportunity to engage in dialogue with the SMS governed organization. The objective of this dialogue is to agree on proposed corrective measures and an action plan that adequately addresses the deficiencies that led to the contravention and to afford the service provider a reasonable time to implement them. This approach aims to nurture and sustain effective safety reporting, whereby service providers' employees can report safety deficiencies and hazards without fear of punitive action. A service provider can therefore, without apportioning blame, and without fear of enforcement action, analyze the event and the organizational or individual factors that may have led to it, in order to incorporate remedial measures that will best help prevent recurrence.

## 4. Remedial measures

[State's CAA], through the inspector responsible for the oversight of the service provider, will evaluate the corrective measures proposed by the service provider, and/or the systems currently in place to address the event underlying the contravention. If corrective measures proposed are considered appropriate and likely to prevent recurrence and foster future compliance, the review of the violation will then be concluded with no enforcement action. In cases where either the corrective measures or the systems in place are considered inappropriate, [State's CAA] will continue to interact with the service provider to find a satisfactory resolution that would prevent enforcement action. However, in cases where the service provider refuses to address the event and provide effective corrective measures, [State's CAA] will consider taking enforcement action or other administrative action regarding the certificate.

## 5. Enforcement procedures

Breaches of aviation regulations may occur for many different reasons, from a genuine misunderstanding of the regulations, to disregard for aviation safety. [State's CAA] has a range of enforcement procedures in order to effectively address safety obligations under the [applicable State Act] in light of different circumstances. These procedures may result in a variety of actions such as:

- Counselling
- Remedial training; or
- Variation, suspension and cancellation of authorisations

## 6. Impartiality of enforcement actions

Enforcement decisions must not be influenced by:

- Personal conflict;
- Considerations such as gender, race, religion, political views or affiliation;

or

- Personal, political or financial power of those involved.

## 7. Proportionality of responses

Enforcement decisions must be proportional responses to the identified breaches and the safety risks they underlie, based in two principles:

- [State's CAA] will take an action against those who consistently and deliberately operate outside civil aviation regulations; and
- [State's CAA] will seek to educate and promote training or supervision of those who show commitment in resolving safety deficiencies

## 8. Natural justice and accountability

Enforcement decisions must be:

- Fair and follow due process;
- Transparent to those involved;
- Take into account the circumstances of the case and the attitude/actions of the service provider when considering action;
- Consistent actions/decisions between like/similar circumstances; and
- Subject to appropriate internal and external review.

## 9. Exceptions

This policy is not applicable if there is evidence of a deliberate effort to conceal non-compliance.

This policy is not applicable if the service provider fails to provide confidence in its means of hazard identification and safety risk management.

This policy is not applicable if the service provider is a recurrent violator. A recurrent violator is a violator who, in the past [term], has had the same or closely related violations.

In such circumstances, the penalty matrix (or applicable measurement) of the established enforcement procedures will be applicable

(Signed)

_____

State [CAA] Accountable Executive

# Enforcement procedures in an SMS environment

## 1. General

This guidance assists in determining enforcement procedures used for investigations of contraventions by service providers conducting activities under an SMS.

Under the [State's] State Safety Programme (SSP), the [State's CAA] is responsible for oversight of certificate holders operating in an SMS environment. Enforcement procedures must provide guidance to those responsible for the oversight of service providers operating in an SMS environment, by advising on the appropriate response to acts or omissions to ensure that if enforcement action is taken it will be successful. Enforcement procedures play a supporting function in the process and the final decision regarding any enforcement issue is the responsibility of the accountable executive.

## 2. Applicability

These procedures apply to contraventions that may have been committed by persons or service providers conducting activities under an SMS.

These procedures are effective as of [date]. They replace and supersede previous procedures identified in [State's Civil Aviation Regulations].

Where service providers have demonstrated the willingness to conduct their operations under an SMS, SMS enforcement procedures may be used in respect to contraventions by those service providers that, although they do not have an accepted SMS, have some essential core components of an SMS are in place and are in the process of full implementation.

[State's CAA] will not apply the SMS enforcement procedures to any service providers that, subsequent to the initiation of an investigation of a contravention, arbitrarily claim to be developing an SMS. These procedures will be used for service providers that have been diligently involved in the development of an SMS which would eventually meet the requirements of the SMS regulations, and are following a "phased approach" process similar to the one outlined in [State's CAA] published advisory material [AC-xxx] - Implementation Procedures Guide for SMS.

Where service providers have not demonstrated they are operating in an SMS environment, the enforcement actions may apply without the advantages of procedures explained in paragraph 3.

## 3. Procedures

For the purpose of determining whether an investigation should be conducted using SMS enforcement procedures, it will be necessary for aviation enforcement investigators to determine the SMS implementation status of any specific service provider. This determination would initially be made through communication between the investigators and the principal inspector who is responsible for oversight and certification of the service provider under investigation.

The principal inspector will ascertain if the service provider meets the above-mentioned criteria for SMS enforcement procedures. In order to facilitate initial assessment, [State's CAA] may develop a list of service providers that have initiated the SMS development and implementation process. Making the list available to aviation enforcement will assist the investigators in making a decision regarding the use of the SMS enforcement procedures.

During the "phased approach" stage of the service provider's SMS, [State's CAA] will apply the SMS enforcement procedures to service providers that do not have a fully implemented SMS, provided that certain conditions are met.

[State's CAA] will require, as a minimum, that the three following conditions be met before SMS enforcement procedures may be applied:

1) The service provider has an effective internal hazard reporting programme supported by upper management;

2) The service provider has a proactive event analysis process commensurate to the size and complexity of its operations and adequate for determining causal factors and developing corrective measures;

3) The information derived from the process referred to in paragraph 2 above is communicated appropriately protected so as not to endanger SDCPS upon request to the principal inspector assigned to the specific service provider.

### 3.1 Initial report of violation

Aviation enforcement inspectors must conduct a preliminary analysis in all cases where a contravention is detected or where information about a possible contravention is received.

### 3.2 Preliminary analysis

The following questions should be considered based on the information received:

1) Are there reasonable grounds to believe that a person or organization conducting activities under an SMS may have committed a contravention?

2) Is the event of such serious nature that enforcement action should be considered?

3) Is there any perishable evidence that should be secured for enforcement action?

### 3.3 Providing effective support

When the three questions are answered in the affirmative, the principal inspector shall be notified. The information shall identify the event and the contravention.

When requested, aviation enforcement investigators will provide effective support to the accountable executive by advising on the appropriate response the contravention, in order to ensure that if enforcement action is taken, it will be successful. Support for the accountable executive includes collecting or securing perishable evidence.

### 3.4 Initiating an enforcement investigation

An enforcement investigation shall only be initiated upon the request of the principal inspector not the enforcement investigators

### 3.5 Immunity

No information derived from a SDCPS established under an SMS will be used as the basis for enforcement action.

***Note**: The SMS enforcement policy and associated procedures may also apply to foreign air operators who operate under SMS regulations and that follow the requirements and guidance ser forth by the International Civil Aviation Organization (ICAO) are meeting the conditions mentioned above in paragraph 3*

- - - - - - - - - - - - - - -

*Page left blank intentionally*

# Appendix 5 to Chapter 11

# GUIDANCE ON AN SSP IMPLEMENTATION PLAN

## INTRODUCTION

### 1. Background

This Appendix provides guidance to assist States in developing an SSP implementation plan. An SSP implementation plan describes how a State will put in practice, sequentially and in a principled manner, the processes, procedures and means that will allow discharging the State's responsibilities associated with the management of safety in civil aviation.

The implementation of an SSP must be commensurate with the size and complexity of the State's aviation system, and may require coordination among multiple authorities responsible for individual element functions in the State. This guidance is intended as a reference and may need to be tailored to meet the particular needs of States.

The development of an SSP implementation plan will allow States to:

- Formulate an overarching strategy for the management of safety in the State;
- Coordinate the processes executed by the different State aviation organizations under the SSP;
- Establish the controls that govern how service providers safety management systems (SMS) will operate;
- Ensure that the operation of service providers' SMS follows established controls; and
- Support the interaction between the SSP and the operation of service providers SMS.

When the State is responsible for the provision of specific services (e.g. aerodromes, air navigation services, etc.) the organization providing the service should develop and implement an SMS (refer to the SMS implementation plan as in Appendix 2 to Chapter 10).

> ***Note***. – *Within the context of this Appendix the term "service provider" refers to any organization providing aviation services. The term includes approved training organizations that are exposed to safety risks during the provision of their services, aircraft operators, approved maintenance organizations, organizations responsible for type design and/or manufacture of aircraft, air traffic services providers and certified aerodromes, as applicable.*

### 2. SSP gap analysis

In order to develop an SSP implementation plan, a gap analysis of structures and processes existing in the State should be conducted against the ICAO SSP framework. This will allow the State to assess the existence and maturity within the State of the elements of an SSP. Once the gap analysis is completed and documented, the components/elements identified as missing or deficient will form, together with those already existing or effective, the basis of the SSP implementation plan.

Each component/element should be assessed to determine if the State must create or modify regulations, policies or procedures to develop the required components /elements into the SSP. The ICAO SSP framework that forms the basis for the development of the SSP implementation plan includes four components and eleven elements, as follows:

1. State safety policy and objectives

a) State safety legislative framework

b) State safety responsibilities and accountabilities

c) Accident and incident investigation

d) Enforcement policy

2. State safety risk management

a) Safety requirements for service providers SMS

b) Agreement of service providers safety performance

3. State safety assurance

a) Safety oversight

b) Safety data collection, analysis and exchange

c) Safety data driven targeting of oversight on areas of greater concern or need

4. State safety promotion

a) Internal training, communication and dissemination of safety information

b) External training, communication and dissemination of safety information

## 3. SSP implementation plan

The SSP implementation plan is a blueprint of how the SSP will be developed and integrated into the State safety management activities. Given the potential magnitude of the effort, it is important to properly manage the workload associated to the activities underlying the development and implementation of the SSP. It is proposed that the four components and eleven elements of the ICAO SSP framework be implemented in a sequential order that allows for the achievement of specific deliverables. The sequential order will depend on the result of the gap analysis and the complexity and scope of the aviation system within each State.

One of the specific objectives of an SSP is to generate a context which is supportive of the implementation of SMS by service providers. Therefore, within the scope of the SSP activities, four specific steps support SMS implementation by service providers. These four steps are discussed in Chapter 11.

### 3.1 State safety policy and objectives

#### a) State safety legislative framework

- Review, develop and promulgate, as necessary, a national safety legislative framework and specific regulations in compliance with international and national standards that define how the State will oversee the management of safety within its jurisdiction.
- Establish a national-level group within the State in a form of board, committee etc., to ensure the coordinated participation of State aviation organizations in specific activities related to the management of safety in the State, and the establishment of the roles, responsibilities, and relationships of such organizations.

- Establish a timeframe to periodically review the safety legislation and specific operating regulations to ensure they remain relevant and appropriate to the State.

**b) State safety responsibilities and accountabilities**

- Identify, define and document the requirements, responsibilities and accountabilities regarding the establishment and maintenance of the SSP. This includes the directives to plan, organize, develop, maintain control and continuously improve the SSP in a manner that meets the State safety objectives. Include a clear statement about the provision of the necessary resources for the implementation of the SSP.
- Identify and appoint the Accountable Executive for the State SSP ,that shall have *inter-alia*,
    - the ultimate responsibility and accountability, on behalf of the State, for the implementation and maintenance of the SSP;
    - full authority on human resources issues related to State aviation organizations;
    - full authority on major financial issues related to State aviation organizations;
    - final authority over service providers certificate management aspects; and
    - final responsibility for the resolution of all State's aviation safety issues.
- Establish the SSP implementation team.
- Assign the time required for each task associated to the implementation of the SSP among the different management levels of the State aviation organizations.
- Introduce all staff to SSP concepts at a level commensurate to each staff involvement within the SSP.
- Develop and implement a State safety policy that includes at least, but not necessarily limited to:
    - the commitment to develop and implement strategies and processes to ensure that all aviation activities under oversight will achieve the highest level of safety performance;
    - the development and promulgation of national safety legislative framework and applicable operating regulations for the management of safety in the State;
    - the commitment to allocate the necessary resources within the State aviation organizations to allow their personnel to discharge their responsibilities, both safety-related and otherwise;
    - the support of the management of safety in the State through an effective hazard reporting and communication system;
    - the establishment of provisions for the protection of safety data, collection and processing systems (SDCPS);
    - the commitment to an effective Interaction with service providers in the resolution of safety concerns;
    - the commitment to communicate, with visible endorsement, the State safety policy to all staff; and
    - an enforcement policy that reflects service providers operations under an SMS environment.
- Establish the necessary means to ensure that the State safety policy is understood, implemented and observed at all levels within the State aviation organizations.

- Establish the Acceptable Level of Safety (ALoS) for the SSP, comprising a combination of safety measurement and safety performance measurement.
    - Safety measurement includes the quantification of the outcomes of high-level, high-consequence events or high-level State functions, such as accident rates, serious incident rates, regulatory compliance, etc.
    - Safety performance measurement includes the quantification of the outcomes of the low-level, low-consequence processes that provides a measure of the actual performance of an individual SSP beyond accident rates and/or regulatory compliance.

### c) Accident and incident investigation

- Develop and establish the mechanisms to ensure an independent accident and incident investigation process, the sole objective of which is the prevention of accidents and incidents, in support of the management of safety in the State, and not the apportioning of blame or liability.
- Develop and establish the necessary arrangements to ensure the independence of the accident and incident investigation authority from other aviation organizations of the State.

### d) Enforcement policy

- Develop and promulgate an enforcement policy that establishes the conditions and circumstances under which service providers are allowed to deal with, and resolve, events involving certain safety deviations internally, within the context of the service provider safety management system (SMS), and to the satisfaction of the appropriate State authority. The enforcement policy also establishes the conditions and circumstances under which to deal with safety deviations through established enforcement procedures.
- The policy should also ensure that no information obtained from an internal hazard reporting system or a flight data monitoring system established under an SMS will be used for enforcement action

### e) SSP documentation

- Develop and establish a State safety library that documents the requirements, responsibilities and accountabilities regarding the establishment and maintenance of the SSP. The safety library will maintain and update as necessary, the SSP documentation related to the national safety legislative framework, the State safety policy and objectives, the SSP requirements, the SSP processes and procedures, the accountabilities, responsibilities and authorities for processes and procedures, and the State acceptable level of safety (ALoS) for the SSP.

**Deliverables**

1. State safety legislative framework promulgated.
2. State safety responsibilities and accountabilities established, documented and published.
3. State safety and enforcement policies signed by Accountable Executive
4. Safety and enforcement policies distributed within the aviation organizations of the State and among service providers under oversight.
5. ALoS established, documented and published.
6. Independent accident and incident investigation process in place.

7. SSP organizational structure in place.

**Milestones**

1. Identification of the Accountable Executive.
2. Draft proposal of safety policy.
3. Lines of safety responsibility and accountability established.
4. ALoS approved.
5. Proposal of SSP organizational structure approved.
6. Budget for SSP processes approved.

*Note: The deliverables and milestones proposed in this Appendix are just an example and should not be limited to other deliverables that may be foreseen from the implementation of the components of the SSP framework in States with different scope and complexity of their aviation activity.*

### 3.2 State safety risk management

#### a) Safety requirements for service providers SMS

- Establish the requirements, specific operating regulations and implementation policies for service providers SMS (SMS regulatory framework, advisory circulars, etc.) as the controls which govern how service providers will identify hazards and manage and control safety risks.
- Establish a timeframe for consultation with service providers on those requirements.
- Establish a timeframe to periodically review the requirements and specific operating regulations to ensure they remain relevant and appropriate to the service providers.

#### b) Agreement of service provider safety performance.

- Develop and establish a procedure for the agreement on safety performance of individual service providers SMS based on:
  - safety performance indicators;
  - safety performance targets; and
  - safety requirements
- Include within the agreed procedure that service providers safety performance should be commensurate to:
  - The complexity of individual service provider's specific operational contexts; and
  - The availability of individual service provider's resources to address safety risks.

- Establish the measurement of safety performance of service providers SMS, through periodic reviews of the agreed safety performance of the SMS to ensure that safety performance indicators and safety performance targets remain relevant and appropriate to the service provider.
- Develop means to assess lower level outcomes and most frequent processes among different service providers.
- Determine measurable performance outcomes within different SMS.

**Deliverables**

1. SMS regulations promulgated.
2. Guidance material on implementation of SMS distributed to service providers.
3. Agreement on service providers safety performance completed.
4. First annual review of agreed service providers safety performance completed.

**Milestones**

1. Draft proposal of SMS regulations distributed to service providers for review.
2. Draft proposal of SMS guidance material distributed to service providers for review.
3. Consultation among service providers on the establishment of safety requirements completed.
4. Procedure of agreement on service providers safety performance completed.

### 3.3 State safety assurance

#### a) Safety oversight

- Establish mechanisms to ensure an effective monitoring of the eight critical elements of the safety oversight function.
- Establish mechanisms that guarantee that the identification of hazards and the management of safety risks by service providers follow established regulatory controls.
- Establish mechanisms that guarantee that safety risk controls are integrated into service provider's SMS.
- Develop an internal SSP audit.

#### b) Safety data collection, analysis and exchange

- Develop and establish means of collecting, analysing and storing data about hazards and safety risks at the State level:
    - establish a mandatory hazard reporting system;
    - establish a confidential hazard reporting system;

- develop a State hazard database;
- establish a mechanism to develop information from the stored data;
- establish means to collect hazards at an aggregate State level as well as at individual service provider level; and
- establish means to implement corrective action plans.

- Ensure that service provider's hazard identification and safety risk management processes follow established regulatory requirements and that safety risk controls are appropriately integrated into the service providers' SMS, including, but not necessarily limited to:
  - inspections;
  - audits; and
  - surveys
- Observe the following sequence for implementation:
  - regulatory safety risk controls integrated with service provider's SMS;
  - oversight activities to ensure service provider's hazard identification and safety risk management processes follow established regulatory requirements implemented; and
  - conduct oversight activities to verify that safety risk controls are practiced by service providers.

**c) Safety data driven targeting of oversight of areas of greater concern or need.**

- Establish procedures to prioritize inspections, audits and surveys, based on analysis of hazards and safety risks.

**Deliverables**

1. Information on hazards and safety risks at an aggregate State level as well as individual service provider level collected.
2. First cycle of oversight mechanisms on safety risk controls of service providers completed.
3. First annual review of the safety policy and objectives.
4. First annual review of the enforcement policy.

**Milestones**

- Hazards and safety risks data storage and processing at State as well as individual service's provider level developed.

## 3.4 State safety promotion

**a) Internal training, communication and dissemination of safety information**

- Identify internal training requirements.
- Develop and provide generic safety training to all staff.
- Develop a training programme on key components of an SSP and SMS for staff that includes:
    - Indoctrination/initial safety training.
    - On the job (OJT) safety training.
    - Recurrent safety training.
- Establish means to measure the effectiveness of training.
- Develop means to communicate safety related issues internally, including:
    - safety policies and procedures;
    - newsletters;
    - bulletins; and
    - a website.

**b) External training, communication and dissemination of safety information**

- Establish the means to provide two-way communication of safety relevant information to support SMS implementation among service providers, including small operators.
- Develop training and guidance material on implementation of SMS for service providers.
- Establish the means to communicate safety related issues externally including:
    - safety policies and procedures;
    - newsletters;
    - bulletins; and
    - a website.

**Deliverables**

1. First cycle of generic safety training to staff completed.
2. Training programme on key components of an SSP and SMS for technical and supporting staff completed.
3. Guidance material of SMS distributed to service providers, including small operators
4. First cycle of training on implementation of SMS to service providers completed.

5. Means to communicate safety related information internally and externally established.

**Milestones**

1. Establishment of minimum knowledge and experience requirements for technical personnel performing safety oversight functions.
2. Guidance material of SMS developed and published.
3. Training programmes on SMS for aviation organizations of the State and service providers developed.
4. State newsletter and bulletins developed.

- - - - - - - - - - - - - - -

# Attachment A

# ICAO ACCIDENT/INCIDENT DATA REPORTING (ADREP) SYSTEM

In accordance with Annex 13, Aircraft Accident and Incident Investigation, States report to ICAO information on all aircraft accidents that involve aircraft of a maximum certified take-off mass of over 2 250 kg. ICAO also gathers information on aircraft incidents (involving aircraft over 5 700 kg) considered to be important for safety and accident prevention. This reporting system is known as ADREP. States report specific data in a predetermined (and coded) format to ICAO. When ADREP reports are received from States, the information is checked and electronically stored, constituting a databank of worldwide occurrences.

ICAO does not require States to investigate incidents. However, if a State does investigate a serious incident, it is requested to submit formatted data to ICAO. The types of serious incidents of interest to ICAO include:

a) multiple system failures;

b) fires or smoke on board an aircraft;

c) terrain and obstacle clearance incidents;

d) flight control and stability problems;

e) take-off and landing incidents;

f) flight crew incapacitation;

g) decompression; and

h) near collisions and other serious air traffic incidents.

- - - - - - - - - - - - - - -

# Attachment B

# EMERGENCY RESPONSE PLANNING

## INTRODUCTION

Perhaps because aviation accidents are rare events, few organizations are prepared when one occurs. Many organizations do not have effective plans in place to manage events during or following an emergency or crisis. How an organization fares in the aftermath of an accident or other emergency can depend on how well it handles the first few hours and days following a major safety event. An emergency plan outlines in writing what should be done after an accident, and who is responsible for each action. In aerodrome operations, such emergency planning is referred to as an Airport Emergency Plan (AEP). In this manual, the generic term Emergency Response Plan (ERP) is used.

While it is normal to think of emergency response planning with respect to aircraft or aerodrome operations, usually as a result of an aircraft accident, the concept can equally be applied to other service providers. In the case of ATS providers this may include a major power outage, or loss of radar, communications or other major facilities. For a maintenance organization it may involve a hangar fire or major fuel spill. In this context, an emergency is considered to be an event that could cause major harm or disruption to an organization.

At first glance, emergency planning may appear to have little to do with safety management. However, effective emergency response provides an opportunity to learn, as well as to apply safety lessons aimed at minimizing damage or injury.

Successful response to an emergency begins with effective planning. An Emergency Response Plan (ERP) provides the basis for a systematic approach to managing the organization's affairs in the aftermath of a significant unplanned event – in the worst case, a major accident.

The purpose of an emergency response plan is to ensure that there is:

a) Orderly and efficient transition from normal to emergency operations;

b) Delegation of emergency authority;

c) Assignment of emergency responsibilities;

d) Authorization by key personnel for actions contained in the plan;

e) Coordination of efforts to cope with the emergency; and

f) Safe continuation of operations, or return to normal operations as soon as possible.

## ICAO REQUIREMENTS

Any organization conducting or supporting flight operations should have an emergency response plan. For example:

a) The ICAO Annex 14 — Aerodromes states that, an aerodrome emergency plan shall be established at an aerodrome, commensurate with the aircraft operations and other activities conducted at an airport. The plan shall provide for the coordination of the actions to be taken in an emergency occurring at an aerodrome or in its vicinity.

b) The ICAO manual entitled Preparation of an Operations Manual (Doc 9376) states that the operations manual of a company should give instructions and guidance on the duties and obligations of personnel following an accident. It should include guidance on the establishment and operation of a central accident/emergency response centre – the focal point for crisis management. In addition to guidance for accidents involving company aircraft, guidance should also be provided for accidents involving aircraft for which it is the handling agent (for example, through code-sharing agreements or contracted services). Larger companies may choose to consolidate all this emergency planning information in a separate volume of their operations manual.

c) The ICAO Airport Services Manual, Part 7 — Airport Emergency Planning (Doc 9137) gives guidance to both airport authorities and aircraft operators on preplanning for emergencies, as well as on coordination between the different airport agencies, including the operator.

To be effective, an ERP should be:

a) Be relevant and useful for the people who are likely to be on duty at the time of an accident;

b) Include checklists and quick reference contact details of relevant personnel;

c) Be regularly tested through exercises; and

d) Be updated when details change.

## PLAN CONTENTS

An Emergency Response Plan (ERP) would normally be documented in the format of a manual. It should set out the responsibilities and roles and actions for the various agencies and personnel involved in dealing with emergencies. An ERP should take account of such considerations as:

**Governing policies**. The ERP should provide direction for responding to emergencies, such as governing laws and regulations for investigations, agreements with local authorities, company policies and priorities, etc.

**Organization**. The ERP should outline management's intentions with respect to the responding organizations by:

a) Designating who will lead and who will be assigned to the responding teams;

b) Defining the roles and responsibilities for personnel assigned to the response teams;

c) Clarifying the reporting lines of authority;

d) Setting up of a Crisis Management Centre (CMC);

e) Establishing procedures for receiving a large number of requests for information, especially during the first few days after a major accident;

f) Designating the corporate spokesperson for dealing with the media;

g) Defining what resources will be available, including financial authorities for immediate activities;

h) Designating the company representative to any formal investigations undertaken by State officials; and

i) Defining a call-out plan for key personnel, etc.

An organization or flow chart could be used to show organizational functions and communication relationships.

**Notifications**. The plan should specify who in the organization should be notified of an emergency, who will make external notifications and by what means. The notification needs of the following should be considered:

a) Management;

b) State authorities (Search and Rescue, regulatory authority, accident investigation board, etc.);

c) Local emergency response services (airport authorities, fire fighters, police, ambulances, medical agencies, etc);

d) Relatives of victims — a sensitive issue, in many States handled by the police;

e) Company personnel;

f) Media;

g) Legal, accounting, insurers, etc.

**Initial response**. Depending on the circumstances, an initial response team may be dispatched to the accident site to augment local resources and oversee the organization's interests. Factors to be considered for such a team include:

a) Who would lead the initial response team?

b) Who would be included on the initial response team?

c) Who would speak for the organization at the accident site?

d) What would be required by way of special equipment, clothing, documentation, transportation, accommodation, etc.?

**Additional assistance**. Employees with appropriate training and experience can provide useful support during the preparation, exercising and updating of an organization's ERP. Their expertise may be useful in planning and executing such tasks as:

a) Acting as passengers in crash exercises;

b) Handling of survivors;

c) Dealing with next of kin, etc.

**Crisis Management Centre (CMC)**. A CMC should be established at the organization's headquarters once the activation criteria have been met. In addition, a command post (CP) may be established at or near the accident site. The ERP should address how the following requirements are to be met:

a) Staffing (perhaps for 24 hours a day 7 days per week during the initial response period);

b) Communications equipment (telephones, fax, Internet, etc.);

c) Documentation requirements, maintenance of emergency activities logs;

d) Impounding related company records;

e) Office furnishings and supplies;

f) Reference documents (such as emergency response checklists and procedures, company manuals, airport emergency plans, telephone lists, etc.).

The services of a crisis centre may be contracted from an airline or other specialist organization to look after the operator's interests in a crisis away from home base. Company personnel would normally supplement such a contracted centre as soon as possible.

**Records**. In addition to the organization's need to maintain logs of events and activities, the organization will also be required to provide information for any State investigation team. The ERP should provide the following types of information to investigators:

a) All relevant records such as the aircraft, the flight crew and the operation;

b) Lists of points of contact and any personnel associated with the occurrence;

c) Notes of any interviews (and statements) with anyone associated with the event;

d) Any photographic or other evidence, etc.

**Accident site**. After a major accident, representatives from many jurisdictions have legitimate reasons for accessing the site, for example, police, fire fighters, medics, airport authorities, coroners (medical examining officers) to deal with fatalities, State accident investigators, relief agencies such as the Red Cross and even the media. Although coordination of the activities of these stakeholders is the responsibility of the State's police and/or investigating authority, the aircraft operator should clarify the following aspects of activity at the accident site:

a) Nominating a senior company representative at the accident site: 1) If at home base;

1) If away from home base;

2) If offshore or in a foreign State.

b) Management of surviving passengers;

c) Needs of relatives of victims;

d) Security of wreckage;

e) Handling of human remains and personal property of the deceased;

f) Preservation of evidence;

g) Provision of assistance (as required) to the investigation authorities;

h) Removal and disposal of wreckage; etc.

**News media**. How the company responds to the media may affect how well the company recovers from the event. Clear direction is required. For example:

a) What information is protected by statute (FDR data, CVR and ATC recordings, witness statements etc.);

b) Who may speak on behalf of the parent organization at head office and at the accident site (Public Relations Manager, Chief Executive Officer or other senior executive, manager, owner);

c) Direction regarding a prepared statement for immediate response to media queries;

d) What information may be released (What should be avoided);

e) The timing and content of the company's initial statement;

f) Provisions for regular updates to the media.

**Formal investigations**. Guidance for company personnel dealing with State accident investigators and police should be provided.

**Family assistance**. The EPR should also include guidance on the organization's approach to assisting the families of accident victims (crew and passengers). This guidance may include such things as:

a) State requirements for the provision of family assistance services;

b) Travel and accommodation arrangements to visit the accident location and survivors;

c) Programme coordinator and point(s) of contact for each family;

d) Provision of up-to-date information;

e) Grief counselling, etc.;

f) Immediate financial assistance to victims and their families;

g) Memorial services, etc. Some States define the types of assistance to be provided by an operator.

**Post critical incident stress counselling**. For personnel working in stressful situations, the ERP may include guidance, specifying duty limits and providing for post incident stress counselling.

**Post occurrence review**. Direction should be provided to ensure that, following the emergency, key personnel carry out a full debrief and record all significant lessons learned which may result in amendments to the ERP and associated checklists.

## AIRCRAFT OPERATOR'S RESPONSIBILITIES

The aircraft operator's emergency response plan (ERP) should be coordinated with the airport emergency plan (AEP) so that the operator's personnel know which responsibilities the airport will assume and what response is required by the operator. 39 As part of their emergency response planning, aircraft operators in conjunction with the airport operator are expected to:40

a) Provide training to prepare personnel for emergencies;

b) Make arrangements to handle incoming telephone queries concerning the emergency;

c) Designate a suitable holding area for uninjured persons ("meeters and greeters");

d) Provide a description of duties for company personnel (e.g. person in command, receptionists for receiving passengers in holding areas);

e) Gather essential passenger information and coordinating fulfillment of their needs;

f) Develop arrangements with other operators and agencies for the provision of mutual support during the emergency;

g) Prepare and maintain an emergency kit containing:

1) Necessary administrative supplies (forms, paper, name tags, computers, etc.); and

2) Critical telephone numbers (doctors, local hotels, linguists, caterers, airline transport companies, etc.).

In the event of an aircraft accident on or near the airport, operators will be expected to take such actions as:

a) Report to airport command post to coordinate the aircraft operator's activities;

b) Assist in the location and recovery of any flight recorders;

c) Assist investigators with the identification of aircraft components and ensure that hazardous components are made safe;

d) Provide information regarding passengers and flight crew, and the existence of any dangerous goods on board;

e) Transport uninjured persons to the designated holding area;

f) Make arrangements for any uninjured persons who may intend to continue their journey, or who need accommodations or other assistance;

g) Release information to the media in coordination with the airport public information officer and police; and

h) Remove the aircraft (and/or wreckage) upon the authorization of the investigation authority.

While this paragraph is oriented towards an aircraft accident, some of the concepts also apply to emergency planning by aerodrome operators and air traffic service providers.

## CHECKLISTS

Everyone involved in the initial response to a major aircraft accident will be suffering from some degree of shock. Therefore, the emergency response process lends itself to the use of checklists. These checklists can form an integral part of the company's Operations or Emergency Response Manuals. To be effective, checklists must be regularly:

a) Reviewed and updated (for example, currency of callout lists, contact details, etc.);

b) Tested through realistic exercises.

## TRAINING AND EXERCISES

An emergency response plan is a paper indication of intent. Hopefully, much of an ERP will never be tested under actual conditions. Training is required to ensure that these intentions are backed by operational capabilities. Since training has a short "shelf-life", regular drills and exercises are advisable. Some portions of the ERP, such as the callout and communications plan can be tested by "desktop" exercises. Other aspects, such as "on-site" activities involving other agencies, need to be exercised at regular intervals. Such exercises have the advantage of demonstrating deficiencies in the plan, which can be rectified before an actual emergency.

- - - - - - - - - - - - - - -

# Attachment C

# RELATED ICAO GUIDANCE MATERIAL

Aviation Medicine Manual (Doc 8984)

Preparation of an Operations Manual (Doc 9376)

Manual of Aircraft Ground De-icing/Anti-icing Operations(Doc 9640)

Manual of All-Weather Operations (Doc 9625)

Airworthiness Manual (Doc 9760)

Manual of Aircraft Accident and Incident Investigation (Doc 9756)

Part I, Organization and Planning

Part III, Investigation

Part IV, Reporting

Guidance on Assistance to Aircraft Accident Victims and Their Families (Circular 285)

Hazards at Aircraft Accident Sites (Circular 315)

Training Guidelines for Aircraft Accident Investigators (Circ 298)

ADREP Reporting (http://www.icao.int/anb/aig/Reporting.html)

Manual of Procedures for Operations Inspection, Certification and Continued Surveillance (Doc 8335)

Manual of Advanced-Surface Movement Guidance and Control Systems (Doc 9830)

Global Air Navigation Plan (Doc 9750)

Global ATM Operational Concept (Doc 9854)

Manual on Interception of Civil Aircraft (Doc 9433)

Manual concerning Safety Measures Relating to Military Activities Potentially Hazardous to Civil Aircraft Operations (Doc 9554)

Manual on Radiotelephony (Doc 9432)

Manual on Airspace Planning Methodology for the Determination of Separation Minima (Doc 9689)

Manual on Reduced Vertical Separation Minimum (RVSM) (Doc 9574)

Manual on Simultaneous Operations on Parallel or Near-Parallel Instrument Runways (Doc 9643)

Manual on Global Performance of the Air Navigation System (Doc 9833)

Performance Based Navigation Manual (Doc 9613)

Manual on Required Communication Performance (Doc 9869)

Manual on ATM System Requirements (Doc 9882)

Methodology for the Determination of Separation Minima Applied to the Spacing between parallel Tracks in ATS Route Structures (Cir 120)

A unified framework for collision risk modelling in support of the manual on airspace planning methodology with further applications. Advanced edition (Cir 319)

Assessment of ADS-B to Support Air Traffic Services and Guidelines for Implementation. Draft, First Edition – 2006 (Cir 311)

Airport Services Manual (Doc 9137)

Aerodrome Design Manual (Doc 9157

Manual on Certification of Aerodromes (Doc 9774)

Manual on IBIS (Doc 9332)

Manual on SMGCS (Doc 9476)

Operation of New Larger Aeroplanes at Existing Aerodromes (Circ 305)

Human Factors Guidelines for Aircraft Maintenance Manual (Doc 9824)

Human Factors Guidelines for Air Traffic Management (ATM) Systems (Doc 9758)

Human Factors Guidelines for Safety Audits Manual (Doc 9806)

Human Factors Training Manual (Doc 9683)

Line Operations Safety Audit (LOSA) (Doc 9803)

Normal Operations Safety Survey (NOSS) (Doc 9910)

Human Factors Digest No 15 – Human Factors in Cabin Safety (Circ 300)

Human Factors Digest No. 16 – Cross-cultural Issues in Aviation Safety (Circ 302)

Human Factors Digest No. 17 – Threat and Error Management (TEM) in Air Traffic Control (Circ 314)

Safety Oversight Audit Manual (Doc 9735)

Safety Oversight Manual (Doc 9734)

- - - - - - - - - - - - - - -