

**Doc 9859
AN/474**



Safety Management Manual (SMM)

Approved by the Secretary General
and published under his authority

Second Edition — 2009

International Civil Aviation Organization

Published in separate English, Arabic, French, Russian and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 University Street, Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents
and booksellers, please go to the ICAO website at www.icao.int

Second edition 2009

ICAO Doc 9859, *Safety Management Manual (SMM)*

Order Number: 9859

ISBN 978-92-9231-295-4

© ICAO 2009

All rights reserved. No part of this publication may be reproduced, stored in a
retrieval system or transmitted in any form or by any means, without prior
permission in writing from the International Civil Aviation Organization.

TABLE OF CONTENTS

	<i>Page</i>
ACRONYMS AND ABBREVIATIONS	(ix)
Chapter 1. OVERVIEW OF THE MANUAL	1-1
1.1 General.....	1-1
1.2 Objectives.....	1-1
1.3 Concept	1-1
1.4 Contents	1-1
1.5 Structure	1-3
Chapter 2. BASIC SAFETY CONTENTS	2-1
2.1 Objective and contents	2-1
2.2 The concept of safety	2-1
2.3 The evolution of safety thinking	2-2
2.4 Accident causation — The Reason model.....	2-5
2.5 The organizational accident.....	2-6
2.6 People, context and safety — The Shel model.....	2-9
2.7 Errors and violations	2-15
2.8 Organizational culture.....	2-23
2.9 Safety investigation.....	2-31
Chapter 3. INTRODUCTION TO SAFETY MANAGEMENT	3-1
3.1 Objective and contents	3-1
3.2 The safety stereotype	3-1
3.3 The management dilemma	3-2
3.4 The need for safety management.....	3-5
3.5 Strategies for safety management.....	3-9
3.6 The imperative of change	3-13
3.7 Safety management — Eight building blocks	3-13
3.8 Four responsibilities for managing safety	3-14
Chapter 4. HAZARDS	4-1
4.1 Objective and contents	4-1
4.2 Hazards and consequences	4-1
4.3 First fundamental — Understanding hazards	4-2
4.4 Second fundamental — Hazard identification.....	4-4
4.5 Third fundamental — Hazard analysis.....	4-6
4.6 Fourth fundamental — Documentation of hazards	4-7

	<i>Page</i>
Appendix 1 to Chapter 4. Safety information analysis	4-APP 1-1
Appendix 2 to Chapter 4. Management of safety information	4-APP 2-1
Chapter 5. SAFETY RISKS	5-1
5.1 Objective and contents	5-1
5.2 Definition of safety risk.....	5-1
5.3 First fundamental — Safety risk management.....	5-2
5.4 Second fundamental — Safety risk probability	5-5
5.5 Third fundamental — Safety risk severity	5-6
5.6 Fourth fundamental — Safety risk tolerability	5-8
5.7 Fifth fundamental — Safety risk control/mitigation.....	5-9
5.8 The five fundamentals of safety risk management — Summary.....	5-13
Appendix 1 to Chapter 5. Anycity International Airport construction plan	5-APP 1-1
Appendix 2 to Chapter 5. Converging runway operations	5-APP 2-1
Appendix 3 to Chapter 5. Commercial operations at Andes City International Airport.....	5-APP 3-1
Chapter 6. ICAO SAFETY MANAGEMENT SARPs	6-1
6.1 Objective and contents	6-1
6.2 ICAO safety management SARPs — General.....	6-1
6.3 State safety programme (SSP).....	6-2
6.4 Acceptable level of safety (ALoS).....	6-3
6.5 Safety management system (SMS).....	6-8
6.6 SMS safety performance	6-9
6.7 Management accountability	6-13
6.8 Relationship between an SSP and an SSM.....	6-13
6.9 Compliance and conformance	6-16
Chapter 7. INTRODUCTION TO SAFETY MANAGEMENT SYSTEMS	7-1
7.1 Objective and contents	7-1
7.2 Introductory concepts	7-1
7.3 SMS features	7-4
7.4 System description	7-4
7.5 Gap analysis	7-6
7.6 SMS and QMS.....	7-8
7.7 SSP/SMS and the accident investigation process	7-11
7.8 Integration of management systems.....	7-11
7.9 Clarifying terms.....	7-12
7.10 The difference between safety slogans and safety principles.....	7-12
Appendix 1 to Chapter 7. Guidance on system description	7-APP 1-1
Appendix 2 to Chapter 7. Guidance on the development of an SMS GAP analysis for service providers	7-APP 2-1

	<i>Page</i>
Chapter 8. SMS PLANNING.....	8-1
8.1 Objective and contents	8-1
8.2 The components and elements of an SMS.....	8-1
8.3 The ICAO SMS framework	8-3
8.4 Management commitment and responsibility.....	8-3
8.5 Safety accountabilities	8-6
8.6 Appointment of key safety personnel.....	8-9
8.7 Coordination of emergency response planning	8-11
8.8 SMS documentation	8-12
8.9 SMS implementation plan.....	8-12
Appendix 1 to Chapter 8. Framework for safety management systems (SMS)	8-APP 1-1
Appendix 2 to Chapter 8. Sample job description for a safety manager.....	8-APP 2-1
Chapter 9. SMS OPERATION.....	9-1
9.1 Objective and contents	9-1
9.2 Safety risk management — General.....	9-1
9.3 Hazard identification	9-2
9.4 Risk assessment and mitigation	9-3
9.5 Safety assurance — General.....	9-3
9.6 Safety performance monitoring and measurement.....	9-4
9.7 Protection of sources of safety information.....	9-8
9.8 The management of change.....	9-11
9.9 Continuous improvement of the SMS	9-12
9.10 The relationship between safety risk management (SRM) and safety assurance (SA)	9-13
9.11 Safety promotion — Training and education.....	9-15
9.12 Safety promotion — Safety communication.....	9-16
Chapter 10. PHASED APPROACH TO SMS IMPLEMENTATION.....	10-1
10.1 Objective and contents	10-1
10.2 Why adopt a phased approach to SMS implementation.....	10-1
10.3 Phase I — Planning SMS implementation.....	10-2
10.4 Phase II — Reactive safety management processes	10-3
10.5 Phase III — Proactive and predictive safety management processes	10-3
10.6 Phase IV — Operational safety assurance	10-4
Appendix 1 to Chapter 10. Guidance on the development of a State's regulation on SMS.....	10-APP 1-1
Appendix 2 to Chapter 10. Guidance on the development of an SMS implementation plan for service providers	10-APP 2-1
Chapter 11. STATE SAFETY PROGRAMME.....	11-1
11.1 Objectives and contents	11-1
11.2 The components and elements of an SSP	11-1

	<i>Page</i>
11.3 The ICAO SSP framework.....	11-2
11.4 SSP development.....	11-3
11.5 SSP implementation.....	11-4
11.6 The role of the SSP in supporting SMS implementation.....	11-5
Appendix 1 to Chapter 11. Framework for the State safety programme (SSP).....	11-APP 1-1
Appendix 2 to Chapter. 11 Guidance on the development of a State safety policy statement.....	11-APP 2-1
Appendix 3 to Chapter 11. Guidance on the development of a State safety programme (SSP) gap analysis.....	11-APP 3-1
Appendix 4 to Chapter 11. Guidance on the development of a State's enforcement policy and enforcement procedures in an SMS environment.....	11-APP 4-1
Appendix 5 to Chapter 11. Guidance on the development of an SSP implementation plan.....	11-APP 5-1

Attachments:

A — ICAO accident/incident data reporting (ADREP) system.....	ATT A-1
B — Emergency response planning.....	ATT B-1
C — Related ICAO guidance material.....	ATT C-1

ACRONYMS AND ABBREVIATIONS

ADREP	Accident/incident data reporting (ICAO)
AEP	Aerodrome emergency plan
AIRPROX	Aircraft proximity
ALARP	As low as reasonably practicable
ALoS	Acceptable level of safety
AMJ	Advisory material joint
AMO	Approved maintenance organization
AOC	Air operator certificate
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)
CAA	Civil aviation authority
CDA	Constant descent arrivals
CEO	Chief executive officer
CFIT	Controlled flight into terrain
CIP	Commercially important person
Cir	Circular
CMC	Crisis management centre
CRDA	Converging runway display aid
CRM	Crew resource management
CVR	Cockpit voice recorder
DME	Distance measuring equipment
Doc	Document
ERP	Emergency response plan
FDA	Flight data analysis
FDM	Flight data monitoring
FDR	Flight data recorder
FOD	Foreign object (debris) damage
ft	Feet
GPS	Global positioning system
ILS	Instrument landing system
IMC	Instrument meteorological conditions
ISO	International Organization for Standardization
kg	Kilogram(s)

LOFT	Line-oriented flight training
LOSA	Line operations safety audit
m	Metre(s)
MDA	Minimum descent altitude
MEL	Minimum equipment list
MOR	Mandatory occurrence report
MRM	Maintenance resource management
NM	Nautical mile(s)
OJT	On-the-job training
PC	Personal computer
QA	Quality assurance
QC	Quality control
QMS	Quality management system
RVSM	Reduced vertical separation minimum
SA	Safety assurance
SAG	Safety action group
SARPs	Standards and Recommended Practices (ICAO)
SDCPS	Safety data collection and processing systems
SHEL	Software/Hardware/Environment/Liveware
SMM	Safety management manual
SMS	Safety management system(s)
SMSM	Safety management systems manual
SOPs	Standard operating procedures
SRB	Safety review board
SRM	Safety risk management
SSP	State safety programme
TLH	Top level hazard
TRM	Team resource management
USOAP	Universal Safety Oversight Audit Programme (ICAO)
VIP	Very important person
VMC	Visual meteorological conditions
VOR	Very high frequency omnidirectional range

Chapter 1

OVERVIEW OF THE MANUAL

1.1 GENERAL

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 the International Standards and Recommended Practices (SARPs) contained in Annex 1 — *Personnel Licensing*, Annex 6 — *Operation of Aircraft*, Annex 8 — *Airworthiness of Aircraft*, Annex 11 — *Air Traffic Services*, Annex 13 — *Aircraft Accident and Incident Investigation* and Annex 14 — *Aerodromes*.

1.2 OBJECTIVES

The objective of this manual is to provide States with:

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

1.3 CONCEPT

The concept underlying this manual is that of a continuous loop (see Figure 1-1). The manual initially presents basic safety concepts, as the foundation upon which to understand the need for both an SMS and an SSP. The manual then discusses how these safety concepts are embodied in the ICAO SARPs contained in Annexes 1, 6, 8, 11, 13 and 14. The manual thereafter outlines a principled approach to the implementation of an SMS by service providers and the progressive implementation and maintenance of an SSP, with emphasis on the role civil aviation authorities play in supporting SMS implementation by service providers.

1.4 CONTENTS

1.4.1 The manual include is comprised of eleven chapters, as follows:

- a) Chapter 1 — Overview of the manual;
- b) Chapter 2 — Basic safety concepts;

- c) Chapter 3 – Introduction to safety management;
- d) Chapter 4 — Hazards;
- e) Chapter 5 — Safety risks;
- f) Chapter 6 — ICAO safety management requirements;
- g) Chapter 7 — Introduction to safety management systems (SMS);
- h) Chapter 8 — SMS planning;
- i) Chapter 9 — SMS operation;
- j) Chapter 10 — Phased approach to SMS implementation; and
- k) Chapter 11 — State safety programme (SSP).

1.4.2 The manual also contains several appendices with practical examples and information directly linked to the implementation and maintenance of an SMS and an SSP. These 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 containing useful information 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”.

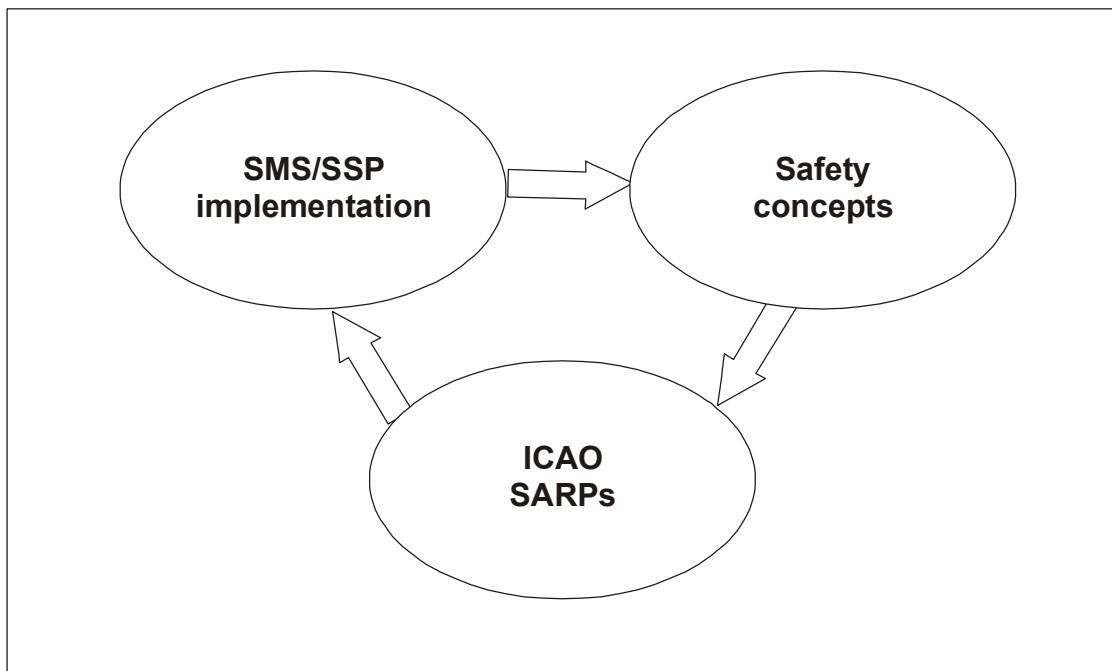


Figure 1-1. Continuous-loop concept used in this manual

1.5 STRUCTURE

1.5.1 The manual follows a building-block approach. Chapter 2 sets the foundation, by discussing contemporary safety concepts. Chapter 3 introduces the basics of safety management, with 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 through 11 present a principled approach to the design, implementation and maintenance of safety management processes using the SSP and SMS as the systems to manage safety within States and organizations, respectively. These chapters also introduce the notion of safety management as a systematic activity.

1.5.2 Chapter 11 on the State safety programme is provided as interim guidance material while experience is accrued by ICAO and States on the development and implementation of an SSP, at which point a manual dedicated to the State safety programme will be developed. Further detailed guidance on the development and implementation of an 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 This second edition of the ICAO *Safety Management Manual (SMM)* (Doc 9859) supersedes the first edition, published in 2006, in its entirety. It also supersedes the ICAO *Accident Prevention Manual* (Doc 9422), which is obsolete.

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 topics:

- a) The concept of safety;
- b) The evolution of safety thinking;
- c) Accident causation — The Reason model;
- d) The organizational accident;
- e) People, operational contexts and safety — The SHELL model;
- f) Errors and violations;
- g) Organizational culture; and
- h) 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 of employees of aviation organizations towards unsafe acts and conditions;
- d) error avoidance; and
- e) regulatory compliance.

2.2.2 Whatever the connotation, they all have one underlying commonality: the possibility of absolute control. Zero accidents, freedom from hazards, and so forth, convey the idea that it would be possible — by design or 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 absolute control

is certainly desirable, they 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 relative rather than absolute control. As long as safety risks and operational errors are kept under a reasonable degree of control, a system as open and dynamic 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. 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 loosely regulated activity characterized by underdeveloped technology; lack of a proper infrastructure; limited oversight; an insufficient understanding of the hazards underlying aviation operations; and production demands incommensurate with the means and resources actually available to meet such demands.

2.3.2 It is a given in systems safety theory that production systems that set ambitious production objectives without deploying the necessary means and resources to deliver them develop the potential for frequent breakdowns. Therefore, it is hardly surprising that the early days of commercial aviation were characterized by a high frequency of accidents, that the overriding priority of the early safety process was the prevention of accidents, and that accident investigation was the principal means of prevention. In those early days, accident investigation, hampered by the absence of other than basic technological support, was a daunting task.

2.3.3 Technological improvements (due in no small measure to accident investigation), together with the eventual development of an appropriate infrastructure, led to a gradual but steady decline in the frequency of accidents, as well as an ever-increasing regulatory drive. By the 1950s, aviation was becoming (in terms of accidents) one of the safest industries, but also one of the most heavily regulated.

2.3.4 This resulted in the still pervasive notion that safety can be guaranteed as long as rules are followed and that deviation from rules necessarily leads to safety breakdowns. Without denying the immense importance of regulatory compliance, its limitations as the mainstay of safety have increasingly been recognized, particularly as the complexity of aviation operations has increased. It is simply impossible to provide guidance on all conceivable operational scenarios in an operational system as open and dynamic as aviation.

2.3.5 Processes are driven by beliefs. Therefore, under the belief that regulatory compliance was the key to aviation safety, the early safety process was broadened to encompass regulatory compliance and oversight. This new safety process focused on outcomes (i.e. accidents and/or incidents of magnitude) and relied on accident investigation to determine the cause, including the possibility of technological failures. If technological failures were not evident, attention was turned to the possibility of rule-breaking by operational personnel.

2.3.6 The accident investigation would backtrack looking for a point or points in the chain of events where people directly involved in the safety breakdown did not do what they were expected to do, did something they were not expected to do, or a combination of both. In the absence of technological failures, investigations would look for unsafe acts by operational personnel, i.e. 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 safety breakdown, blame in different degrees and under different guises was the inevitable consequence, and 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 safety breakdown, almost exclusively. Little emphasis was placed on the hazardous conditions that, although present, were not “causal” in the occurrence under investigation, even though they held damaging potential for aviation operations under different circumstances.

2.3.8 While this perspective was quite effective in identifying “what” happened, “who” did it and “when” it happened, it was considerably less effective in disclosing “why” and “how” it happened (Figure 2-1). While at one time it was important to understand “what”, “who” and “when”, increasingly it became necessary to understand “why” and “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.

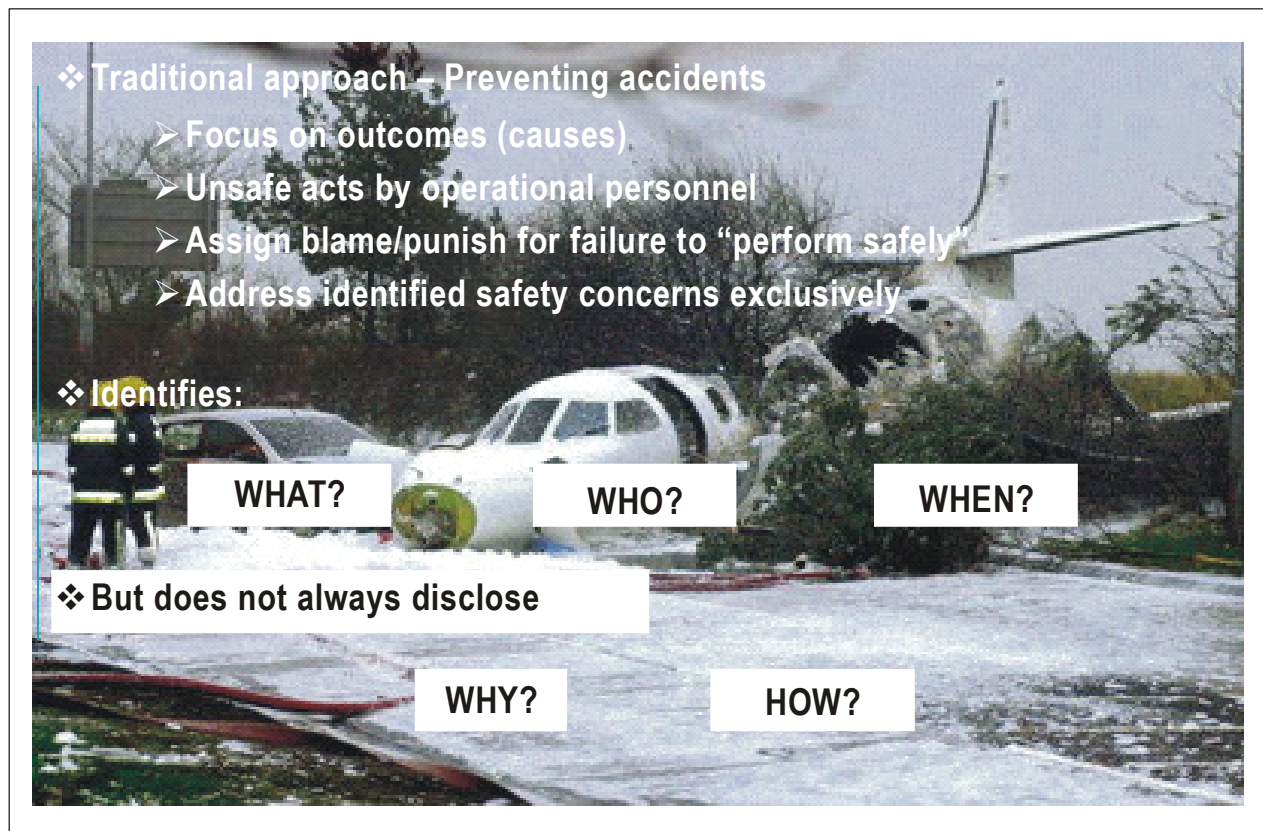


Figure 2-1. Traditional approach — Preventing accidents

2.3.9 The early days of aviation, those before and immediately following the Second World War until the 1970s, can be characterized as the “technical era” where safety concerns were mostly related to technical factors. Aviation was emerging as a mass transportation industry, yet the technology supporting its operations was not fully developed, and technological failures were the recurring factor in safety breakdowns. The focus of safety endeavours was rightly placed on the investigation and improvement of technical factors.

2.3.10 The early 1970s saw major technological advances with the introduction of jet engines, radar (both airborne and ground-based), autopilots, flight directors, improved navigation and communications capabilities and similar performance-enhancing technologies, both in the air and on the ground. This heralded the beginning of the “human era”, and the focus of safety endeavours shifted to human performance and Human Factors, with the emergence of crew resource management (CRM), line-oriented flight training (LOFT), human-centred automation and other human performance interventions. The mid-1970s to the mid-1990s 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, in spite of the massive investment of resources in error mitigation, by the mid-1990s human performance continued to be singled out as a recurring factor in safety breakdowns (Figure 2-2).

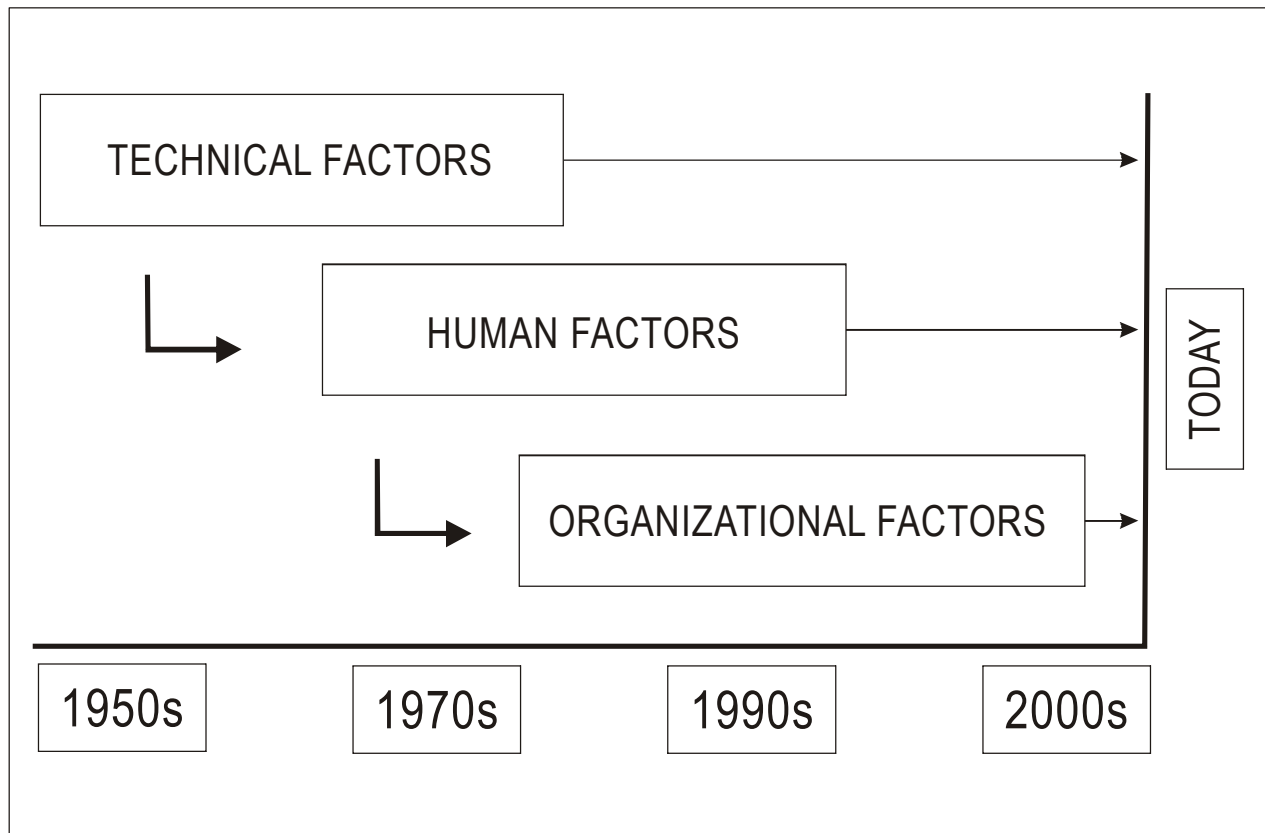


Figure 2-2. The evolution of safety thinking

2.3.11 The downside of Human Factors endeavours during a significant portion of the “golden era” was that 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 1990s that it was first acknowledged that individuals do not operate in a vacuum, but within defined operational contexts. Although scientific literature was available regarding how features of an operational context can influence human performance and shape events and outcomes, it was not until the 1990s that aviation acknowledged that fact. This signalled the beginning of the “organizational era” when safety began to be viewed from a systemic perspective, to encompass organizational, human and technical factors. It was also at that time that the notion of the organizational accident was embraced by aviation.

2.4 ACCIDENT CAUSATION — THE 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, which provided 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 in the aviation system. Equipment failures or operational errors are never the cause of breaches in safety defences, but rather the triggers. Breaches in safety defences are a delayed consequence of decisions made at the highest levels of the system, which remain dormant until their effects or damaging potential are 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 by the organization, regulatory authorities, etc. to protect the aviation system. 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- and violation-producing conditions in any operational context that may affect individual or team performance.

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, budgets, and politics. Since downsides in managerial decisions cannot always be prevented, steps must be taken to detect them and to reduce their adverse consequences.

2.4.6 Decisions by line management may result in inadequate training, scheduling conflicts 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 initial cost 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, 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 system's defences, they also contribute to the robustness of the system's defences

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).

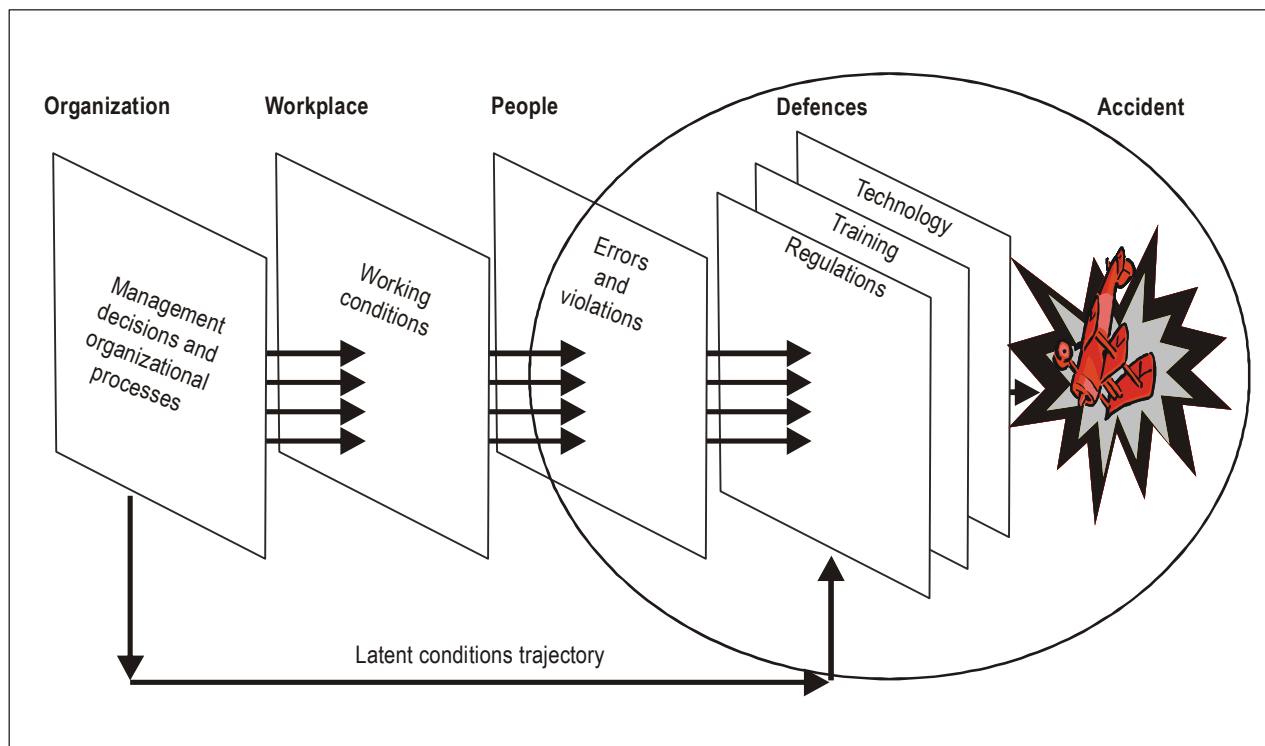


Figure 2-3. A concept of accident causation

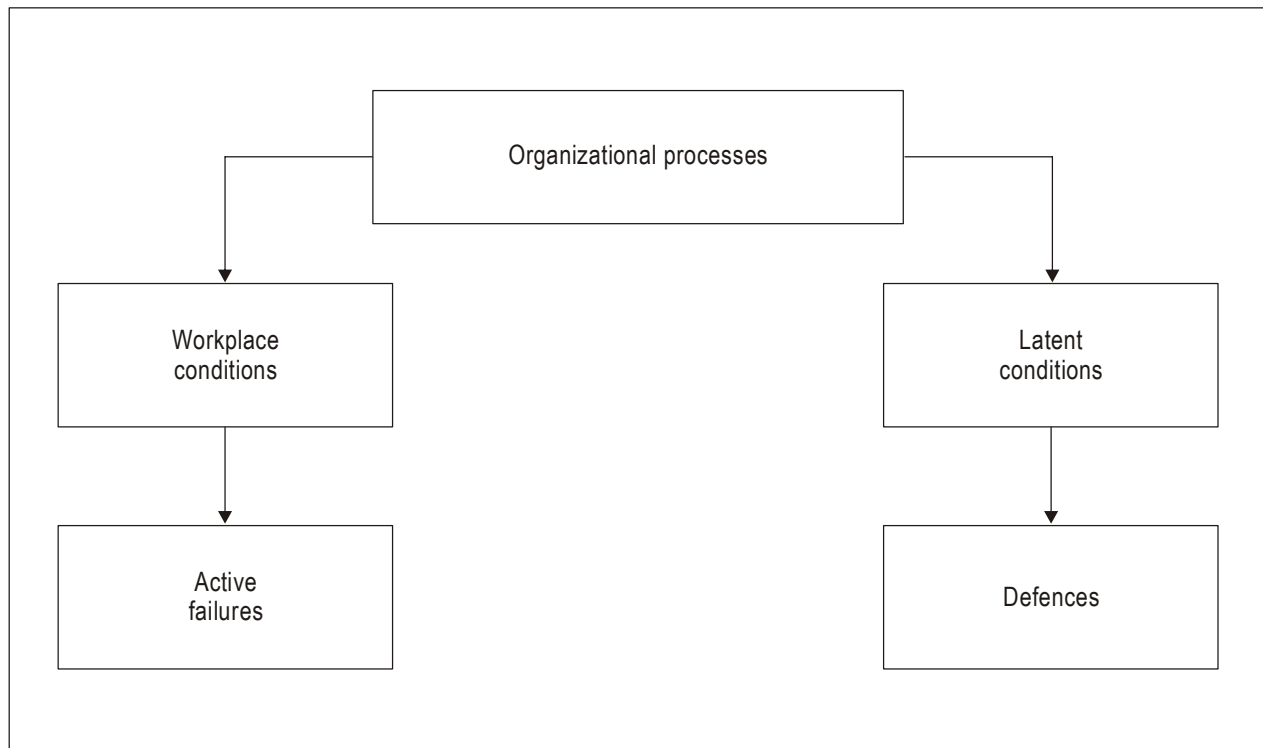


Figure 2-4. The organizational accident

2.5.2 The top block represents the organizational processes. These are activities over which any organization has a reasonable degree of direct control. Typical examples 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, and training deficiencies. 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 in 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: workforce stability, qualifications and experience, morale, management credibility, and traditional ergonomics factors such as lighting, heating and cooling.

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 processes 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).

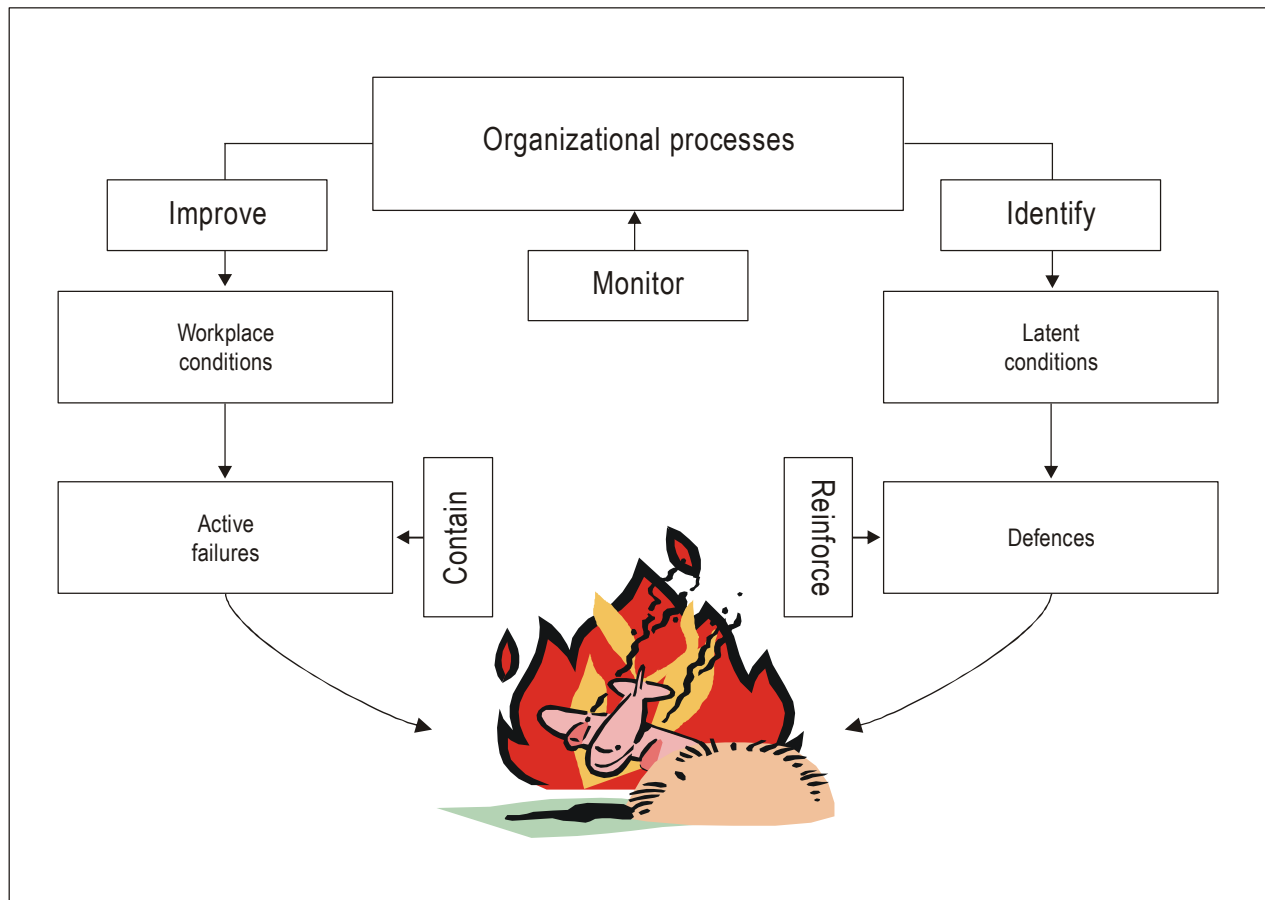


Figure 2-5. The perspective of the organizational accident

2.6 PEOPLE, CONTEXT AND SAFETY — THE SHEL 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 the 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.



Figure 2-6. People and safety

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 rain gear is also a source of 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.

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 line.

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 straight line, but rather a zigzagging path. As a consequence, delays in delivery take place, and also incidents occur (Figure 2-7B).

2.6.9 At this point, system managers have two options. One option is to follow the traditional perspective discussed in 2.3.6 — produce hollow reminders to runners to do what they know and have been trained to do 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 a 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 a 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.

2.6.11 Figure 2-8 also illustrates a scenario where the two managerial options discussed in 2.3.6 might apply. Following the traditional approach would lead to reminders about being careful when leaning (or not to lean) on windowsills and the dangers of pushing flowerpots out of the window, the re-writing of procedures to the previous effects, or 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 containment net under the window, broadening the windowsill, using flowerpots of the frangible type, re-routing traffic under the window or, in extreme circumstances, fencing off the window. The bottom line is that by removing or modifying the error-inducing features of the operational context, an exponential reduction in the probability and severity of the consequences of operational errors is achieved.

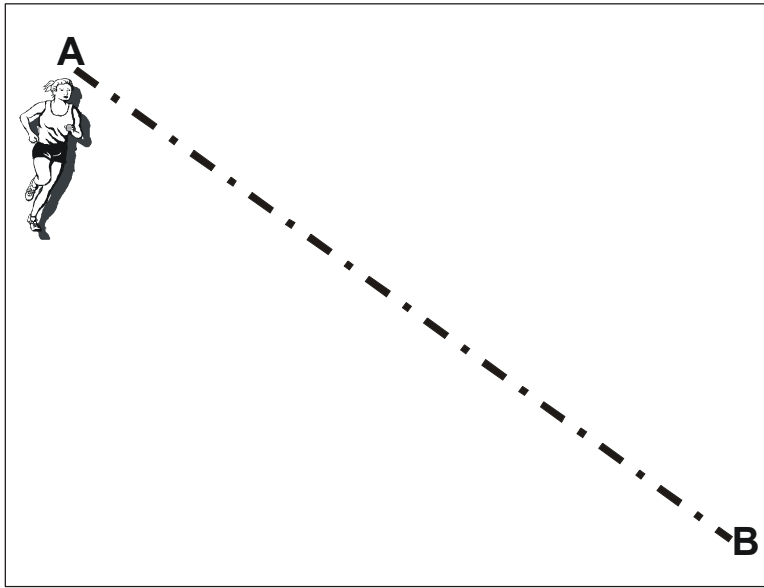


Figure 2-7A. Understanding human performance

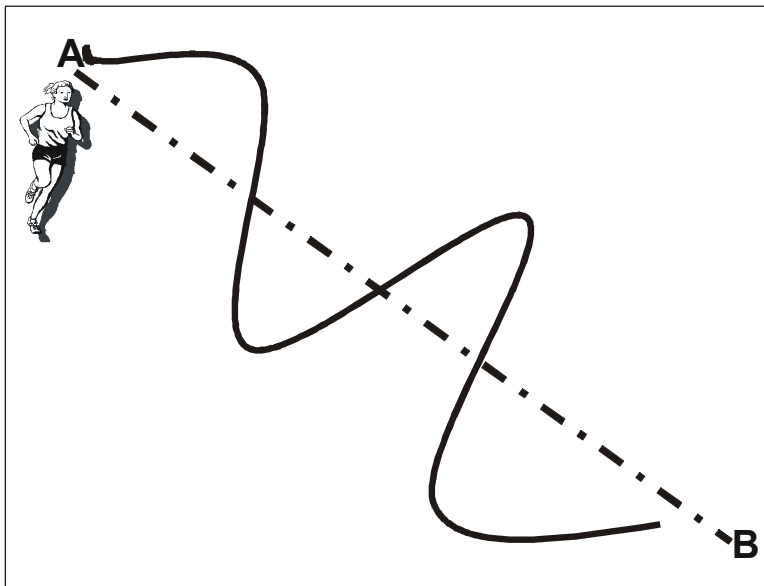


Figure 2-7B. Understanding human performance

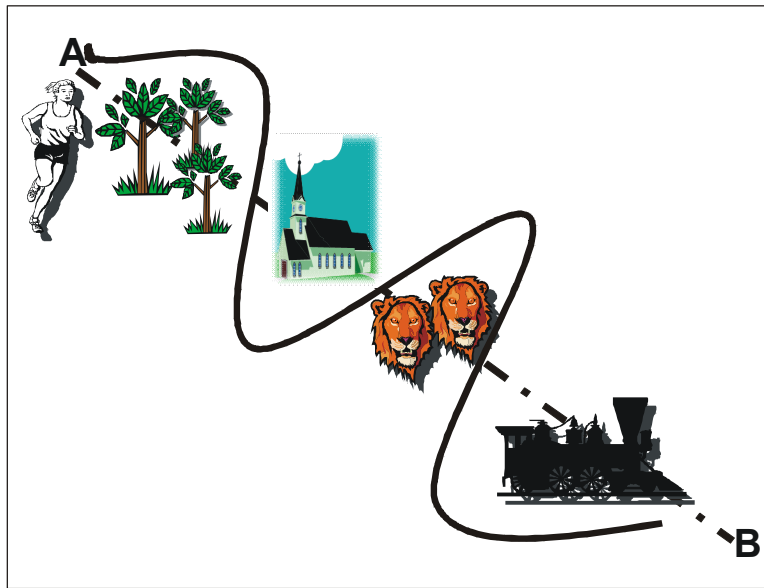


Figure 2-7C. Understanding human performance

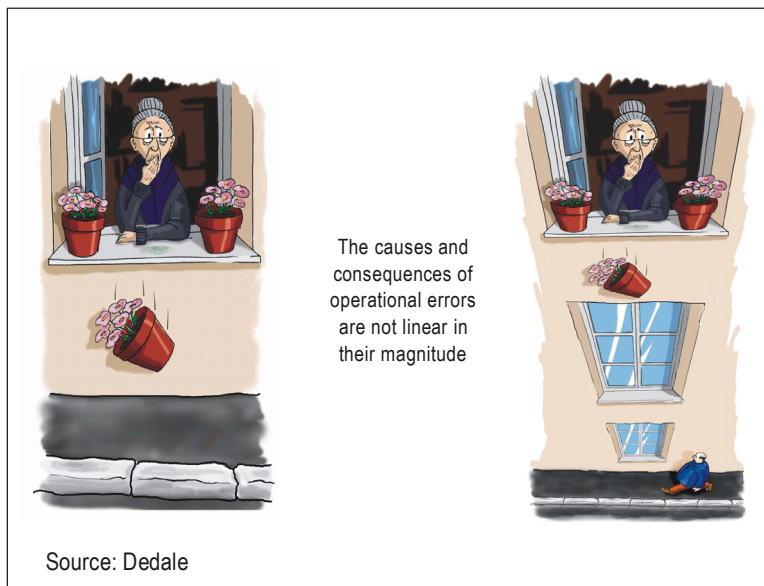


Figure 2-8. Processes and outcomes

2.6.12 A simple, yet visually powerful, conceptual tool for the analysis of the components and features of operational contexts and their 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.

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.

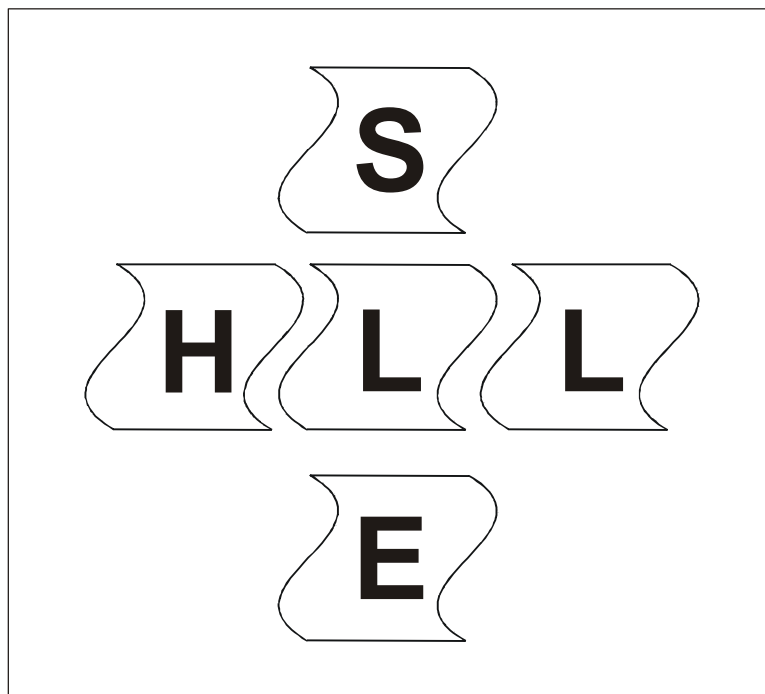


Figure 2-9. The SHEL model

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:

- a) **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.
- b) **Liveware-Software (L-S).** The L-S interface is the relationship between the human and the supporting systems found in the workplace, e.g. 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.
- c) **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.
- d) **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 twenty-four hour a day, seven days a week, 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:

- a) The designer can ensure the performance reliability of the equipment under specified operating conditions.
- b) During the certification process, the regulatory authority can define realistic conditions under which the equipment may be used.
- c) The organization’s management can develop standard operations procedures (SOPs) and provide initial and recurrent training for the safe use of the equipment.
- d) 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 increased demand 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 demand for the increase in the delivery of services, while maintaining existing margins of safety.

2.7.2 Technology is thus introduced on a massive scale in an effort to satisfy production demands. One result of this mass introduction of technology aimed at improved service delivery is that the Liveware-Hardware interface of the SHELL model is overlooked, or not always considered to the extent that it should. As a consequence, technology that is not sufficiently developed may be introduced prematurely, leading to unexpected failures.

2.7.3 While the introduction of underdeveloped technology is an inevitable consequence of the needs of any mass production industry, its relevance to the management of safety cannot be disregarded. People on the front lines, 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 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 behaviour 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 and forgetfulness, and how they 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 operational errors 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 this 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 is 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 the aviation safety tradition to consider operational errors as a 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, 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 indicative of substandard 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 explaining operational errors.

2.7.8 Following the alternative perspective on operational errors discussed, by considering operational errors as an emerging property of human/technology systems, and by 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 in aviation operations, the scope for operational errors in aviation is enormous. Understanding how these mismatches can affect the average human 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 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 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 built-in defences of the aviation system, and their damaging potential is mitigated, thus preventing negative consequences. In other words, control of operational errors takes place on a daily basis through the effective performance of the aviation system defences.

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.

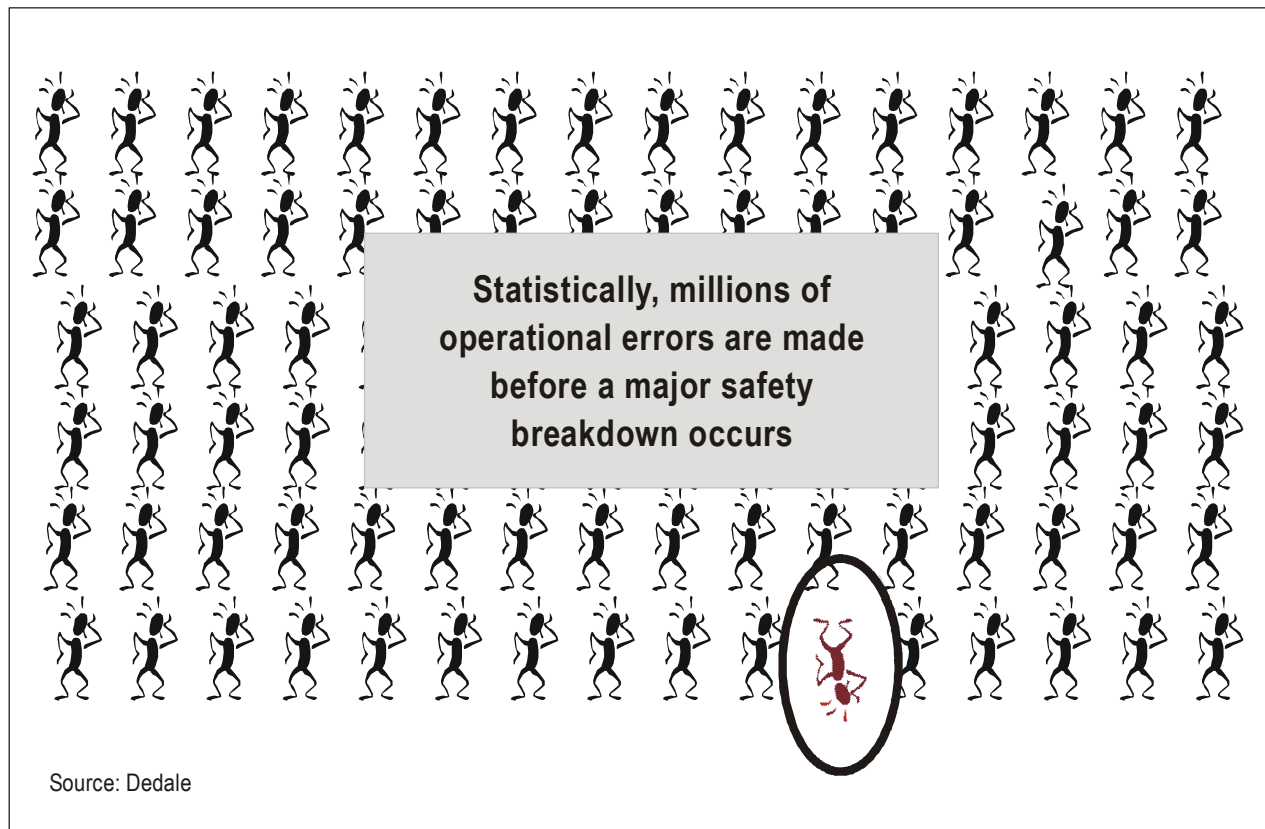


Figure 2-10. Operational errors and safety — A non-linear relationship

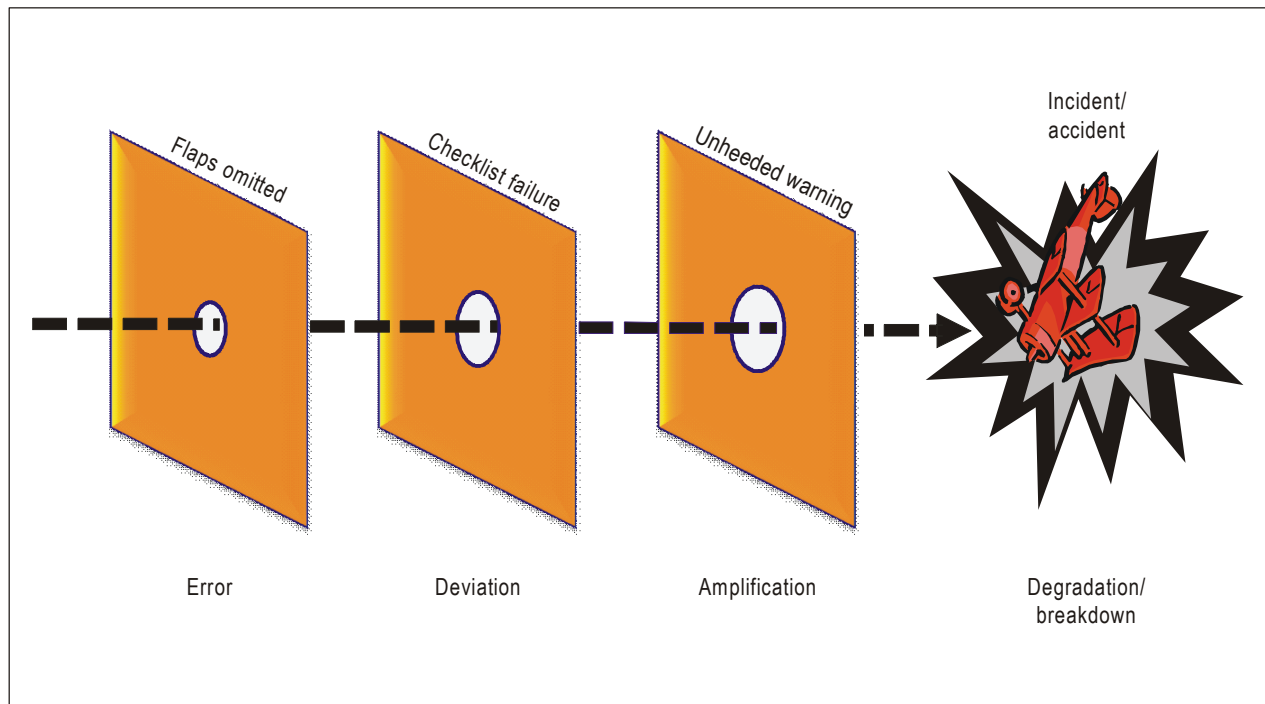


Figure 2-11A. Investigation of major breakdowns — Once in a million flights

2.7.13 The flight crew performs the after-engines-start checklist, but do not detect the incorrect flap setting, and the aircraft initiates taxiing for departure. A second opportunity is thus missed to recover from the consequences of the operational error, which continues to remain in the system, still harmless. Nevertheless, the system is now in a state of deviation or undesired state (i.e. aircraft taxiing for departure with an incorrect flap setting). The flight crew performs the taxiing checklist and the before take-off 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, or 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's 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 conceivably be 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 built-in system defences, 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.

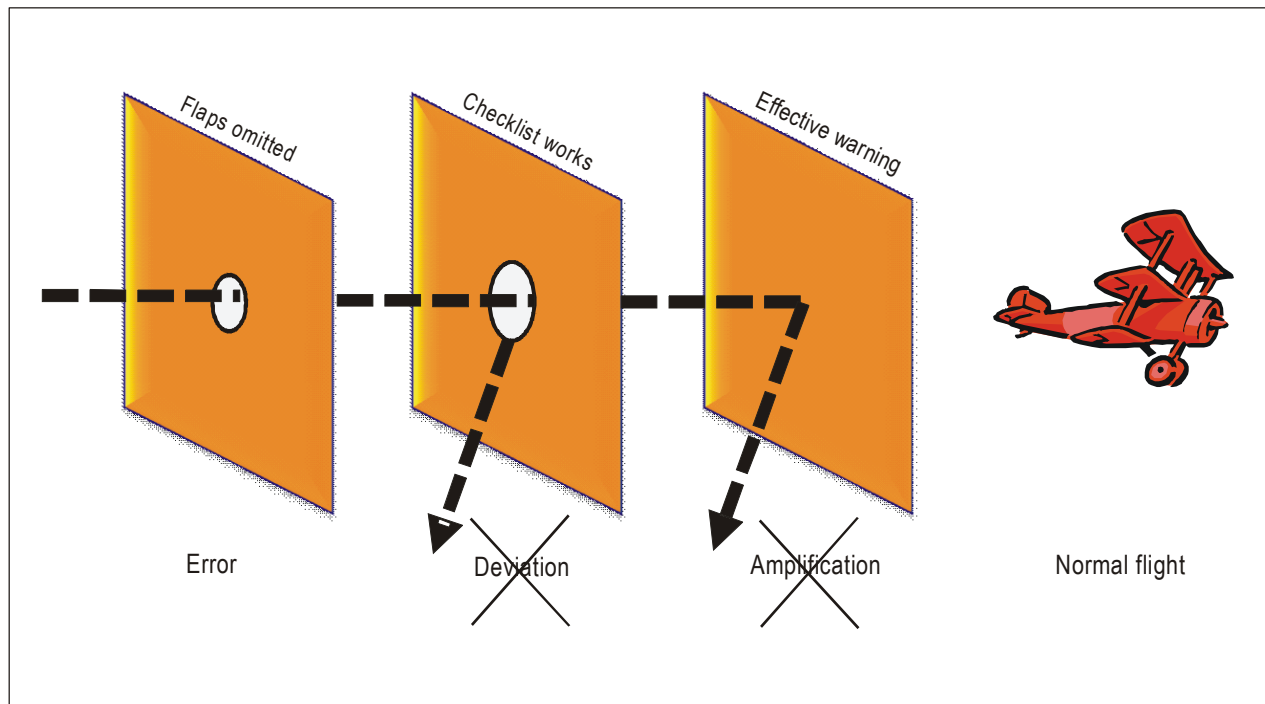


Figure 2-11B. Safety management — On almost every flight

2.7.16 The more built-in defences and layers of containment the system includes, and 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 2.7.12 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 as a 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 2.7.12 through 2.7.14 (Figure 2-11B). 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):

- a) the after start checklist;
- b) the taxiing checklist;
- c) the before-take-off checklist; and
- d) the take-off configuration warning.

2.7.19 There are other instances, not as obvious but 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 could 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 where operational errors induce catastrophic breakdowns are rare, while scenarios where operational errors induce 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 should have been triggered, but it can in all likelihood only describe 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 and how they were. These sources characterize 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 above are frequent, these alternative sources of safety information, if deployed, can provide a 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 that can be drawn from this second scenario is that safety resiliency is not so much a question of error-free operational performance, but rather a question of effective operational error management.

Three strategies to control operational errors

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 **Reduction strategies** intervene directly at the source of the operational error by reducing or eliminating the factors contributing 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, and reducing environmental distractions, i.e.:

- a) human-centred design;
- b) ergonomic factors; and
- c) 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 do not directly serve to eliminate the error, i.e.:

- a) checklists;
- b) task cards; and
- c) flight strips.

2.7.25 **Tolerance strategies** refer to the ability of a system to accept an operational error without serious consequences. An 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, i.e.:

- a) system redundancies; and
- b) structural inspections.

2.7.26 Operational error management must not be limited to front-line personnel. The performance of front-line personnel is, as depicted by the SHELL model, influenced by organizational, regulatory and environmental factors. For example, organizational processes, such as inadequate communication, ambiguous procedures, unreasonable scheduling, insufficient resources and unrealistic budgeting 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 versus violations

2.7.27 Thus far, the discussion in this section has focused on operational errors, which have been characterized 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 between, and understanding of, operational errors and violations are essential for 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 errors, they fail to achieve their expectations. People committing violations, on the other hand, know that they are engaging in behaviour that involves 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 workarounds 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 knowing 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 business” within a work group. They occur when the work group has difficulty following established 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 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 “optimizing” devices, since they aim at saving time and effort by simplifying a task (even if it involves cutting corners).

2.7.33 A third type of violation, which is often overlooked, is **organization-induced violations**, which can be viewed as an extension of routine violations. The full potential of the safety message that violations can convey can be

understood only when considered against the demands imposed by the organization regarding the delivery of the services for which the organization was created. 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 risks.

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 the highest safety risks is undesirable, not only from a safety standpoint but also from a financial standpoint. Thus, organizations weight 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 defines 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 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 the tools (technology) necessary to safely and effectively achieve service delivery; how to foster the behaviour the workforce must exhibit to safely and efficiently use the tools (training), and the set of norms and procedures that dictate workforce performance (regulations).

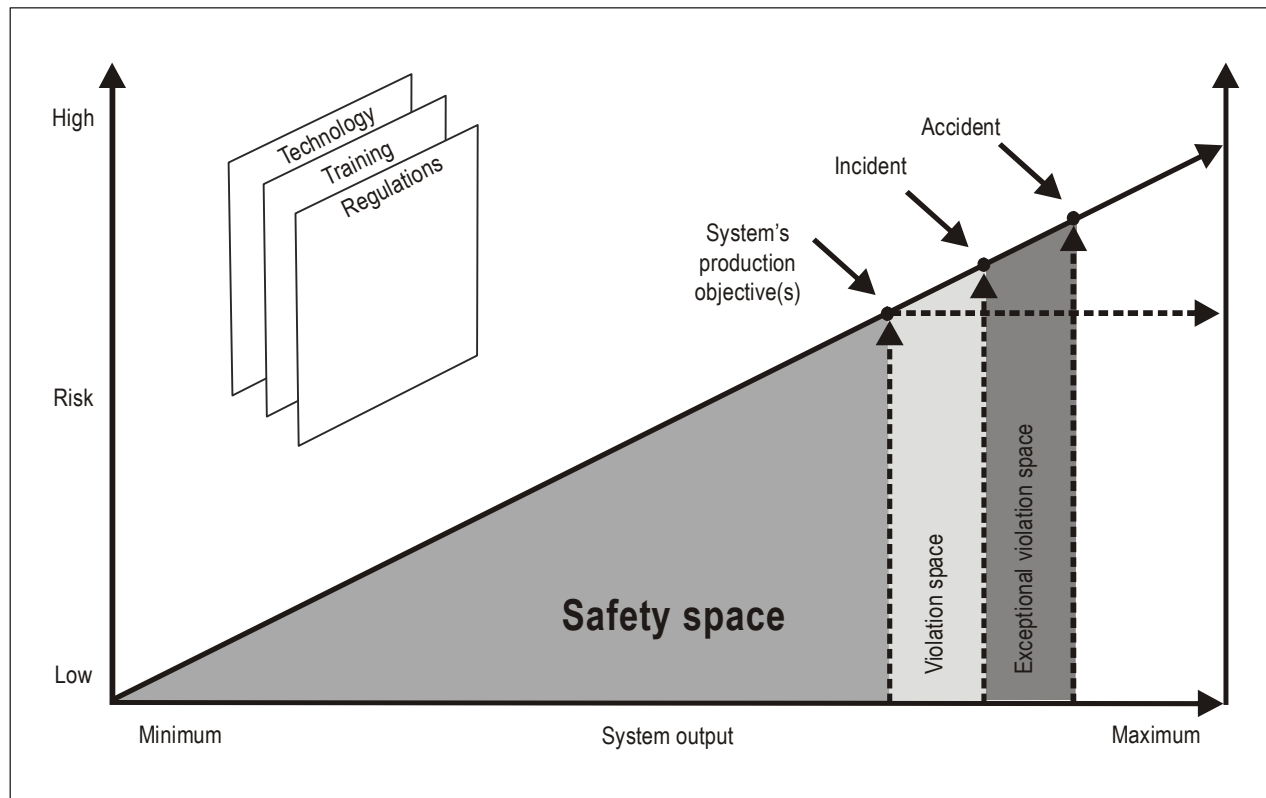


Figure 2-12. Understanding violations

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 afforded by that safety space is that the defences erected by the organization are commensurate with the planned system output, which in turn is commensurate with the tolerable safety risk. In other words, the resources allocated by the organization to protect are appropriate to and commensurate with 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 level of 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, aviation organizations may occasionally face transient, short-term demands for increased output (i.e. increased delivery of services) for brief periods of time, for example, seasonal variations in seat demands, specific circumstances such as a worldwide sporting event, and so forth. In order to maintain the safety zone intact, the organization should review and rearrange 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. Too often, as the aftermath of safety breakdowns show, aviation 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; “optimizing” 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 the same resources, operational personnel must deviate from established processes by resorting to short cuts or workarounds sanctioned by the organization. Operational personnel do not elect to engage in such short cuts or workarounds, the organization does. 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 behaviour 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 conduct 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 — about differences, not judgement. 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 minimizing 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:

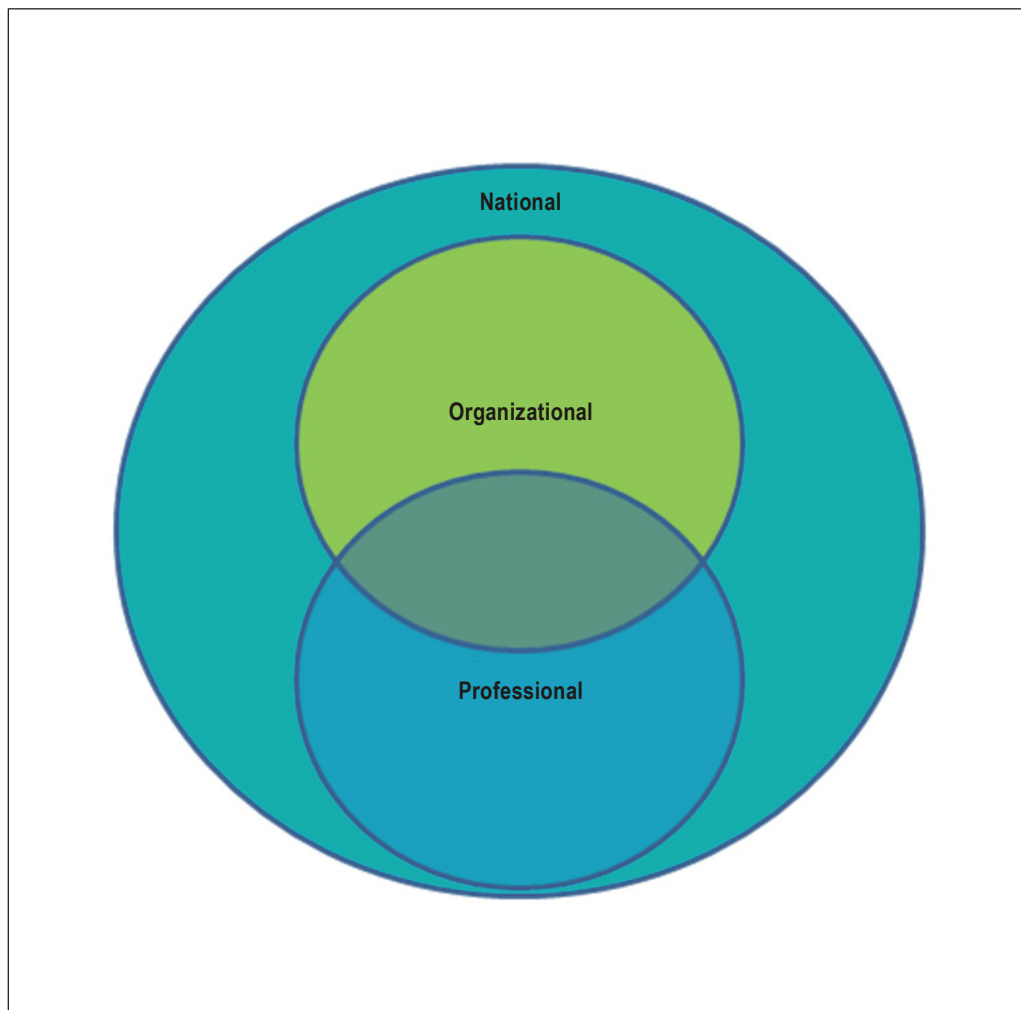


Figure 2-13. Three distinct cultures

- 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 a 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.
- c) **Organizational culture** differentiates the characteristics and value systems of particular organizations (the behaviour of members of one company versus that of another company, or government versus 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 versus civilian experience, bush or commuter operations versus development within a large carrier). They may also come from different organizational cultures due to corporate mergers or layoffs.

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 possesses 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 safety risk tolerance, enforce strict SOP compliance, tolerate breeches of SOPs or promote open two-way communications? Thus, the organization is a major determinant of the behaviour 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 behaviour;
- 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 a generative organizational culture 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 than will 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 feel responsible for and consider 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, whether by the board of directors, a driver on the ramp, or 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, and what works the way it is supposed to and 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 places 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 potential sources of damage;
- c) senior management defines the operational requirements needed to support active hazard reporting, ensures that key safety data are properly registered, demonstrates a receptive attitude to the reporting of hazards by operational personnel and implements measures to address the consequences of hazards;
- d) senior management ensures that key safety data are properly safeguarded and promotes a system of checks and balances so that reporters of hazards feel confident that hazard reporting will not be put to uses other than for which it was implemented (the management of safety);
- e) personnel are formally trained to recognize 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 hazardous 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 2.8.14:

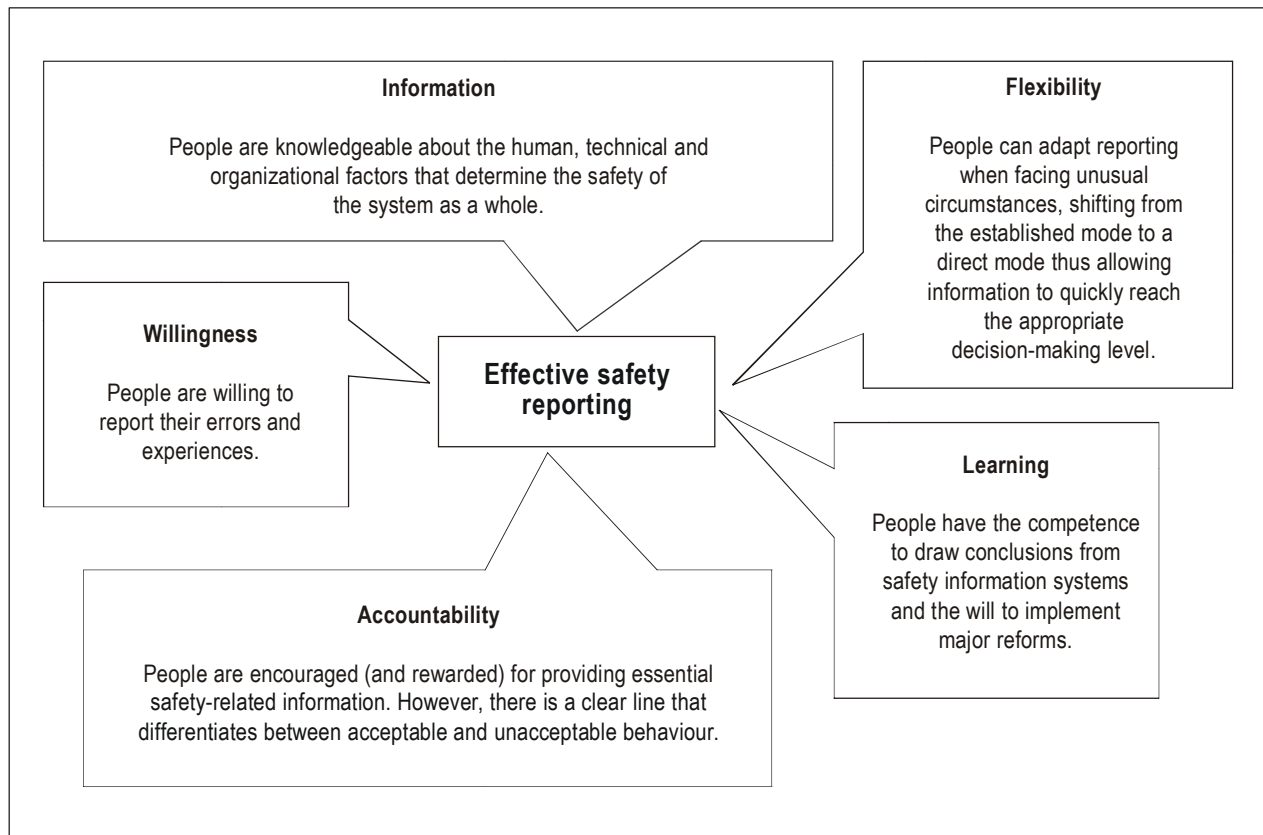


Figure 2-14. Effective safety reporting — Five basic traits

- 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 are 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 recognize 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 of key safety data being 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, data on hazards is turned into safety information. 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 the 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.

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; and
- c) generative — value the information.

2.8.18 Table 2-1 presents a matrix of key aspects of the management of safety information in terms of the three organizational characterizations discussed in 2.8.17.

	<i>Poor</i>	<i>Bureaucratic</i>	<i>Positive</i>
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
<i>Source: Ron Westrum</i>			

Table 2-1. Three possible organizational cultures

Effective safety reporting and culture

2.8.19 The voluntary reporting systems that were first developed in the late 1970s focused on the reporting of operational errors resulting from existing conditions or circumstances. Effective safety reporting, as described in this manual, goes further by also seeking out and identifying the causes of those operational errors so that they may be eliminated before they happen or mitigated. This has led to voluntary reporting systems that also include the reporting of hazards. As a general rule, it is the hazard that needs to be managed and it is more practical, easier and, to a large extent, more effective to make the operation safer than it is to make people safer. The systematic identification of hazards and other safety deficiencies may therefore pay a much higher dividend for safety management than error reporting alone. However, the difference between error and hazard reporting is fundamental and may lead to implementation issues that need to be acknowledged and addressed. A significant difference is that while hazard reporting is predictive and should be objective and neutral, error reporting is reactive and may incriminate the reporter or the reported, which may lead to blame and punishment.

2.8.20 Effective safety reporting relies upon voluntary error and hazard reporting by people. These people are mainly operational personnel who coexist with or encounter hazards. However because a hazard may also be more obvious to a person who is unfamiliar or unconnected with an operation (and the circumstances in which it is undertaken) there should not be any restriction on who may report and on what. Reporting should not be discouraged in any way; hence, the protection of reporters and sources of safety information was, and is, a key and often contentious issue in establishing both types of reporting systems, and could be a significant obstacle for the progress and success of safety management.

2.8.21 The attempts to protect safety information and the reporter from punishment were developed using the term *culture*, for example, “non-punishing culture”, “non-blame/blame-free culture” and lately “safety culture” or “just culture”. The word *culture* does have specific meanings and the context in which it is used in this case can lead to misperception and misunderstanding. Nevertheless, safety and just culture have become broadly accepted, although not universally defined, terms to describe the context in which safety practices are fostered within an organization. These safety practices include a series of organizational processes, procedures and policies that aim to achieve a specific outcome, the identification of hazards. The processes (effective safety reporting), procedures (hazard reporting system) and policies (safety policy, fair treatment of reporters, etc.) are complex, specific ideas and behaviours that can be packaged in such a way as to make them easily understandable to a wide audience and therefore easier to apply on a large scale. However, their substance and application will reflect the culture, in the true sense of the word, of the State or organization that develops them. Global adoption of a single, common safety or just culture could therefore be considered discriminatory, perhaps even judgemental, if the local culture is not the same.

2.8.22 The safety policy should actively encourage effective safety reporting and, by defining the line between acceptable performance (often unintended errors) and unacceptable performance (such as negligence, recklessness, violations or sabotage), provide fair protection to reporters. A safety or just culture may not however preclude the “criminalization of error”, which is legally, ethically and morally within the sovereign rights of any State, provided established international agreements are observed. A judicial investigation, and consequences of some form, may be expected following an accident or serious incident especially if a system failure resulted in lives lost or property damaged, even if no negligence or ill-intent existed. A potential issue could therefore exist if voluntary hazard reports, which relate to latent deficiencies of a system or its performance, are treated in the same way as those concerning accident and serious incident investigations. The intent of protecting hazard reports should not challenge the legitimacy of a judicial investigation or demand undue immunity. However, legal argument does usually take precedence over any technical or safety-related argument.

2.8.23 States and organizations should take into consideration the advantages and disadvantages of the adoption of safety and just culture, and any cultural and legal implications. For purposes related to the management of safety, the process that needs to be promoted, nurtured and defended is effective safety reporting; the “criminalization of error” is of lesser relevance. Effective safety reporting can be achieved in many different ways and following many different strategies. How it is achieved should be left to the preferences, possibilities and constraints of the specific operational contexts rather than proposing off-the-shelf solutions with the potential to clash with local culture.

2.9 SAFETY INVESTIGATION

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

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

- a) to put losses behind;
- b) to reassert trust and faith in the system;
- c) to resume normal activities; and
- d) 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:

- a) to learn about system vulnerability;
- b) to develop strategies for change; and
- c) 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 ice accretion, engines 2 and 3 incur a 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 communication and limited navigation capabilities.
- While attempting to conduct an emergency landing, battery power is depleted and 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 checklist to resolve the powerplant 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 of visual information on the emergency checklist was poor.
- There were issues regarding internal quality assurance procedures for flight operations.

2.9.7 ***Causes***

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

2.9.8 ***Safety recommendations***

- The authority should remind pilots to use correct phraseology.
- The authority should research the 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 into 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.
- 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, i.e. facilitating industry development versus 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.
- There were deficiencies in the State's training system.

2.9.11 Causes

- The flight crew's 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 safety culture.

2.9.12 Safety recommendations

- The report includes numerous front-line-oriented recommendations regarding flight crew performance.
 - The report also contains recommendations with regard to:
 - reviewing the process of granting an 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.
-

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.

3.1.2 The chapter includes the following topics:

- a) The safety stereotype;
- b) The management dilemma;
- c) The need for safety management;
- d) Strategies for safety management;
- e) The imperative of change;
- f) Safety management — Eight building blocks; and
- g) 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 do not hold ground when considered from the perspective that the management of safety is 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 aviation 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 how 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 and supervision, 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 and legal management.

3.2.5 The perspective advanced by this manual is that safety is not the first priority of aviation organizations. 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 as 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 a 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 characterized 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).

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. In 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 production objectives (albeit introducing numerous caveats to the contrary). Inevitably, as shown in Figure 3-1B, such partial organizational decision making leads to a catastrophe. It is simply a matter of time.

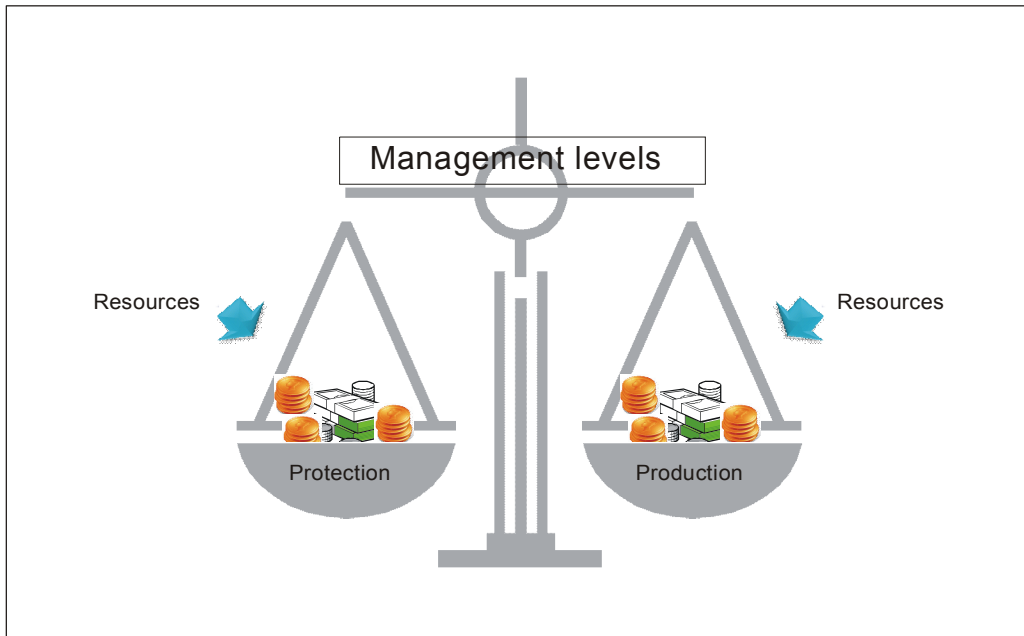


Figure 3-1A. The management dilemma

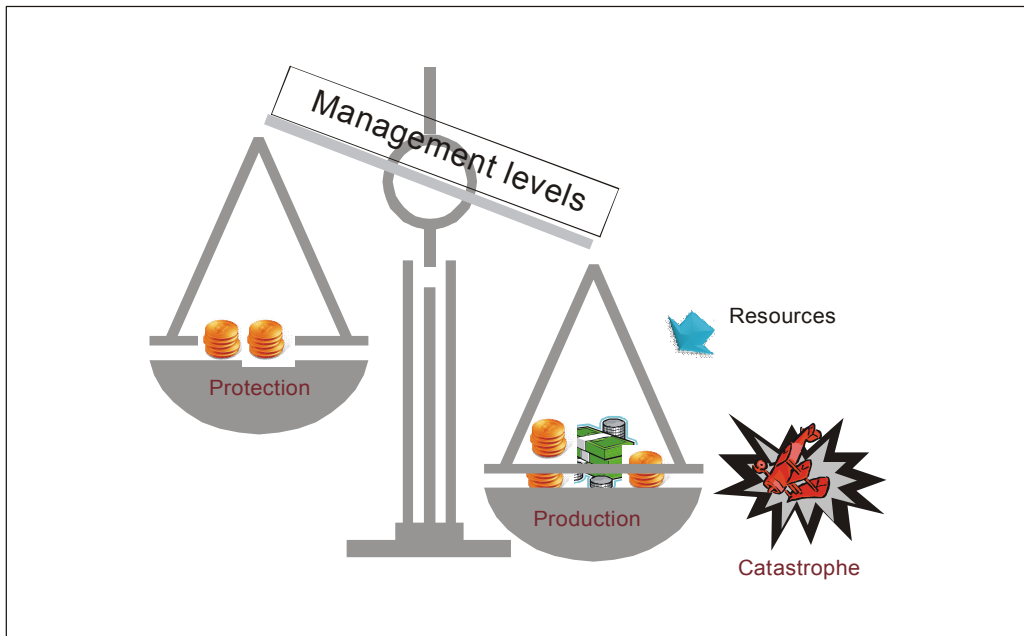


Figure 3-1B. The management dilemma

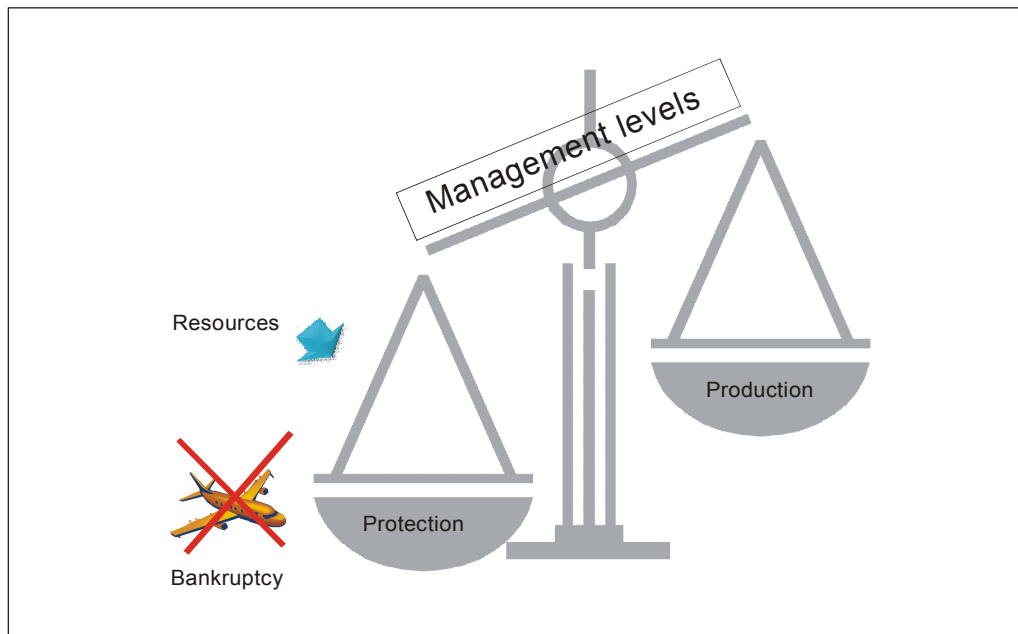


Figure 3-1C. The management dilemma

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 one to the importance of sensible organizational decision making regarding allocation of resources. In the final analysis, it is clear that the development of the “dilemma of the two Ps” is denied by an organizational perspective that focuses on safety management as a core business function, at the same level and with the same importance as other core business processes. In this way, safety management becomes part of the fabric of the organization, and an allocation of resources commensurate with the overall resources available to the organization is ensured.

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 a 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 to meet 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 had disappeared. This, however, is impractical, because it would destroy the viability of the aviation industry. Aviation operations must therefore be conducted under conditions that are dictated not so much by operational safety considerations but rather by service delivery considerations.

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 in, activities related to production or delivery of services.

This reinforces the need for safety management as a core business function that ensures an analysis of an organization's resources and goals and allows for a balanced and realistic allocation of resources between protection and production goals, which supports the overall service delivery needs of the organization.

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 an increase in accidents as a consequence of such growth. While accident reduction will always remain a priority of aviation, there are more compelling reasons than statistical projections underlying the transition to a safety management environment in international civil aviation worldwide.

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 whose histories span centuries. It is a tribute to the aviation safety community and its unrelenting endeavours that in a mere century aviation has progressed, from a 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) into 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 1960s (the technical era discussed in Chapter 2), aviation could be characterized 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 took it upon themselves to move 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 1970s until the mid-1990s (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 to the investigation of incidents. This shift to a broader perspective of safety and incident investigation was accompanied by a mass 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-1990s 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 further 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-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 above.

3.4.6 The application of business management practices to aviation safety, with its underlying routine collection and analysis of operational data, has as its objective the development of the safety space discussed in Chapter 2. Within that 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 a 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 an extension of that 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.

3.4.8 It will be recalled that organizational decision making leading to excess allocation of resources for protection can have an impact on the financial state 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, provide 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 daily collection and analysis of specific financial indicators: market trends, changes in prices of commodities and external resources required by the organization to deliver its services. In doing so, financial management not only defines the financial boundary of the safety space, but also re-adjusts its position constantly.

3.4.10 It will also be recalled that organizational decision making leading to excess allocation of resources for production can have an impact on the safety performance 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, which 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 aviation organizations, if any, 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 lack thereof) as an 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 of safety reliability discussed in 3.4.3 to 3.4.5 argues the need to develop additional, alternative means of safety data collection, beyond accident and incident reports. Up to the late 1970s, 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 were 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 significantly lesser consequence than those that trigger the accident and serious incident safety data capture process. The fact nevertheless remains that safety data from reporting programmes becomes available only after safety deficiencies trigger a low-consequence event.

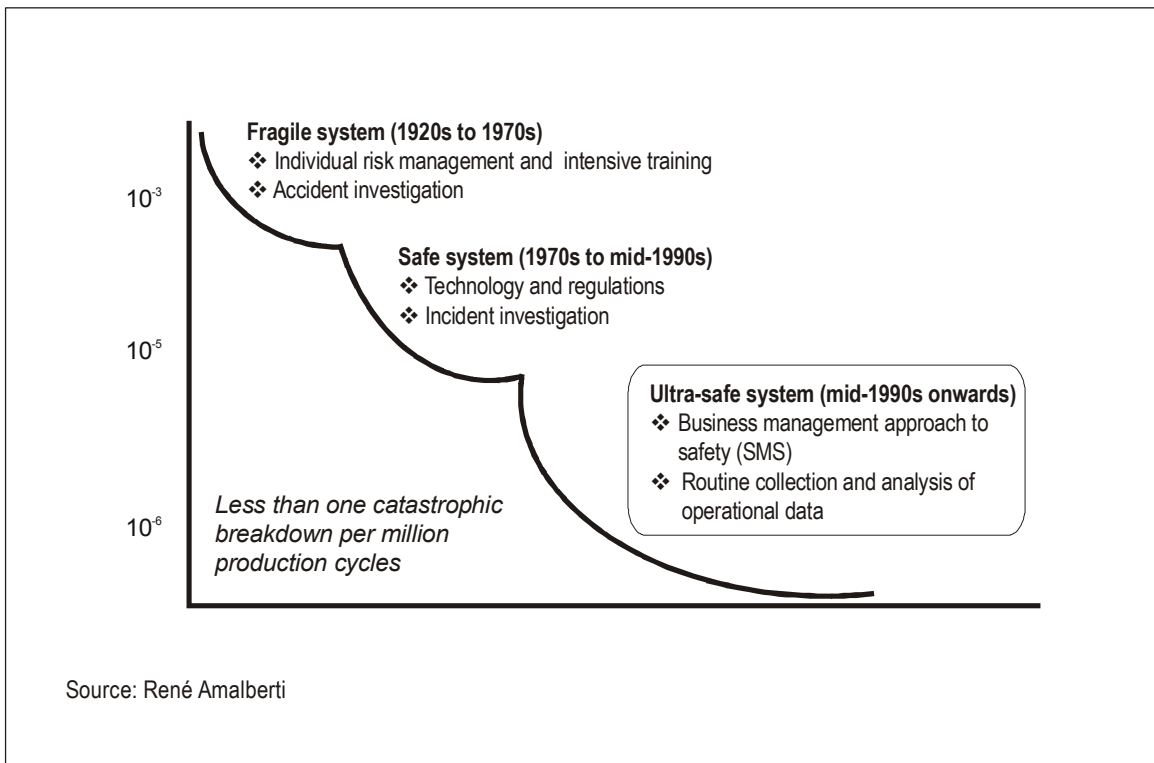


Figure 3-2. The first ultra-safe industrial system

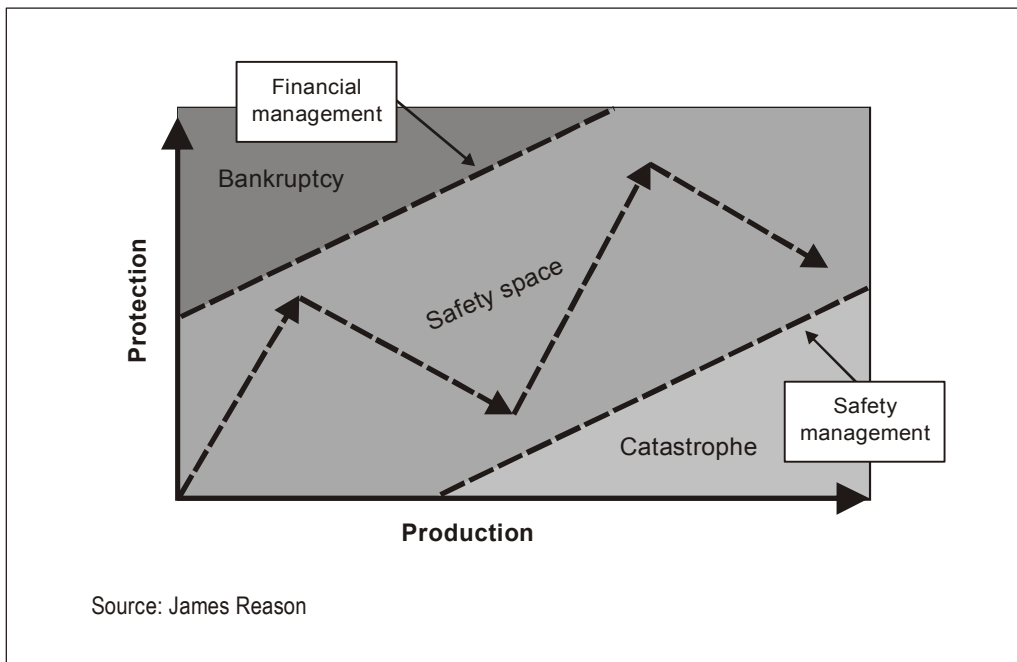


Figure 3-3. The safety space

3.4.15 By the early 1990s, 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 for 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 for 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 than because it is impossible to anticipate all possible operational interactions between people, technology and the context in which aviation operations take place. Monitoring normal operations on a real-time basis allows for the identification and correction of flaws and drawbacks that were not anticipated during system design. This argument is further advanced in 3.4.17 to 3.4.19.

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:

- a) what resources are necessary to achieve such production goals? and
- b) how can the system be protected from hazards during the operations necessary to achieve the production goals?

System designers utilize 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 those operational interactions.

3.4.18 The end result of the process is an initial system design based upon three basic assumptions: the technology needed to achieve the system production goals, the training necessary for people to properly operate the technology, and 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 time. 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 a consequence of real-life operations. Since the drift is a consequence of daily practice, it is referred to as a "practical drift".

3.4.20 A practical drift from baseline performance to operational performance is unavoidable in any system, no matter how careful and well thought out its design planning may 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 on 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 the 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 professionals), 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 Capturing what takes place within the practical drift through formal means (e.g. formally capturing collective domain expertise) holds considerable learning potential about successful safety adaptations and, therefore, for the control of safety risks. The formal capture of 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 the practical drift discussed in this paragraph.

3.5 STRATEGIES FOR SAFETY MANAGEMENT

3.5.1 The development of the practical drift is inevitable. All aviation organizations, even the soundest, 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 opposing "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".

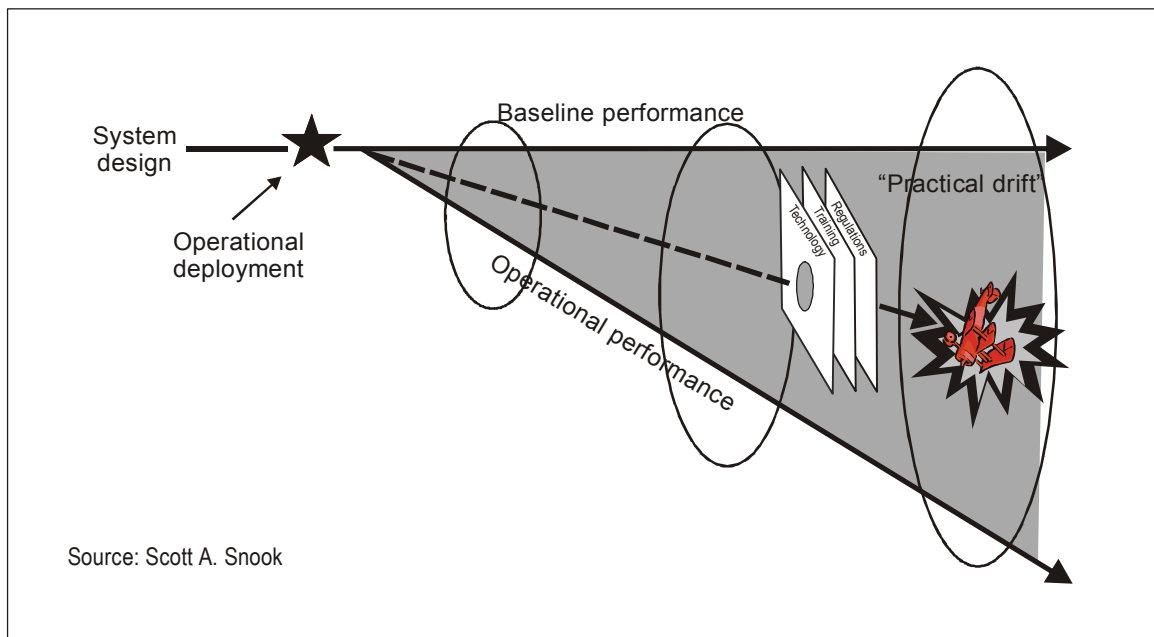


Figure 3-4. The practical drift

3.5.2 In order to successfully navigate the practical drift, organizations need navigation aids that generate the necessary information to negotiate currents and obstacles (see Figure 3-5). These navigation aids capture operational data that, once analysed, will inform organizations of the best passages through the currents and obstacles. There are a number of navigation aids available to aviation organizations, which 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** navigation aids require a very serious triggering event, with oftentimes considerable damaging consequences, to take place in order to launch the safety data capture process. Reactive navigation 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 navigation aids are an integral part of mature safety management. The contribution of reactive navigation 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 navigation aids.

3.5.4 **Proactive** navigation aids require a less serious triggering event, probably with little or no damaging consequences, to take place in order to launch the safety data capture process. Proactive navigation 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 navigation aids.

3.5.5 **Predictive** navigation aids do not require a triggering event to take place in order to launch the safety data capture process. Routine operational data are continually captured, in real time. Predictive navigation 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 that may be indicative of emerging safety risks from a variety of sources.

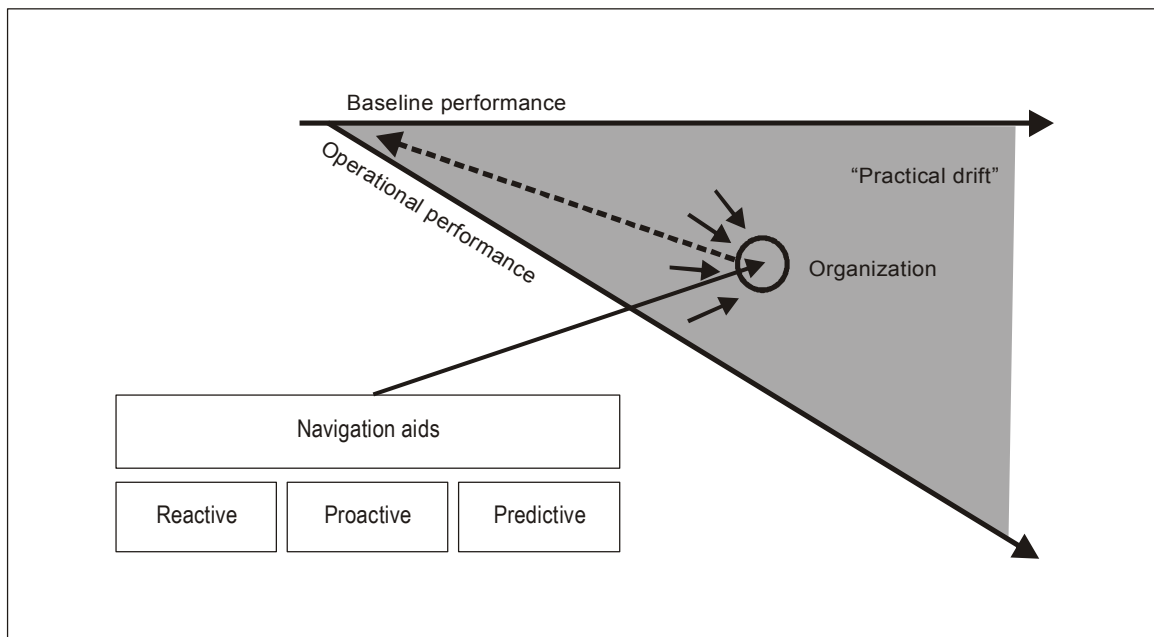


Figure 3-5. Navigating the practical drift

3.5.6 Predictive safety data collection systems are essentially statistical systems, whereby a considerable volume of operational data, which alone are largely meaningless, are 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 around obstacles and currents and position themselves optimally within the drift. Hazard reporting systems, flight data analysis and normal operations monitoring are examples of predictive navigation aids.

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.

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, one must return to the practical drift, as pictured in Figure 3-7. Hazards exist as a continuum along the practical drift. If uncontained, they travel down the drift with increasing 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 along the practical drift, the more they gather momentum and increase their damaging potential. 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.

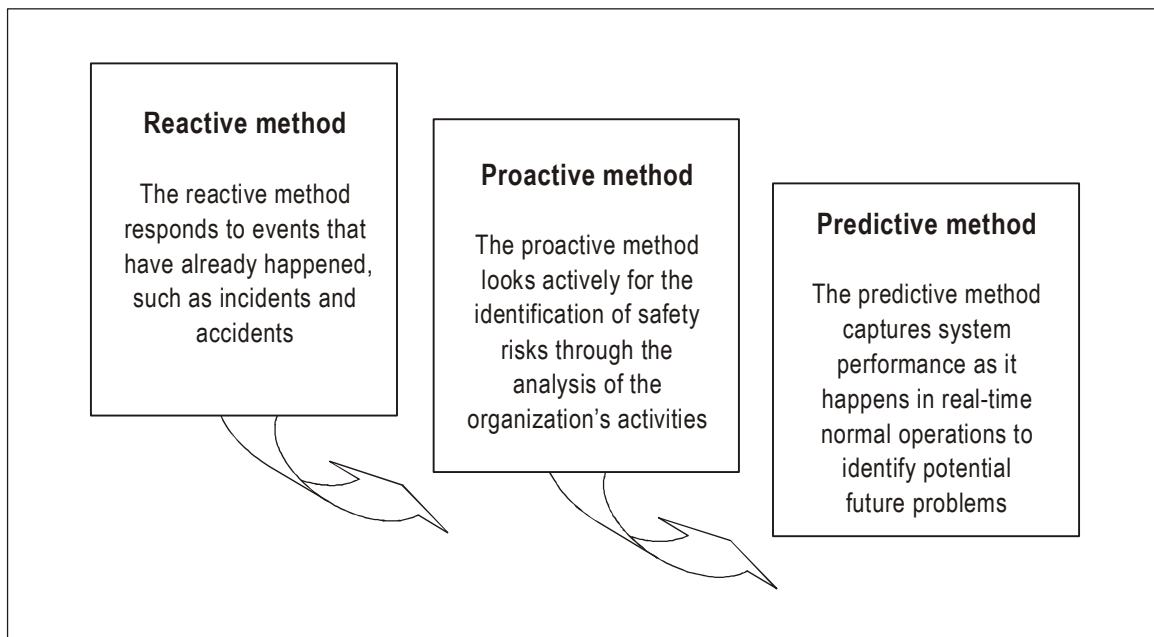


Figure 3-6. Safety management strategies

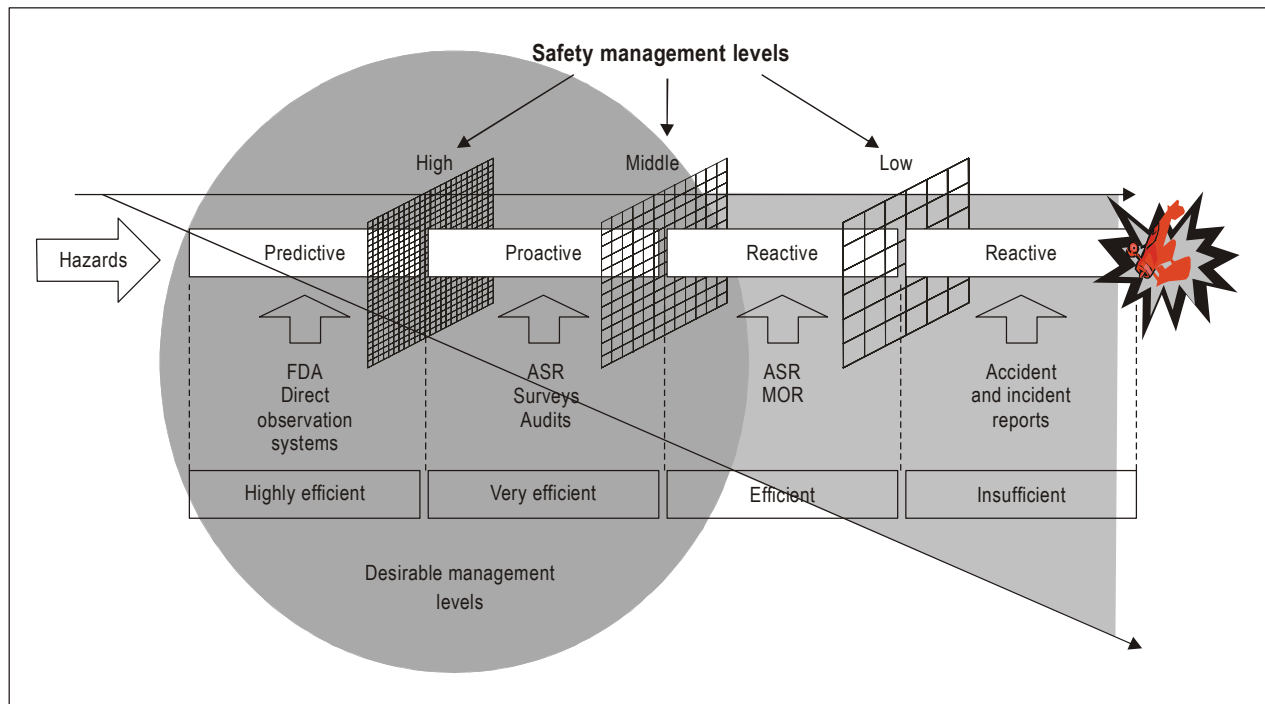


Figure 3-7. Strategies — Levels of intervention and tools

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 the one hand, they deal with hazards when they are in their infancy, 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 containment nets or filters of such tightness that they 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 of 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 the opportunity to start developing their damaging potential. Because of this, the mitigations developed from proactive safety data turn into containment nets or filters that, while tight, allow the 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 as 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 containment nets or filters with a loose texture, which can frequently be penetrated by hazards. At the lowest level of reactive safety data capture systems, strategies and methods, accidents and serious incident investigation operate in a damage repair mode. The information derived 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 continue to grow, deeply changed operational contexts with their new challenges make traditional methods of managing safety to an acceptable level less effective and efficient. Different, evolved methods of 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 the safety endeavours of the past.

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

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

3.6.3 A contrasting, contemporary safety paradigm is evolving, which 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:

- a) The aviation system does not perform most of the time as per design specifications (i.e. operational performance leads to the practical drift);
- b) Rather than relying on regulatory compliance exclusively, real-time performance of the system is constantly monitored (performance-based); and
- c) 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.

- a) **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.
- b) **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 allow 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.
- c) **Continuous monitoring** through systems that collect safety data on hazards during normal operations. 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 are collected and relegated to a drawer are as good as no data at all. Furthermore, it is essential to share the safety information and intelligence gleaned with those who operate the system daily for they are the ones who are in constant contact with the hazards, the consequences of which effective safety reporting aims to mitigate.

- d) **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.
- e) **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 sharing safety data must be maintained and, if at all possible, reinforced.
- f) **Integration of safety training for operational personnel.** Seldom do 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 is 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.
- g) **Effective implementation of standard operating procedures (SOPs)**, including the use of checklists and briefings. SOPs, checklists and briefings, whether on a flight deck, in an air traffic control room, in a maintenance shop or an aerodrome apron, are amongst the most effective safety devices operational personnel have 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, checklists and briefings should never be underestimated.
- h) **Continuous improvement of the overall level of safety.** Managing safety is not a one-day affair. It is an ongoing activity that can be successful only through continuous improvement.

3.7.2 The result 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:

- a) **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 behaviour the organization expects from operational personnel in day-to-day operations.
- b) **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.

- c) **Adoption of best industry practices.** The tradition of aviation regarding safety excellence has led to the continuous development of robust safety practices. Aviation has, in addition, a tradition regarding exchange of safety information through both institutional and informal channels. These two positive traits should be reinforced and practised to foster adoption of best industry practices.
- d) **Incorporation of 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 a need for a regulatory framework as the bedrock for safety management endeavours. In fact, sensible safety management can develop only from sensible regulations.

3.8.2 In summary, safety management:

- a) includes the entire operation;
 - b) focuses on processes, making a clear differentiation between processes and outcomes;
 - c) is data-driven;
 - d) involves constant monitoring;
 - e) is strictly documented;
 - f) aims at gradual improvement as opposed to dramatic change; and
 - g) is based on strategic planning as opposed to piecemeal initiatives.
-

Chapter 4

HAZARDS

4.1 OBJECTIVE AND CONTENTS

This chapter presents the fundamentals of hazard identification and analysis and includes the following topics:

- a) Hazards and consequences;
- b) First fundamental — Understanding hazards;
- c) Second fundamental — Hazard identification;
- d) Third fundamental — Hazard analysis; and
- e) 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 than forty years ago. The difference between traditional system safety and present-day safety management is that, because of its engineering roots, system safety focused mostly on the safety implications of technical aspects and components of the system under consideration, somewhat at 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 of 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 hazards into two components: the hazard itself, and its consequences. A 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 to cause 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 a 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 to cause 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 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 improving 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 crosswind. It is only then, when the hazard interfaces with the operations of the system (take-off or landing of an aeroplane) 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 aeroplane as a consequence of the crosswind). This example illustrates the discussion in 4.2.3: a hazard should not necessarily be considered as a “bad thing” or something with a negative connotation. Hazards are an integral part of operational contexts, and their consequences can be addressed through various mitigation strategies to contain the hazard’s damaging potential, which will be discussed later in this manual.

4.2.5 A consequence is defined as the potential outcome (or outcomes) of a hazard. The damaging potential of a hazard materializes 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 materialize 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 materialize 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 the potential for loss of 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 hazards (discussed in Chapter 5). The assessment of the safety risks of the consequences of hazards allows an organization to make an informed decision about 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 the safety risks will 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 happens, 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 stating and naming hazards allows one to identify the nature and damaging potential of the hazard, to correctly infer the sources or mechanisms of the hazard and, most importantly, to evaluate the outcomes (other than extreme outcomes) in terms of the magnitude of the potential loss, which is one of 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 a state of disrepair. This complicates the task of ground navigation by aerodrome users, both aircraft and ground vehicles. In this case, the correct naming of the hazard could be “unclear aerodrome signage” (i.e. a condition with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function). As a result of this hazard, many possible consequences are possible. 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 taxiing 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 into 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:

- a) severe weather or climatic events (e.g. hurricanes, winter storms, droughts, tornadoes, thunderstorms, lighting and wind shear);
- b) adverse weather conditions (e.g. icing, freezing precipitation, heavy rain, snow, winds and restrictions on visibility);
- c) geophysical events (e.g. earthquakes, volcanoes, tsunamis, floods and landslides);
- d) geographical conditions (e.g. adverse terrain or large bodies of water);
- e) environmental events (e.g. wildfires, wildlife activity, and insect or pest infestation); and/or
- f) 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:

- a) aircraft and aircraft components, systems, subsystems and related equipment;
- b) an organization’s facilities, tools and related equipment; and/or
- c) facilities, systems, subsystems 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:

- a) growth;
- b) recession; and
- c) cost of material or equipment.

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 of 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 resilience of equipment to errors and failures; and
- i) human performance, restricted to 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 are 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:

- a) flight data analysis;

- b) company voluntary reporting system;
- c) safety surveys;
- d) safety audits;
- e) normal operations monitoring schemes;
- f) trend analysis;
- g) feedback from training; and
- h) investigation and follow-up of incidents.

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

- a) accident reports;
- b) State mandatory occurrence reporting system;
- c) State voluntary reporting system;
- d) State oversight audits; and
- e) information exchange systems.

4.4.5 The fundamental point in this discussion is that no source or programme entirely replaces others, or 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 in aviation organizations should receive the appropriate safety management training, at a level commensurate with their responsibilities, so that everybody in the organization is prepared and able to identify and report hazards. From this perspective, hazard identification and reporting are 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 of 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 their operations. Nevertheless, hazard identification, regardless of implementation, complexity and size, must be a formal process, clearly described in the organization's 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 more in-depth and far-reaching hazard identification activities and include:

- a) any time the organization experiences an unexplained increase in safety-related events or regulatory infractions;
- b) any time major operational changes are foreseen, including changes to key personnel or other major equipment or systems; and
- c) 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:

- a) **First step.** Identify the generic hazard (also known as top level hazard, or TLH). Generic hazard, in the context of this manual, is 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.
- b) **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.
- c) **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 re-pave one of two crossing runways. The following three-step hazard analysis process would apply:

- a) **Step A.** State the generic hazard (hazard statement or TLH)
 - airport construction
- b) **Step B.** Identify specific hazards or components of the generic hazard
 - construction equipment
 - closed taxiways, etc.
- c) **Step C.** Link specific hazards to specific consequence(s)
 - aircraft colliding with construction equipment (construction equipment)
 - aircraft taking off into the wrong taxiway (closed taxiways), etc.

4.5.4 The runway construction example discussed in 4.5.3 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 of 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:

- a) 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
- b) 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.

4.6 FOURTH FUNDAMENTAL — DOCUMENTATION OF HAZARDS

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

- a) not thinking about operational conditions with the potential to unleash the damaging potential of hazards;
- b) not knowing about operational conditions with the potential to unleash the damaging potential of hazards;

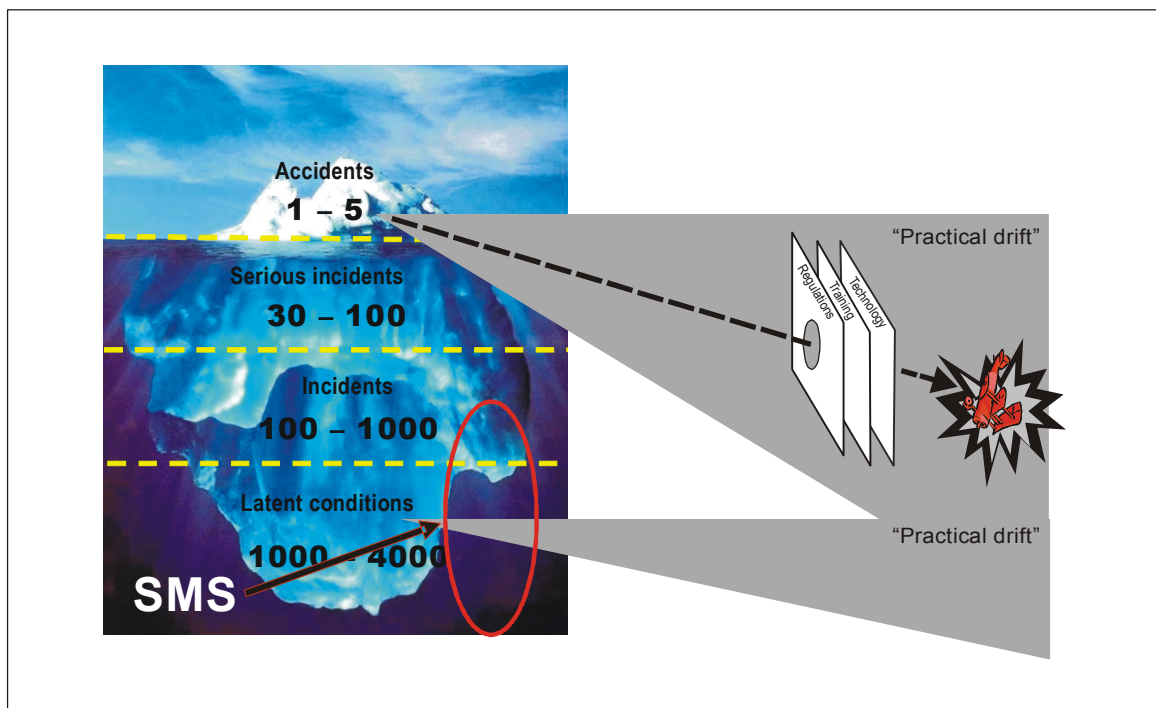


Figure 4-1. The focus of hazard identification

- c) unwillingness to consider or investigate operational conditions with the potential to unleash the damaging potential of hazards; and
- d) 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 be overcome only through knowledge. The formal documentation of hazards is therefore an essential requirement for hazard identification as well as a trait of mature safety management. Safety information (i.e. analysed raw data) and 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 opinions.

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 are facilitated by standardizing:

- a) definitions of terms used;
- b) understanding of terms used;
- c) validation of safety information collected;
- d) reporting (i.e. what the organization expects);
- e) measurement of safety information collected; and
- f) management of safety information collected.

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 consequence 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, seminars and the like).

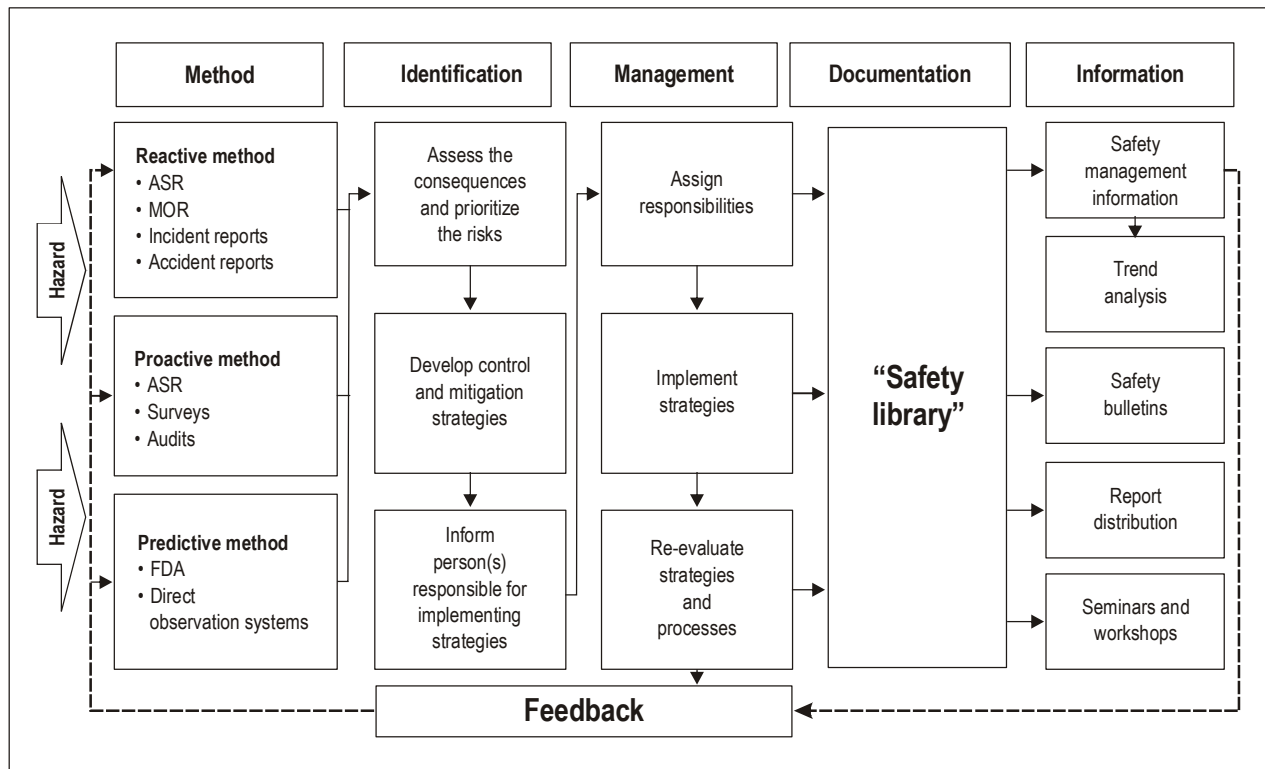


Figure 4-2. Documentation of hazards

Appendix 1 to Chapter 4

SAFETY INFORMATION ANALYSIS

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

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. 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

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.
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 one already believes to be true.

ANALYTICAL METHODS AND TOOLS

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:

- a) **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's safety management activities 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.

- b) **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.
- c) **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.
- d) **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.
- e) **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.
- f) **Cost-benefit analysis.** The acceptance of recommended safety risk control measures may be dependent on credible cost-benefit analyses. The cost 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

1. GENERAL

1.1 Quality safety data 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).

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.

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 of 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.

2. INFORMATION SYSTEM REQUIREMENTS

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.

3. UNDERSTANDING DATABASES

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 to be 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.

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).

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 makes and models 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.

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. 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.

5. DATABASE INTEGRITY

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.

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.

6. DATABASE MANAGEMENT

Protection of safety data

Given the potential for misuse of safety data that have 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.

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.

8. DATABASE SELECTION CONSIDERATIONS

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 are 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.** 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 are 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.** 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.

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

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

- a) Definition of safety risk;
- b) First fundamental — Safety risk management;
- c) Second fundamental — Safety risk probability;
- d) Third fundamental — Safety risk severity;
- e) Fourth fundamental — Safety risk tolerability;
- f) Fifth fundamental — Safety risk control/mitigation; and
- g) 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 an outcome and safety risk management as a 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 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 on the prevention of bad outcomes. However, under the notion of safety management, agreeing on the consequences of identified hazards and describing them in operational terms are not enough to engage in mitigation deployment. It is necessary to evaluate the seriousness of the 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. By “putting a number” on 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 a definition to the concepts of hazards and consequences 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 a 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 product of the human mind intended to measure the seriousness of, or “put a number” on, the consequences of hazards.

5.2.8 Safety risk is defined as the assessment, expressed in terms of predicted probability and severity, of the consequences of a hazard, taking as reference the worst foreseeable situation. Typically, safety risks are designated through an alphanumeric 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 one to link safety risks with hazards and consequences, thus closing the loop in the hazard-consequence-safety risk trilogy:

- a) a wind of 15 knots blowing directly across the runway is a hazard;
- b) the potential for a runway lateral excursion because a pilot might not be able to control the aircraft during take-off or landing is one of the consequences of the hazard; and
- c) the assessment of the consequences of a runway lateral excursion, expressed in terms of probability and severity as an alphanumeric 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 foundation for a balanced allocation of

resources between all assessed safety risks and those safety risks the control and mitigation of which are viable. In other words, safety risk management assists in resolving the “dilemma of the two Ps”. Safety risk management is therefore a 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 an 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, and an even fewer number will be assessed in such a way that the assessment falls straight in the acceptable region.

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 consequences of the hazards are of such a magnitude, and 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:

- a) allocate resources to reduce the exposure to, and/or the magnitude of, the damaging potential of the consequences of the hazards; or
- b) if mitigation is not possible, cancel the operation.

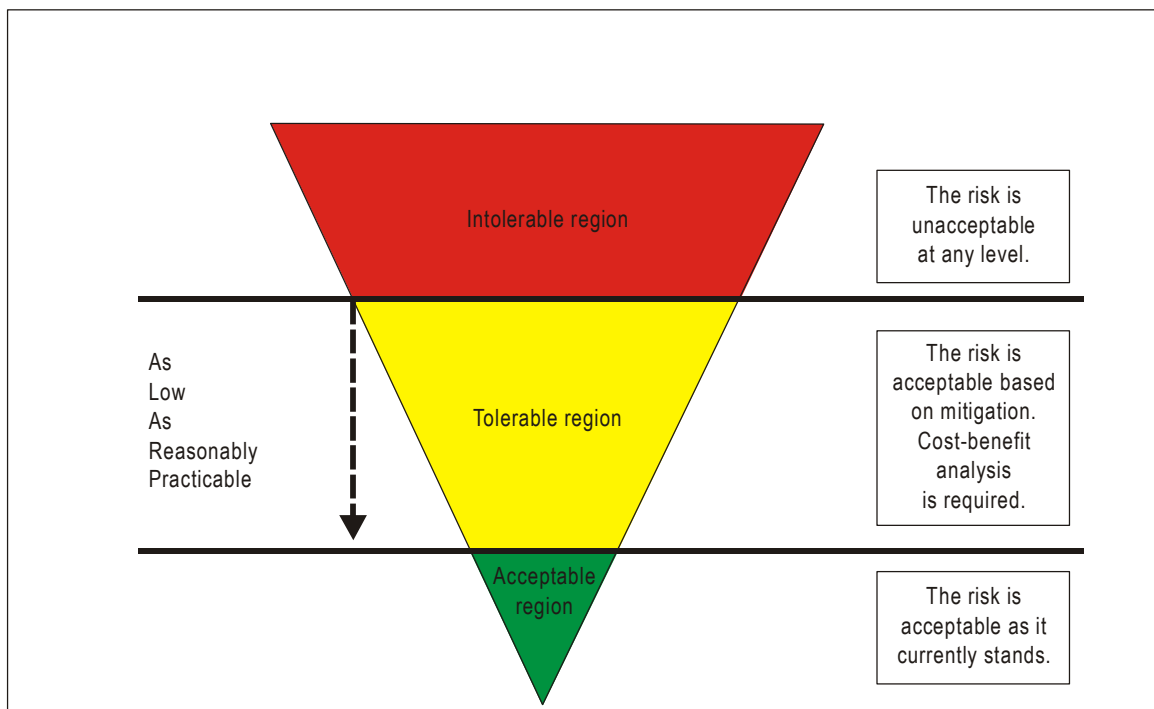


Figure 5-1. Safety risk management

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 consequences of hazards 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:

- a) Is there a return on the investment underlying the allocation of resources to bring the probability and/or severity of the consequences of hazards under organizational control? or
- b) 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 consequences of hazards 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 both to 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 cost. It should, however, be borne in mind that when an organization “accepts” a safety risk, this does not mean that the safety risk has been 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 consequences of hazards 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, 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 consequences of hazards under organizational control; it only transfers the monetary risk from the organization to the insurer. The safety risk 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, with the organization incurring the cost 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 cost of the involvement of their staff in the investigation, as well as the cost 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 and possibly shut down unsafe operations.

5.3.10 Cost-benefit analyses produce results that can be numerically precise and analytically exact. Nevertheless, there are less exact 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 consequences of hazards under organizational control starts by assessing the probability that the consequences of hazards materialize 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, on industry trends and, at worst, on opinion.

5.4.5 Based on the considerations emerging from the replies to questions such as those listed in 5.4.2, 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 table, in this case, a five-point table. The table includes five categories to denote the probability of occurrence of an unsafe event or condition, the meaning of each category, and an assignment of a value to each category. 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 with 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 to be of a complexity that is suitable for educational purposes as well as for the needs of this manual.

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 consequences of hazards under organizational control is the assessment of the severity of the consequences of the hazard if its damaging potential materializes during operations aimed at delivery of services. This is known as assessing the safety risk severity.

	Meaning	Value
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (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

5.5.2 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 consequences of the hazard if its damaging potential materializes 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 and economic impact for the State)?
- c) What is the likelihood of environmental impact (spillage of fuel or other hazardous product, and physical disruption of the 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 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 five categories to denote the level of severity of the occurrence of an unsafe event or condition, the meaning of each category, and the assignment of a value to each category. As with the safety risk probability table, this table is an example presented for educational purposes only, and the same caveats expressed in 5.4.6 apply.

Severity of occurrence	Meaning	Value
Catastrophic	<ul style="list-style-type: none"> — Equipment destroyed — Multiple deaths 	A
Hazardous	<ul style="list-style-type: none"> — 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 — Serious injury — Major equipment damage 	B
Major	<ul style="list-style-type: none"> — 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 — Serious incident — Injury to persons 	C
Minor	<ul style="list-style-type: none"> — Nuisance — Operating limitations — Use of emergency procedures — Minor incident 	D
Negligible	<ul style="list-style-type: none"> — 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 consequences of 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 consequences of the unsafe event or condition under organizational control is the assessment of the tolerability of the consequences of the hazard if its damaging potential materializes 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 5.2, it can be seen, through this example, that a safety risk is just a number or alphanumeric 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.

5.6.3 Second, the safety risk index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix that describes the tolerability criteria. The criterion for a safety risk assessed as 4B is, according to the tolerability table 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 consequences of the hazards;
- b) allocate resources to reduce the magnitude or the damaging potential of the consequences of the hazards; or
- c) cancel the operation if mitigation is not possible.

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

Suggested criteria	Assessment risk index	Suggested criteria
Intolerable region	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances
Tolerable region	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Acceptable based on risk mitigation. It may require management decision.
Acceptable region	3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E	Acceptable

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 consequences 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 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 the delivery of services which exposes the organization to the consequences of the hazards in question must be cancelled. Figure 5-6 presents the process of safety risk management in graphic format.

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

- a) **Avoidance.** The operation or activity is cancelled because safety risks exceed the benefits of continuing the operation or activity. Examples of avoidance strategies include:
 - 1) operations into an aerodrome surrounded by complex geography and without the necessary aids are cancelled;
 - 2) operations in RVSM airspace by non-RVSM equipped aircraft are cancelled.
- b) **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 reduction strategies include:
 - 1) operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to daytime, visual conditions;
 - 2) operations by non-RVSM equipped aircraft are conducted above or below RVSM airspace.

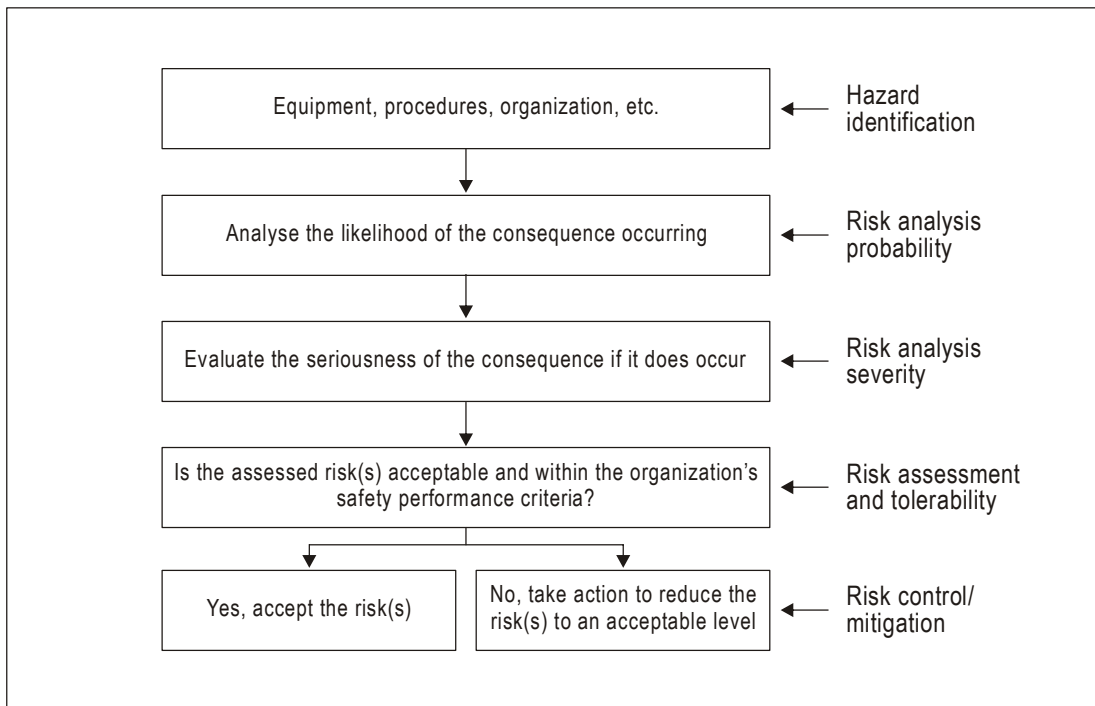


Figure 5-6. The process of safety risk management

- c) **Segregation of exposure.** Action is taken to isolate the effects of the consequences of the hazard or build in redundancy to protect against them. Examples of strategies based on segregation of exposure include:
- 1) operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to aircraft with specific performance navigation capabilities;
 - 2) non-RVSM equipped aircraft are 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 consequences 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.** This mitigation eliminates the safety risk of the consequences of the unsafe event or condition, for example, by providing interlocks to prevent thrust reverser activation in flight.

- 2) **Control mitigations.** This mitigation accepts the safety risk of the consequences 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 on flawless human performance.
 - 3) **Personnel mitigations.** This mitigation accepts that engineering and/or control mitigations are neither efficient nor 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 has been 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 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 to subordinates responsibility for safety risk management.

5.7.6 To summarize, safety risk control/mitigation strategies are mostly based on the deployment of additional safety defences or 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; and
- c) regulations.

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

- a) Do defences to protect against the safety risks of the consequences of the hazards exist?
- b) Do defences function as intended?
- c) Are the defences practical for use under actual working conditions?
- d) Are staff involved aware of the safety risks of the consequences of the hazards, 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 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 and 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 existing defences within the aviation system.

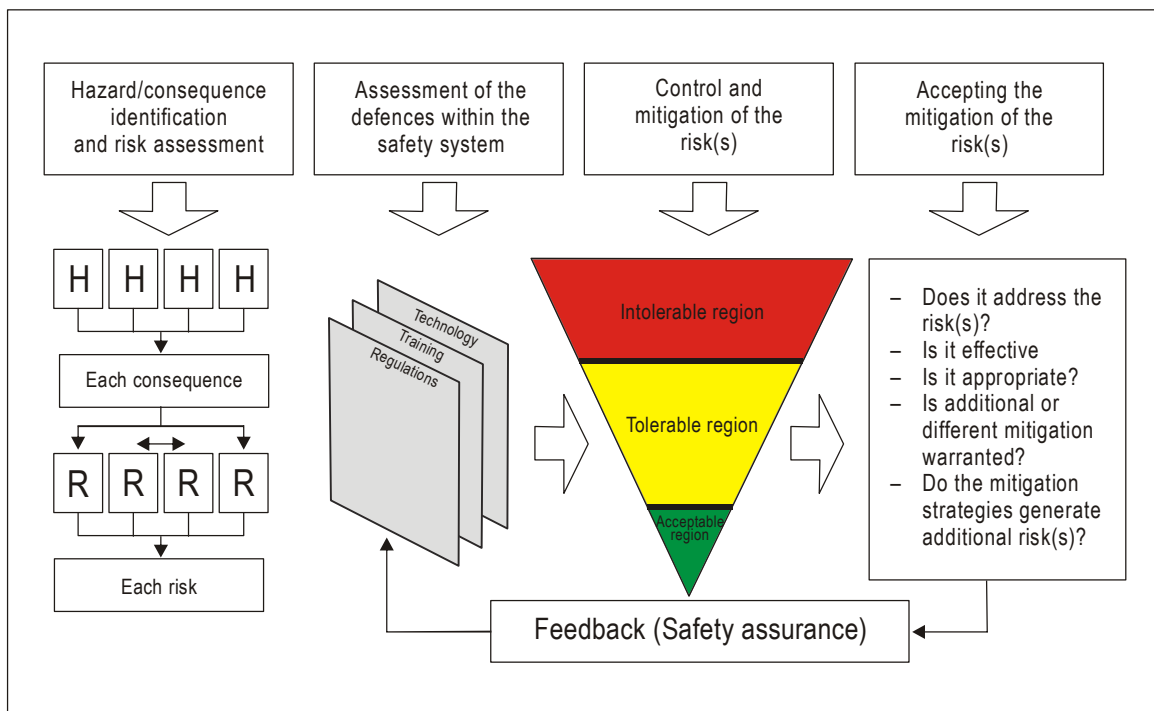


Figure 5-7. The safety risk mitigation process

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

5.7.11 Following reassessment 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 risks?
- b) Is the mitigation effective?
- c) Is the mitigation appropriate?
- d) Is additional or different mitigation warranted?
- e) Do the mitigation strategies generate additional risks?

5.7.12 Once the mitigation has been accepted, the strategies developed and deployed must, as part of the safety assurance process, be fed back into the organization's defences, upon which the mitigation strategies are 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 summarized as follows:

- a) There is no such thing as absolute safety — in aviation it is not possible to eliminate all safety risks.
- b) Safety risks must be managed to a level “as low as reasonably practicable” (ALARP).
- c) Safety risk mitigation must be balanced against:
 - 1) time;
 - 2) cost; and
 - 3) the difficulty of taking measures to reduce or eliminate the safety risk (i.e. managed).
- d) 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.
- e) The rationale for safety risk decisions must be communicated to the stakeholders affected by them, to gain their acceptance.

5.8.2 Figure 5-8 presents the safety risk management process in its entirety. After a safety concern has been perceived, hazards underlying the safety concern and potential consequences of the hazards 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 risks are assessed as acceptable, action as appropriate is taken and the operation continues. For feedback purposes (safety library), the hazard identification and safety risk assessment and mitigation are recorded.

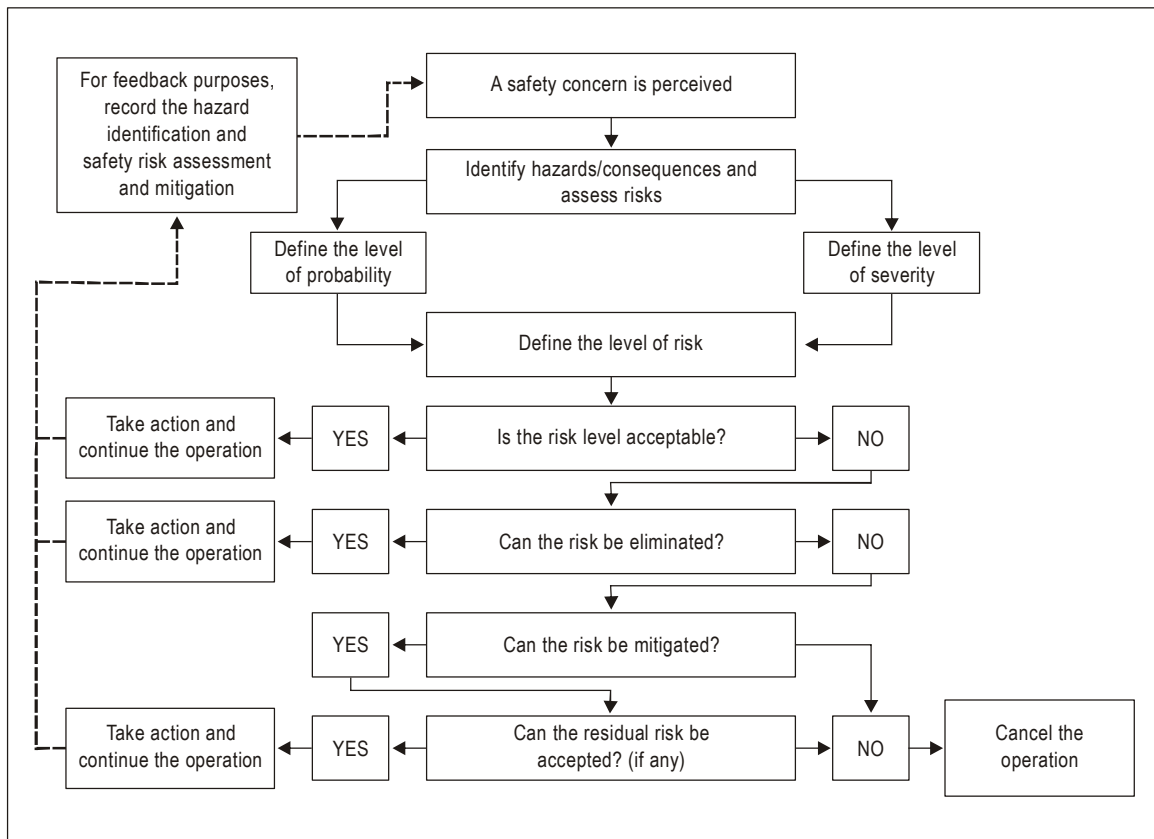


Figure 5-8. The safety risk management process

5.8.3 If the safety risks are assessed as unacceptable, the following questions become relevant:

- 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, the next question is:
- 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 the next question is:
- 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, the operation must be cancelled.

5.8.4 Question 5.8.3 c) reflects the fact that mitigation strategies can never completely mitigate safety risks. It must be accepted that a residual safety risk will always exist, and the organization must ensure that 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 safety risk management scenarios are presented in the appendices 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

1. SCENARIO

1.1 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.

1.2 The 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, which could lead to runway incursions. The SAG applies a safety risk management process to evaluate the safety consequences of the construction plan.

2. 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:

- a) the runway environment during construction at night, including a high volume of construction vehicle traffic between the ramp and the construction site;
- b) the existing driver training programme and the use of escorts for construction vehicles;
- c) the air traffic control tower and the fact that there is no radio communication with construction vehicles, which are not radio-equipped; and
- d) signs, markings and lighting for the taxiways, runways and construction area.

3. 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:

- a) State the generic hazard
 - 1) Airport construction.

- b) State the specific component(s) of the hazard
 - 1) Construction vehicles crossing the primary runway.
- c) Assess the consequences of the specific components of the generic hazard
 - 1) Construction vehicles may deviate from prescribed procedures and cross the primary runway without an escort.
 - 2) Aircraft could conflict with a crossing vehicle.

4. SAFETY RISK ASSESSMENT PROCESS

The third task of the SAG is to identify and assess the safety risks of the consequences of the hazards, and the existing defences, as follows:

- a) The SAG assessment leads to the conclusion that there is a remote probability that a construction vehicle will deviate from prescribed procedures and cross the primary runway without an escort.
- b) There are night air carrier operations at the airport, so there is a remote probability that an aircraft could conflict with a crossing vehicle.
- c) 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.
- d) The SAG assesses existing defences (driver training programme, use of escorts for construction vehicles, signs, markings and lighting).
- e) 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).
- f) 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.

5. 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:

- a) 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.
- b) 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 being extremely improbable. Nevertheless, should an aircraft/construction vehicle conflict occur, the severity of such an occurrence would still be catastrophic.

- c) Use of the perimeter road as mitigation may delay construction vehicles due to the added driving distance, but in the assessment of the SAG:
 - 1) 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), it nevertheless brings the safety risks of the consequences (construction vehicle deviating from prescribed procedures 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).
- d) Using the safety risk assessment matrix (Chapter 5, Figure 5-4) and the safety risk tolerability matrix (Chapter 5, Figure 5-5), the SAG reassesses the safety risk index as 1A (acceptable);
- e) The SAG documents this decision process for future follow-up with the Anycity International Airport safety manager.

6. HAZARD IDENTIFICATION AND SAFETY RISK MANAGEMENT LOG

6.1 The hazard identification and safety risk management log in Table 5-App 1-1 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 safety risk assessments.

6.2 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 safety risk management log is not to be cleared until this action is completed.

Table 5-App 1-1. Hazard identification and safety risk management

<i>Type of operation or activity</i>	<i>Generic hazard</i>	<i>Specific components of the hazard</i>	<i>Hazard-related consequences</i>	<i>Existing defences to control safety risks, and safety risk index</i>	<i>Further action to reduce safety risks, and resulting safety risk index</i>
Airport operations	Airport construction	Construction vehicles crossing primary runway	<p>a) Construction vehicles may deviate from prescribed procedures and cross the primary runway without an escort.</p> <p>b) Aircraft could conflict with a crossing vehicle.</p>	<p>a) The SAG assessment leads to the conclusion that there is a remote probability that a construction vehicle will deviate from prescribed procedures and cross the primary runway without an escort.</p> <p>b) There are night air carrier operations at the airport, so there is a remote probability that an aircraft could conflict with a crossing vehicle.</p> <p>c) 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.</p> <p>d) The SAG assesses existing defences (driver training programme, use of escorts for construction vehicles, signs, markings and lighting).</p> <p>e) 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: Safety risk index: 3A Safety risk tolerability: Unacceptable under the existing circumstances.</p>	<p>a) 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.</p> <p>b) 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 being extremely improbable. Nevertheless, should an aircraft/construction vehicle conflict occur, the severity of such an occurrence could still be catastrophic.</p> <p>c) Use of the perimeter road as mitigation may delay construction vehicles due to the added driving distance, but in the assessment of the SAG:</p> <ol style="list-style-type: none"> 1) 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), it nevertheless brings the safety risks of the consequences (construction vehicle deviating from prescribed procedures and crossing the primary runway without an escort; and aircraft in conflict with a crossing vehicle) to an acceptable level. <p>d) Using the safety risk assessment matrix (Chapter 5, Figure 5-4) and the safety risk tolerability matrix (Chapter 5, Figure 5-5), the SAG reassesses: Safety risk index: 1A Safety risk tolerability: Acceptable.</p> <p>e) The SAG documents this decision process for future follow-up with the Anycity International Airport safety manager.</p>

Appendix 2 to Chapter 5

CONVERGING RUNWAY OPERATIONS

1. SCENARIO

1.1 An air traffic service provider has received feedback from airport users expressing safety concerns regarding converging runway operations at XYZ International Airport. XYZ International Airport consists of three runways, 08L/26R, 08R/26L, and 12/30 (see Figure 5-App 2-1). Converging runway operations are occasionally conducted on 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 in light of the concerns expressed by users.

1.2 The Safety Action Group (SAG) is requested to assist the ATS service provider's 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 pilot's association, airport representatives as well as representatives from the State's 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.

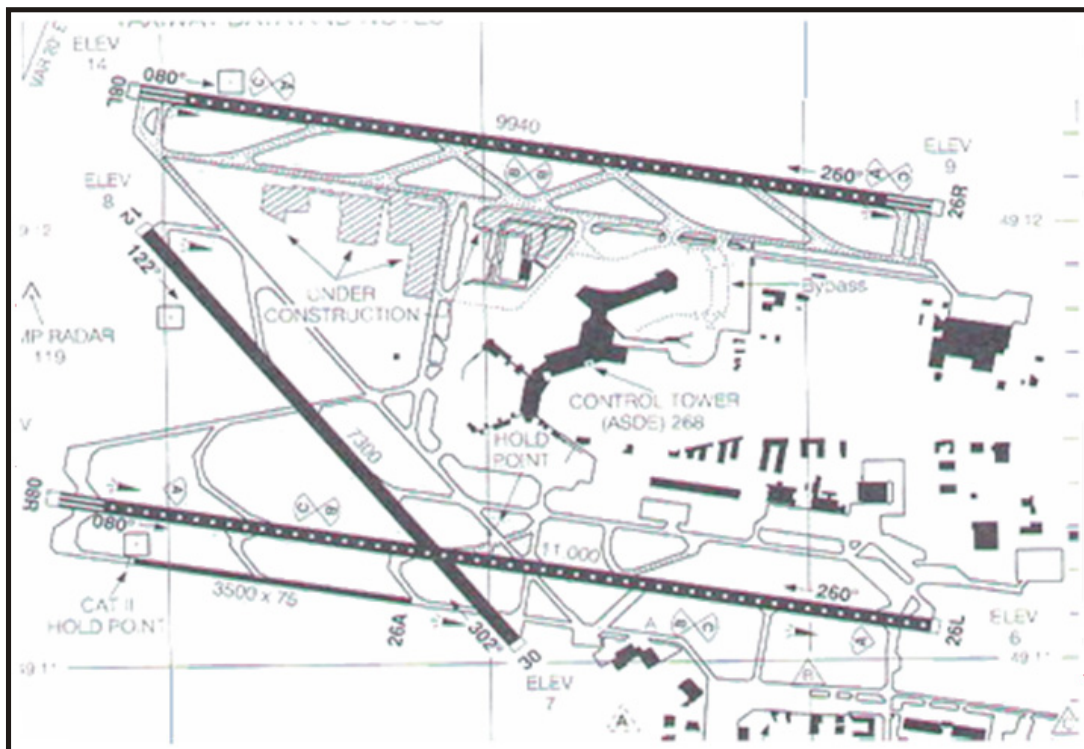


Figure 5-App 2-1. XYZ International Airport

2. SYSTEM DESCRIPTION

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

- a) XYZ International Airport has three main runways and a small secondary runway service.
- b) The airport has about 325 000 movements per year.
- c) 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 7300 feet long. Runway 12 is used mostly for arrivals. Runway 30 is used sometimes for departures and is seldom used for arrivals. Runway 12 physically crosses runways 08R-26L and is considered to be an "intersecting" runway. Runway 08L-26R is 9 940 feet long and is used primarily for arriving traffic and occasionally for departing traffic. Runway 08L is used only for arrivals because departure procedures have not yet been established.
- d) Markings, signage and lighting on the airport meet the standards of both the oversight authorities and ICAO.
- e) There are two control frequencies used for tower control. One frequency covers the south runway (26L-08R) and the west runway (12-30). The second frequency covers the north runway (26R-08L).
- f) The south runways (26L-08R) have converging runway approaches published to avoid conflict with traffic on runway 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.
- g) 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 runways 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.
- h) While IFR traffic separation is provided to IFR traffic on runway 26R, airport control service is provided to VFR and visual approaches to aircraft on runway 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.

3. HAZARD IDENTIFICATION PROCESS

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

- a) State the generic hazard
 - 1) Converging flight paths on runways 26R-08L and 12, irrespective of aircraft on approach or departure.
- b) State the specific component(s) of the hazard
 - 1) Aircraft rejects landing on runway 26R against traffic landing on runway 12.

- 2) Aircraft takes off on runway 26R against traffic landing on runway 12.
 - 3) Aircraft approaches runway 08L against traffic landing on runway 12.
 - 4) An aircraft conducts a "side step" from an approach on runway 08L to runway 08R or runway 08R to runway 08L against traffic landing on runway 12.
- c) Assess the consequence(s) of the specific component(s) of the generic hazard
- 1) Wake turbulence encounter.
 - 2) Evasive action to avoid other traffic.
 - 3) Loss of control following manoeuvre to avoid other traffic.
 - 4) Runway overrun following an unstable approach.
 - 5) Mid-air collision at the departure end of runway 26R between aircraft approaching runway 12 and aircraft approaching runway 08L or departing runway 26R (worst-case consequence).

4. SAFETY RISK ASSESSMENT PROCESS

4.1 The SAG identifies 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 runways 26R-08L and 12.

4.2 The defences include:

- a) controller coordination procedures;
- b) increased spacing to protect airspace for missed approaches during adverse weather;
- c) restrictions on arrivals on runway 12 when runway 26R is used for departures;
- d) aerodrome surface detection equipment (ASDE);
- e) runway incursion prevention programme and wildlife control programme;
- f) airside driver initial and recurrent training and testing;
- g) continual monitoring and statistical follow-up of crosswind limits;
- h) availability and use of approach radar;
- i) standards for runway occupancy time;
- j) separate tower frequencies; and
- k) markings and signage.

4.3 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), assesses the safety risks of the consequences of converging flight paths for runways 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 manoeuvre 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) Mid-air collision at the departure end of runway 26R between aircraft approaching runway 12 and aircraft approaching runway 08L or departing runway 26R: probability improbable, severity catastrophic. Safety risk tolerability: 2A (acceptable based on risk mitigation).

5. SAFETY RISK CONTROL/MITIGATION PROCESS

5.1 The SAG recognizes that prohibiting operations on converging runways would effectively eliminate the worst possible consequence of converging flight paths for runways 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.

5.2 The SAG concludes that there are no safety concerns at XYZ International Airport regarding converging runway operations for runways 26R and 12 that require urgent, immediate action. Existing defences for the safety risks of the consequences of converging flight paths for runways 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 the safety of operations at XYZ International Airport are made. While not of an urgent nature, implementation of these recommendations would provide a greater margin of safety.

5.3 The recommendations include:

- a) Initiate a continuing campaign to encourage flight crews to pass pilot reports (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 runway 08L-26R is kept advised of intersecting traffic on runway 12.

- e) Install an emergency frequency override so that one controller can switch to another controller's frequency to issue emergency instructions.
- 5.4 The SAG documents this decision process for future follow-up with the air traffic service safety manager.

6. HAZARD IDENTIFICATION AND SAFETY RISK MANAGEMENT LOG

6.1 The hazard identification and safety risk management log in Table 5-App 2-1 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.

6.2 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 safety risk management log is not to be cleared until this action is completed.

Table 5-App 2-1. Hazard identification and safety risk management

<i>Type of operation or activity</i>	<i>Generic hazard</i>	<i>Specific components of the hazard</i>	<i>Hazard-related consequences</i>	<i>Existing defences to control safety risks, and safety risk index</i>	<i>Further action to reduce safety risks, and resulting safety risk index</i>
Air traffic control activities	Converging flight paths on runways 26R-08L and 12, irrespective of aircraft on approach or departure	<p>a) Aircraft rejects landing on runway 26R against traffic landing on runway 12.</p> <p>b) Aircraft takes off on runway 26R against traffic landing on runway 12.</p> <p>c) Aircraft approaches runway 08L against traffic landing on runway 12.</p> <p>d) An aircraft conducts a "side step" from an approach on runway 08L to runway 08R or runway 08R to runway 08L against traffic landing on runway 12.</p>	<p>a) Wake turbulence encounter.</p> <p>b) Evasive action to avoid other traffic.</p> <p>c) Loss of control following manoeuvre to avoid other traffic.</p> <p>d) Runway overrun following an unstable approach.</p> <p>e) Mid-air collision at the departure end of runway 26R between aircraft approaching runway 12 and aircraft approaching runway 08L or departing runway 26R (worst-case consequence).</p>	<ul style="list-style-type: none"> • 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 crosswind limits; • Availability and use of approach radar; • Standards for runway occupancy time; • Separate tower frequencies; and • Markings and signage. <p>a) Wake turbulence encounter: Safety risk index: 3C Safety risk tolerability: Acceptable based on risk mitigation.</p> <p>b) Evasive action to avoid other traffic: Safety risk index: 3C Safety risk tolerability: Acceptable based on risk mitigation.</p> <p>c) Loss of control following manoeuvre to avoid other traffic: Safety risk index: 3B Safety risk tolerability: Acceptable based on risk mitigation.</p> <p>d) Runway overrun following an unstable approach: Safety risk index: 3B Safety risk tolerability: Acceptable based on risk mitigation.</p> <p>e) Mid-air collision at the departure end of runway 26R between aircraft approaching runway 12 and aircraft approaching runway 08L or departing runway 26R: Safety risk index: 2A Safety risk tolerability: Acceptable based on risk mitigation.</p>	<p>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;</p> <p>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;</p> <p>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;</p> <p>d) Depict a range of approach speed constraints on arrival type charts; and modify air traffic controller communication procedures so traffic on runway 08L-26R is advised of intersecting traffic on runway 12.</p> <p>e) Install an emergency frequency override so that one controller can switch to another controller's frequency to issue emergency instructions.</p>

Appendix 3 to Chapter 5

COMMERCIAL OPERATIONS AT ANDES CITY INTERNATIONAL AIRPORT

1. SCENARIO

1.1 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 high in the mountains, surrounded by beautiful landscape and showcasing the vestiges of an ancient civilization. Ground transportation can take more than two days through dangerous roads; therefore air transportation is the most suitable means of transportation.

1.2 Andes City is served by a high-elevation aerodrome surrounded by complex geography with no approach navigation aids, resulting in flight operations limited to daytime 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 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 turnaround to the main base, ninety minutes away.

1.3 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 complex geography with no approach navigation aids. The SAG applies a safety risk management process to evaluate the safety consequences of the operation at Andes City International Airport.

2. SYSTEM DESCRIPTION

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

- a) 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.
- b) The aerodrome has only one runway with a length of 3 400 m (11 155 ft), oriented east-west (runway 09-27).
- c) Because of the topography, runway 09 is exclusively used for landing, and runway 27 is exclusively used for take-off.
- d) A VOR is used for instrument letdown approach, located in the valley twenty miles west of the aerodrome.
- e) No ILS approach is available.
- f) 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.

- g) 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.
- h) No landing visual aids are available.
- i) 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 that it is clear of the runway after landing.
- j) The weather at Andes City International Airport is variable, often characterized by a high layer of clouds with a base around 19 000 to 21 000 feet.
- k) Outside temperature is high between 10:00 and 14:00 hours, affecting aircraft performance.
- l) Katabatic winds may impose the need for tailwind take-offs from runway 27 after approximately 16:00 hours daily.
- m) 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 the obstacle clearance and net trajectory.
- n) The national civil aviation authority (CAA) requires that the airline shall demonstrate that the aircraft can comply 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 its operator certificate.
- o) 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 have received special training for the operation at Andes City International Airport.

3. 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:

- a) State the generic hazard
 - 1) Operation at a high-altitude airport surrounded by complex geography.
- b) State the specific components of the hazard
 - 1) Surrounding mountains.
 - 2) High-elevation aerodrome.
 - 3) Lack of approach and landing navigation aids.
 - 4) Lack of visual landing aids.
 - 5) Conflicting traffic.

- 6) Slippery runway when wet.
- 7) Wildlife.
- c) Assess the consequences of the specific components of the generic hazard
 - 1) Controlled flight into terrain (CFIT) due to:
 - i) loss of a critical engine during approach and landing;
 - ii) loss of a critical engine during take-off after V_1 ;
 - iii) loss of a critical engine during en-route climb.
 - 2) Mid-air collision.
 - 3) Landing overrun after landing.
 - 4) Landing overrun following aborted take-off.
 - 5) Bird strike.

4. SAFETY RISK ASSESSMENT PROCESS

Note.— Controlled flight into terrain due to a critical engine during take-off after V_1 is the only consequence analysed in this exercise. In an actual safety risk assessment all consequences need to be analysed and all safety risks assessed and mitigated.

4.1 The third task of the SAG is to assess the effectiveness of existing defences to address the safety risks of the consequences of the hazards.

4.2 The SAG reviews existing safety defences that can be affected or are 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.

4.3 The existing defences identified during the assessment are as follows:

- a) VMC and daylight aircraft operation;
- b) aerodrome layout available in the national AIP;
- c) ATC procedures in place at the aerodrome;
- d) company operations manual;
- e) dispatch performance manual;
- f) aircraft operating manual;
- g) recurrent training on engine failure before and after V_1 and missed approach procedures;
- h) CRM training.

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

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

4.6 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).

5. SAFETY RISK CONTROL/MITIGATION PROCESS

5.1 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 a critical engine during take-off after V_1 . After several meetings, the SAG proposes several mitigations. The proposed mitigations aim at reinforcing the defences and lowering the safety risk to “as low as reasonably practicable” (ALARP). The mitigations include:

- a) Develop take-off and climb procedures in case of the loss of a critical engine after V_1 , considering the possibility of a return to land.
- b) Develop and provide training in the above procedures (full flight simulator and maintain qualification every six months).
- c) Consider Andes City International Airport to be a “special aerodrome operation” requiring special crew qualification, valid for only for one year unless renewed.
- d) Provide appropriate “special aerodrome operation” training to cabin crews. (This mitigation does not address probability but severity — emergency evacuation — of one consequence of the safety risk.)
- e) Provide accurate weather information, particularly surface winds after 16:00 hours.
- f) Develop operational documentation and include it in the company operations manual and dispatch manual, for approval by the CAA.
- g) Prohibit an open minimum equipment list (MEL) critical items policy.
- h) Under the maintenance reliability programme, the maintenance department is to observe the engines of the aircraft allocated to the operation.
- i) Follow up on safety measures and new defences implemented for the control and mitigation of the safety risks related to the operation at Andes City International Airport. A review of the effectiveness of the defences is planned for 6 months and 12 months after the changes have been implemented and the authorization has been granted by the CAA.

5.2 Taking into account the new defences put in place for this special operation, the safety risk of a CFIT due to loss of a critical engine during take-off after V_1 is now assessed as improbable (2 — very unlikely to occur) although the severity of a CFIT still remains catastrophic (A — equipment destroyed — multiple deaths).

5.3 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 are incorporated into the company “safety library”.

6. INDIVIDUAL RESPONSIBILITIES FOR IMPLEMENTING MITIGATION MEASURES

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

- a) Mitigation measures a), f) and i) — director of flight operations;
- b) Mitigation measures b), c) and d) — flight training manager;
- c) Mitigation measure e) — dispatch manager;
- d) Mitigation measures g) and h) — director of maintenance.

7. HAZARD IDENTIFICATION AND SAFETY RISK MANAGEMENT LOG

7.1 The hazard identification and safety risk management log in Table 5-App 3-1 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.

7.2 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, 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 safety risk management log is not to be cleared until this action is completed.

Table 5-App 3-1. Hazard identification and risk management

Type of operation or activity	Generic hazard	Specific components of the hazard	Hazard-related consequences	Existing defences to control safety risks, and safety risk index	Further action to reduce safety risks, and resulting safety risk index	Responsible person
Flight operations	Operation at a high-altitude airport surrounded by complex geography	<ul style="list-style-type: none"> a) Surrounding mountains. b) High elevation aerodrome. c) Lack of approach and landing navigation aids. d) Lack of visual landing aids. e) Conflicting traffic. f) Slippery runway when wet. g) Wildlife. 	<ul style="list-style-type: none"> a) Controlled flight into terrain (CFIT) due to: <ul style="list-style-type: none"> 1) loss of a critical engine during approach and landing; 2) loss of a critical engine during take-off after V₁; 3) loss of a 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. <p><i>Note.— Controlled flight into terrain due to loss of a critical engine during take-off after V₁ is the only consequence analysed in this exercise. In an actual evaluation all consequences need to be analysed and all safety risks assessed and mitigated.</i></p>	<ul style="list-style-type: none"> a) VMC and day-light aircraft operation. b) Aerodrome layout available in the national AIP. c) ATC procedures in place at the aerodrome. d) Company operations manual. e) Dispatch performance manual. f) Aircraft operating manual. g) Recurrent training on engine failure before and after V₁ and missed approach procedures. h) CRM training. <p>Safety risk index: 3A Safety risk tolerability: Unacceptable under the existing circumstances.</p>	<ul style="list-style-type: none"> a) 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. b) Develop and provide training in the above procedures (full flight simulator and maintain qualification every six months). c) Consider Andes City International Airport to be a “special aerodrome operation” requiring special crew qualification, valid for only one year unless renewed. d) Provide appropriate “special aerodrome operation” training to cabin crews. (This mitigation does not address probability but severity — emergency evacuation — of the safety risk). e) Provide accurate weather information, particularly surface winds after 16:00 hours. f) Develop operational documentation and include it in the company operations manual and dispatch manual, for approval by the CAA. g) Prohibit an open minimum equipment list (MEL) critical items policy. h) Under the maintenance reliability programme, the maintenance department is to observe the engines of the aircraft allocated to the operation. 	<ul style="list-style-type: none"> Director of operations Training manager Training manager Training manager Dispatch manager Director of operations Director of maintenance Director of maintenance

<i>Type of operation or activity</i>	<i>Generic hazard</i>	<i>Specific components of the hazard</i>	<i>Hazard-related consequences</i>	<i>Existing defences to control safety risks, and safety risk index</i>	<i>Further action to reduce safety risks, and resulting safety risk index</i>	<i>Responsible person</i>
					<p>i) Follow up on safety measures and new defences implemented for the control and mitigation of the safety risks related to the operation at Andes City International Airport. A review of the effectiveness of the defences is planned for 6 months and 12 months after the changes have been implemented and the authorization has been granted by the CAA.</p> <p>Safety risk index: 2A Safety risk tolerability: Acceptable based on risk mitigation. It might require management decision.</p>	Director of operations

Chapter 6

ICAO SAFETY MANAGEMENT SARPs

6.1 OBJECTIVE AND CONTENTS

This chapter presents the ICAO safety management SARPs included in Annex 1 — *Personnel Licensing*, Annex 6 — *Operation of Aircraft*, Annex 8 — *Airworthiness of Aircraft*, Annex 11 — *Air Traffic Services*, Annex 13 — *Aircraft Accident and Incident Investigation* and Annex 14 — *Aerodromes*. This chapter also presents the relationship between the State safety programme (SSP) and the service provider's safety management system (SMS). This chapter includes the following topics:

- a) ICAO safety management SARPs — General;
- b) State safety programme (SSP);
- c) Acceptable level of safety (ALoS);
- d) Safety management system (SMS);
- e) SMS safety performance;
- f) Management accountability;
- g) Relationship between an SSP and an SMS; and
- h) Compliance and performance.

6.2 ICAO SAFETY MANAGEMENT SARPS — GENERAL

6.2.1 The ICAO safety management SARPs are contained in Annexes 1; 6, Parts I and III; 8; 11; 13 and 14. 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 service providers and certified aerodromes. In the case of Annex 1, the safety management SARPs are limited exclusively to approved training organizations that are exposed to safety risks during the provision of their services.

6.2.2 The safety management SARPs 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 service providers and certified aerodromes, as applicable.

6.2.3 The ICAO safety management SARPs address 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 the provision of services.

6.2.4 The ICAO safety management SARPs introduce the notion of acceptable level of safety (ALoS) as the way of expressing the minimum degree of safety that has been established by the State and must be assured by an SSP, and the notion of safety performance as the way of measuring the safety performance of a service provider and its 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.

6.3.3 In order to assist States in the establishment of their 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. 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 are fulfilled by the State. The organization of the safety responsibilities and accountabilities of a State observing 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 the 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 the safety performance of an SMS, building upon the safety assurance component of both an SSP and an SMS and 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 and a fundamental component of its safety assurance component. The objectives of the State's safety oversight function, as traditionally practised, are satisfied through administrative controls (inspections, audits and surveys) carried out by civil aviation authorities regularly, and do not

necessarily constitute safety risk controls, as discussed in Chapter 5 and in Section 6.8. The SSP is necessary to turn the outcomes of safety oversight 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 monitors 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). In 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 the actual performance of an SSP. The operation of an SSP may then be reduced to simply "ticking the appropriate boxes" under the false pretence of managing safety.

6.4.3 The basic management axiom that one cannot manage what one cannot measure is discussed elsewhere in this 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 the level of design expectations. Thus, measurable performance outcomes permit the actual performance of activities critical to safety to be assessed against existing organizational controls, so that safety risks can be maintained ALARP and necessary corrective action taken. This notion is applicable to both an SSP and an SMS, although with certain considerations related to the specificities of each one, which are highlighted in this Section and in Section 6.6.

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 implementation of the SSP can the objective of continuous improvement of safety underlying safety management be achieved.

6.4.5 The development and implementation of ALoS builds upon certain basic concepts of systems theory. A brief discussion follows.

6.4.6 There is a hierarchy inherent to the basic concepts of systems theory underlying ALoS and the way these concepts must be sequenced in progression when developing ALoS. An understanding of the concepts and their inherent hierarchy is an essential foundation for the development of ALoS regarding an SSP. The concepts involved and their hierarchy are as follows:

- a) **safety** (as defined in Chapter 2);

- b) **level of safety** is the degree of safety of a system. It is an emerging property of the system, which represents the quality of the system, safety-wise. It is expressed through safety indicators;
- c) **safety indicators** are the parameters that characterize and/or typify the level of safety of a system;
- d) **safety targets** are the concrete objectives of the level of safety;
- e) **acceptable level of safety** is the minimum degree of safety that must be assured by a system in actual practice;
- f) **safety indicator value** is the quantification of a safety indicator; and
- g) **safety target value** is the quantification of a safety target.

6.4.7 The selection of appropriate safety indicators is key to the development of ALoS. Such selection should be a function of the detail to which the level of safety of the system is intended to be represented. If the level of safety is to be represented in broad, generic terms, the selection of safety indicators representing high-level/high-consequence system outcomes (quantitative) and/or high-level system functions (qualitative) is appropriate. If the level of safety of the system is to be represented in specific, narrow terms, then the selection of indicators representing low-level/low-consequence system outcomes and lower level system functions is required. In both cases, meaningful safety indicators must be representative of the outcomes, processes and functions that characterize system safety.

6.4.8 Typical examples of safety indicators in the aviation system include, among others:

- a) fatal airline accidents;
- b) serious incidents;
- c) runway excursion events;
- d) ground collision events;
- e) development/absence of primary aviation legislation;
- f) development/absence of operating regulations; and
- g) level of regulatory compliance.

6.4.9 Typical examples of safety targets in the aviation system include, among others:

- a) reduction in fatal airline accidents;
- b) reduction in serious incidents;
- c) reduction in runway excursion events;
- d) reduction in ground collision events; and
- e) the number of inspections completed quarterly.

6.4.10 The first step in developing an ALoS related to an SSP is therefore to decide on the detail to which the level of safety of the particular State aviation system is intended to be represented, and then select meaningful safety

indicators that characterize or typify the level of safety of the State aviation system. The availability of safety data to the State is a determinant factor in the decision regarding the detail of representation, as well as the selection of quantitative or qualitative safety indicators. States that have developed safety data collection and analysis capabilities should be in a position to represent the level of safety in greater detail than States that have not. States in the former group should be able to define quantitative safety indicators, while States in the latter group may elect to initially favour qualitative safety indicators while they develop safety data collection and analysis capabilities. Once safety indicators have been defined, the next step is to define associated safety targets, which can be considered as objectives of improvement.

6.4.11 Once safety indicators and safety targets have been selected, the level of safety representing the particular State aviation system can be established. At such point, the State should be ready to progress to the development of ALoS, the *minimum* degree of safety in civil aviation that must be assured by the SSP in actual practice. In order to develop ALoS, values must be attached to the safety indicators, and objectives of improvement and/or maintenance of such values must be attached to the safety targets. While it is generally accepted that the ALoS related to an SSP is expressed through the safety indicator values and the safety target values, strictly speaking it is the safety target values that are the true expression of ALoS. Figure 6-1 includes an example of safety indicator values and safety target values. Further consideration when establishing ALoS must be given to:

- a) the level of safety risk that applies;
- b) the safety risk tolerance;
- c) the cost/benefits of improvements to the aviation system; and
- d) public expectations about the civil aviation system.

Safety indicator value	→	Safety target value
1. [Rate/number] fatal airline accidents per [number] operations	→	1. Reduce by [number] the number of / Maximum of [number] fatal airline accidents per [number] operations
2. [Rate/number] runway excursion events per [number] operations	→	2. Reduce by [number] the number of / Maximum of [number] runway excursion events per [number] operations
3. [Rate/number] ground collision events per [number] operations	→	3. Reduce by [number] the number of / Maximum of [number] ground collision events per [number] operations
4. [Number] inspections of operators completed [time frame]	→	4. Minimum of [number] inspections completed [time frame]

Figure 6-1. An example of safety indicator values and safety target values

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

6.4.13 **Safety measurement** refers to the quantification of the outcomes of selected high-level, high-consequence events, such as accident and serious incident rates. Safety measurement can also be applied to reflect the quantification of selected high-level State functions, such as the status of development/implementation of primary aviation safety legislation or the absence thereof, the status of development/implementation of specific operating regulations or the absence thereof, and the level of regulatory compliance within the State. Safety measurement is not a continuous process, but is rather a spot check, normally conducted following pre-specified time frames, for example, annually, semi-annually or quarterly. Safety measurement is associated with the SSP and reflects the extent to which the high-level safety objectives of the safety interventions of mitigation strategies have been achieved.

6.4.14 **Safety performance measurement** refers to the quantification of the outcomes of selected low-level, low-consequence processes, such as the number of foreign object debris (FOD) events per specified number of ramp operations, or the number of unauthorized ground vehicle events on taxiways per a 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, by an organization, of selected operational activities that are necessary to deliver the services the organization was constituted to deliver (provision of aerodrome services, air traffic control, training, etc.). Safety performance measurement is mostly, but not exclusively, associated with an SMS, and 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). It also applies to the safety interventions and mitigation strategies established as part of an SSP, as applicable.

6.4.15 The ALoS related to an SSP must be developed based upon a judicious combination of safety measurement and safety performance measurement. The extent to which ALoS represents safety measurement or safety performance measurement depends upon the maturity of the SSP. Initially, immediately following development and implementation of an SSP, the safety indicator values and the safety target values related to ALoS will likely be expressed through quantitative action statements on selected high-level/high-consequence outcomes (safety measurement). Figure 6-2 provides an example of safety indicator values and safety target values based on safety measurement.

6.4.16 As the SSP matures and safety data collection and analysis capabilities are developed through the safety assurance component of the SSP, the safety indicator values and the safety target values related to ALoS can be modified and expressed through a combination of quantitative action statements on selected high-level/high-consequence events (safety measurement) and quantitative action statements on selected low-level/low-consequence outcomes (safety performance measurement). As the SSP achieves maturity, the safety indicator values and the safety target values related to ALoS will be expressed through quantitative action statements on selected low-level/low-consequence outcomes (safety performance measurement). Figure 6-3 provides an example of safety indicator values and safety target values based on safety performance measurement.

6.4.17 Two generic aspects must be considered when assessing whether the specific safety target values of ALoS should represent improvement with respect to, or rather maintenance, of the related safety indicator values. First, consideration must be given to the availability of resources within the State to achieve the improvement considered. Second, consideration must be given to how expensive the action plan(s) deemed necessary to achieve the improvement is. A third consideration, applicable only to safety target values based upon safety performance measurement, is whether the assessment of the safety risks of the consequences of the hazards addressed by the improvement falls in the tolerable region of the safety risk management process discussed in Chapter 5. The safety target value may at one point 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 target value must, in this case, reflect an improvement with respect to its associated safety indicator value to be valid in the changed environment.

Safety indicator value	Safety target value
1. <i>[Number]</i> CFIT approach and landing accidents per <i>[number]</i> departures	1. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> CFIT approach and landing accidents per <i>[number]</i> operations
2. <i>[Number]</i> runway excursions per <i>[number]</i> operations	2. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> runway excursions per <i>[number]</i> operations
3. <i>[Number]</i> ground collision accidents per year on a <i>[x-year]</i> rolling average	3. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> ground collision accidents per year on a <i>[x-year]</i> rolling average
4. <i>[Number]</i> high-severity events captured through the State MOR yearly	4. Minimum of <i>[number]</i> high-severity events captured through the State MOR yearly
5. <i>[Number]</i> inspections of operators completed quarterly	5. Minimum of <i>[number]</i> inspections of operators completed quarterly
6. <i>[Number]</i> AIS facilities with QMS implemented	6. <i>[Number]</i> AIS facilities with QMS implemented by <i>[time]</i>
7. Electronic filing of differences completed within <i>[number]</i> months/weeks	7. Electronic filing of differences completed within <i>[revised number]</i> months/weeks

Figure 6-2. An example of safety indicator values and safety target values based on safety measurement

Safety indicator value	Safety target value
1. <i>[Number]</i> level busts per <i>[number]</i> operations	1. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> level busts per <i>[number]</i> operations by <i>[date]</i>
2. <i>[Number]</i> Cat B and C runway incursions at 5 international <i>[State]</i> airports per <i>[number]</i> operations	2. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> Cat B and C runway incursions at 5 international <i>[State]</i> airports by <i>[date]</i>
3. <i>[Number]</i> TCAS/airprox events per <i>[number]</i> operations	3. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> TCAS/airprox events per <i>[number]</i> operations by <i>[date]</i>
4. <i>[Number]</i> non-conforming approaches (NCA) at 5 international <i>[State]</i> airports per <i>[number]</i> operations	4. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> non-conforming approaches (NCA) at 5 international <i>[State]</i> airports by <i>[date]</i>
5. <i>[Number]</i> apron FOD events at 5 international <i>[State]</i> airports per <i>[number]</i> operations	5. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> apron FOD events at 5 international <i>[State]</i> airports by <i>[date]</i>

Figure 6-3. An example of safety indicator values and safety target values based on safety performance measurement

6.4.19 ALoS is delivered through action plans. These are the tools and means needed to achieve the safety target values of ALoS related to an SSP. Action plans include the operational procedures, technology, systems and programmes to which measures of reliability, availability, performance and/or accuracy can be specified. An example of an action plan for a safety target related to reduction in controlled flight into terrain (CFIT) accidents would be the implementation of constant descent arrival procedures, and arrival procedures charts designed for stabilized approaches. An example of an action plan for a safety target related to reduction in runway incursion events would be deployment of a radar system with an expected 98 per cent availability of critical equipment.

6.4.20 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 implementation of the SSP. Therefore, reference must be always made to the acceptable level of safety related to an SSP. The safety indicator values and safety target values 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 foundation of safety management. By selecting a combination of measurable operational performance outcomes, which are State-specific and which build upon the foundation provided by regulatory compliance, the real effectiveness and efficiency of the safety management processes underlying an SSP can be assured.

6.4.21 The implementation of an ALoS goes above and beyond regulatory compliance with national and international requirements. Establishing an ALoS for an 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.

6.4.22 As a conclusion to the discussion on ALoS, Figures 6-4, 6-5 and 6-6 summarize, in graphical format, the transition from initial to mature ALoS related to an SSP, ALoS reflecting safety measurement, and ALoS reflecting safety performance measurement of the related SMSs, as discussed in this section.

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 service 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:

- a) identify safety hazards;
- b) ensure the implementation of remedial action necessary to maintain agreed safety performance;
- c) provide for continuous monitoring and regular assessment of the safety performance; and
- d) aim at 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:

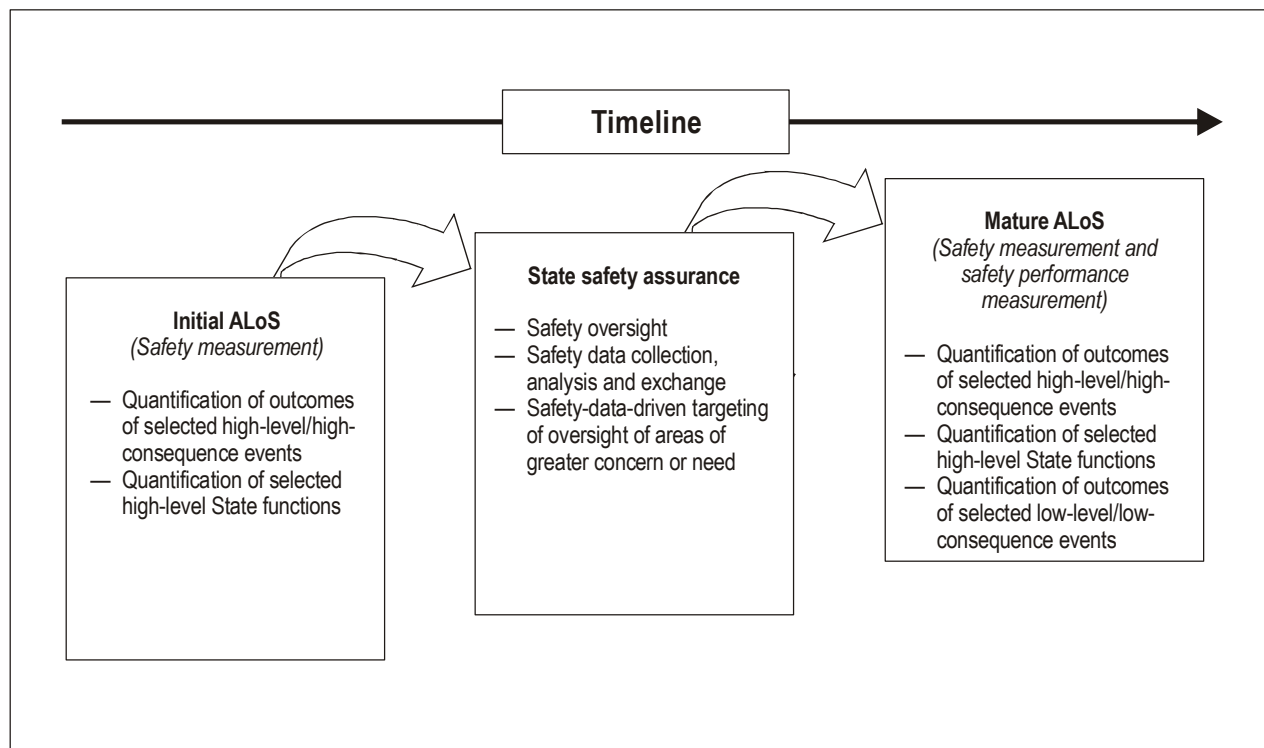


Figure 6-4. Transition from initial to mature ALoS related to an SSP

- a) finding out what 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 an 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 an 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's 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 in the effective operation of an SMS as well as progressing towards a performance-based regulatory environment. It assists in monitoring actual performance of the SMS, and in avoiding just simply "ticking the appropriate boxes". 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 the level of design expectations. These measurable performance outcomes permit the actual performance of activities critical to safety to be assessed against existing organizational controls so that necessary corrective action is taken and safety risks 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 the 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 be achieved.

6.6.4 The safety performance of an SMS is not related to the quantification of high-consequence outcomes (safety measurement) but rather to the quantification of low-consequence processes (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 the 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 conduct 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 the safety performance of the SMS, that 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 about the safety of the aviation industry.

6.6.5 Within each State, the safety performance of each SMS will be agreed separately between the State and individual aviation organizations. Agreed safety performance should be commensurate with the complexity of an individual aviation organization's specific operational contexts, and the availability of an aviation organization's resources to address them. In practice, the safety performance of an SMS is expressed by safety performance indicator values and safety performance target values and is implemented through action plans.

6.6.6 The safety performance indicator values are short-term, 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 indicator values reflect safety performance measurement exclusively. The safety performance indicator values of an SMS should not reflect safety measurement. Since the safety performance of each SMS will be agreed separately between the State and individual aviation organizations, the safety performance indicator values will therefore differ between segments of the aviation industry, such as aircraft operators, certified aerodrome operators and ATS providers. An example is provided.

6.6.7 Through its SMS, a certified aerodrome operator has identified safety concerns regarding foreign object debris (FOD) in ramp operations. It has also identified safety concerns regarding traffic of unauthorized vehicles on taxiways. It therefore defines the following safety performance indicator values, 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 indicator values fulfil the conditions discussed in 6.6.6: they are expressed in numerical terms; they are obvious, measurable and linked to the safety concerns of the aerodrome SMS. Furthermore, both safety performance indicators reflect safety performance measurement.

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

Safety target values	<ol style="list-style-type: none"> 1. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> CFIT and approach and landing accidents per <i>[number]</i> departures. 2. Minimum of <i>[number]</i> inspections of operators completed quarterly. 3. ...
Action plans	<ol style="list-style-type: none"> 1. CFIT training package distributed to industry and supported by training courses. 2. Revision and, if necessary, update of hiring policy. Inspection manual updated. 3. ...
Safety indicator values	<ol style="list-style-type: none"> 1. <i>[Number]</i> CFIT and approach and landing accidents per <i>[number]</i> departures. 2. <i>[Number]</i> inspections of operators completed quarterly. 3. ...
State	Will comply with all applicable international Standards.

Figure 6-5. ALoS reflecting safety measurement

Safety target values	<ol style="list-style-type: none"> 1. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> non-conforming approaches (NCA) at 5 international airports per <i>[number]</i> arrivals by <i>[date]</i>. 2. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> Cat B and C runway incursions at 5 international <i>[State]</i> airports per <i>[number]</i> operations by <i>[date]</i>. 3. ...
Action plans	<ol style="list-style-type: none"> 1. Constant descent arrival (CDA) procedures implemented. Arrival procedures charts designed for stabilized approaches. 2. Installation of ASDE/X at 5 international <i>[State]</i> airports. 3. ...
Safety indicator values	<ol style="list-style-type: none"> 1. <i>[Number]</i> non-conforming approaches (NCA) at 5 international airports per <i>[number]</i> operations. 2. <i>[Number]</i> Cat B and C runway incursions at 5 international <i>[State]</i> airports per <i>[number]</i> operations. 3. ...
State	Will comply with all applicable international Standards.

Figure 6-6. ALoS reflecting safety performance measurement

6.6.9 Continuing with the example discussed in 6.6.7, the aerodrome defines the following safety performance target values, following agreement with the State's civil aviation oversight authority: by January 2009, reduce FOD events in the apron to 8 per 10 000 operations, and maintain 20 events of unauthorized vehicles on the taxiways per 10 000 operations. These safety performance target values fulfil the conditions discussed in 6.6.6: they are expressed in numerical terms; they are obvious, measurable and linked to the safety performance indicators of the aerodrome SMS. Furthermore, both safety performance target values reflect safety performance measurement.

6.6.10 Action plans are the tools and means needed to achieve the safety performance indicator values and safety performance target values 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 an action plan to achieve the safety performance indicator values and safety performance target values of an SMS discussed above would be as follows: implement a thrice-daily walk-in ramp inspection programme, develop and implement a training course for drivers and install (aerodrome-specific) taxiway signage.

6.6.11 The safety performance indicator values and safety performance target values 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 indicator values and safety performance target values 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 value into a more demanding safety performance target value. Second, consideration must be given to how expensive the action plans deemed necessary to change the value of the safety performance indicator into a more demanding value of the safety performance target are. Third, and most importantly, consideration must be given to whether the assessment of the safety risks of the consequences 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 indicator value and the safety performance target value remain the same. The safety performance indicator value 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 value must in this case be turned into a more demanding target value to be valid in the changed environment.

6.6.12 A range of different safety performance indicators and safety performance targets will provide a better insight into 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.

6.6.13 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 at those aerodromes of the network served by non-precision approaches. It therefore defines the following safety performance indicator value, following agreement with the State's civil aviation oversight authority: 10 unstable (or non-conforming) approaches per 1 000 landing operations at aerodromes of the network served by non-precision approaches. Subsequently, the aircraft operator defines the following safety performance target value, following agreement with the State's civil aviation oversight authority: within the next three years, reduce by fifty per cent the number of unstable (or non-conforming) approaches per 1 000 landing operations at aerodromes of the network served by non-precision approaches. The action plan to achieve the safety performance indicator value and the safety performance target value discussed above would be as follows: development of constant descent angle (CDA) GPS approaches at aerodromes of the network served by non-precision approaches.

6.6.14 An 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 has defined the following safety performance indicator value: 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 value: by 2010 reduce Cat A and B (most serious) runway incursions to a rate of not more than 0.5 per million operations.

6.6.15 The safety performance of an SMS should be defined, to the extent possible, through quantitative safety performance indicators and safety performance targets. It is recognized, however, that in many States the safety data collection and analysis capabilities of services providers may not be fully developed. Therefore, while such capabilities are developed, the safety performance of an SMS can be defined through a combination of quantitative and qualitative safety performance indicators and safety performance targets. The objective should nevertheless remain the definition of safety performance of an SMS through quantitative measures only.

6.6.16 The definition of the 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.

6.7 MANAGEMENT ACCOUNTABILITY

6.7.1 The third and last group in the ICAO safety management SARPs in Annexes 1, 6, 8, 11, 13 and 14 is management accountability vis-à-vis the management of safety during the provision of services. The ICAO SARPs dictate that an accepted safety management system shall clearly define the 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 service 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, of a language issue: the use of the term accountability in the ICAO safety management requirements. In the English language, the notion of accountability is different from the notion of responsibility. Responsibility refers to the situation where a person must execute specific actions, while accountability extends this to the obligation or willingness to assume responsibility for the execution of such actions. To express it in safety management terms, safety responsibilities describe the safety purpose of the duties an individual is required to deliver. 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 difference that exists only in the English language. Therefore, the term responsibility, with regard 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 RELATIONSHIP BETWEEN AN SSP AND AN SMS

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 of their SSP, to accept and oversee the development,

implementation and operational performance of the service provider's SMS. In overseeing the safety performance of a service provider's SMS, the notion of ALoS of an SSP, discussed in 6.4, plays a fundamental role in the relationship between an SSP and an SMS. The relationship between an SSP and an SMS is illustrated in Figure 6-7, and is further discussed in Chapter 11.

6.8.2 Chapter 3 discusses a potential management dilemma that may arise from the perspective that considers 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 In Figure 6-7, the SSP is situated on the protection side of the balance mediating between protection and production. The SSP aims at ensuring public safety by controlling safety risks at the State level. An SSP has no production objectives as such. Although efficiency is expected from the 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 the 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.

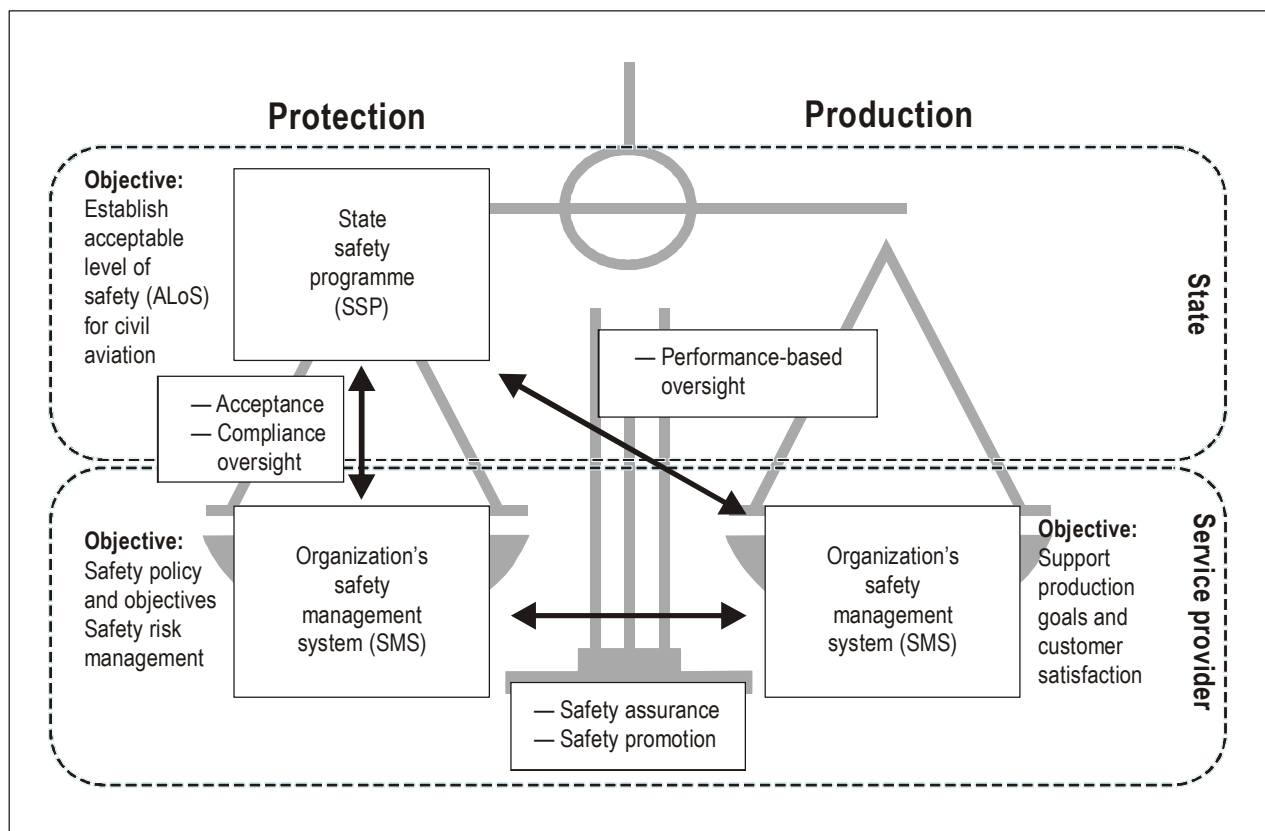


Figure 6-7. Relationship between an SSP and an SMS

6.8.4 The service provider's SMS is only partly situated on the protection side of the balance. 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's SMS is, in terms of protection, the control of safety risks that are a consequence of activities and processes related to the delivery of the products or services that the organization specializes 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, yet important, role.

6.8.5 The State, as part of its SSP, initially accepts a service provider's 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's SMS comply with the 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 of action for its development and implementation. In simple language, acceptance means mostly "ticking the appropriate boxes". But acceptance, while ensuring regulatory compliance, does not guarantee proper SMS performance. Acceptance and compliance oversight are indicated by the vertical arrow linking the SSP and the SMS in Figure 6-7. The way for the State to ensure proper SMS performance (i.e. that the SMS really works) is 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 reason for the safety performance indicators and safety performance targets of an SMS. While acceptance and compliance oversight as discussed in 6.8.5 are prescriptive-based, oversight of safety performance indicators and targets is performance-based. The notion of safety performance discussed in section 6.6 thus extends, to a service provider's 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 action plans. These key, agreed indicators and targets are representative of the generic hazards in the operational context in which the service provider 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 prioritized set of short-term and medium-term safety objectives specific to the particular service provider's 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 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 6-7, 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 utilizes 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's 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 are 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, as it pertains to the acceptance of the SMS and its administrative oversight in terms of regulatory compliance, is represented in the protection side, in an 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 when 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 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 the safety performance of the SMS as a whole, will become obvious: lack of resources will lead either to non-identification of safety hazards or to flawed safety risk management and, consequently, to poor safety performance of the SMS. In such a case, although perhaps regulatory-compliant, the service provider's SMS will not be effective. In Figure 6-7, performance-based acceptance and oversight are represented by the diagonal arrow linking the SSP and the organization's production processes.

6.9 COMPLIANCE AND PERFORMANCE

6.9.1 There is growing conviction within aviation about the need to complement the existing compliance-based approach to safety with a performance-based approach, with a view to achieving a realistic implementation of safety management practices through 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 and this chapter. In a compliance-based safety environment, safety regulations are used as administrative controls. A strict regulatory 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 is implemented in which regulations are developed to respond to and control safety risks, and oversight of compliance with the regulatory framework is supported by data-based identification and prioritization of safety risks, with two objectives: regulatory compliance, but most importantly, verification of effective safety performance.

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

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

6.9.7 Safety indicators and safety targets, and safety performance indicators and safety performance targets provide a measurable way of ensuring and demonstrating the effectiveness of an SSP or an SMS respectively, beyond regulatory compliance. Regulatory compliance still remains at the foundation of safety management for the State as well as for service providers. Figures 6-8 and 6-9 build upon the examples of safety indicators and safety targets, safety performance indicators, safety performance targets, and action plans of an SSP and an SMS respectively, discussed in this chapter, to illustrate where and how prescription and performance fit within an SSP and an SMS.

Performance

Safety target values	<ol style="list-style-type: none"> 1. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> non-conforming approaches (NCA) at 5 international airports per <i>[number]</i> arrivals by <i>[date]</i>. 2. Reduce by <i>[number]</i> the number of / Maximum of <i>[number]</i> Cat B and C runway incursions at 5 international <i>[State]</i> airports per <i>[number]</i> operations by <i>[date]</i>. 3. ...
Action plans	<ol style="list-style-type: none"> 1. Constant descent arrival (CDA) procedures implemented. Arrival procedures charts designed for stabilized approaches. 2. Installation of ASDE/X at 5 international <i>[State]</i> airports. 3. ...
Safety indicator values	<ol style="list-style-type: none"> 1. <i>[Number]</i> non-conforming approaches (NCA) at 5 international airports per <i>[number]</i> operations. 2. <i>[Number]</i> Cat B and C runway incursions at 5 international <i>[State]</i> airports per <i>[number]</i> operations. 3. ...

Prescription

State	Will comply with all applicable international Standards.
-------	--

Figure 6-8. SSP — Prescription combined with performance

6.9.8 In summary, in accordance with the ICAO harmonized safety management SARPs:

- a) States shall establish a State safety programme (SSP), in order to achieve an acceptable level of safety (ALoS) in civil aviation.
- b) The acceptable level of safety (ALoS) to be achieved shall be established by the State.
- c) Service providers shall implement a safety management system (SMS) that:
 - 1) identifies safety hazards;
 - 2) ensures remedial action to maintain safety performance;
 - 3) provides continuous monitoring and regular assessment of the safety performance; and
 - 4) aims at continuous improvement of the overall performance of the SMS.

Performance

Safety target values	<ol style="list-style-type: none"> 1. <i>[Number]</i> events of unauthorized vehicles on the taxiways per <i>[number]</i> operations at 5 <i>[State]</i> international airports by <i>[date]</i>. 2. <i>[Number]</i> of FOD events on the apron per <i>[number]</i> operations. 3. ...
Action plans	<ol style="list-style-type: none"> 1. Training course for drivers/installation of specific signage. 2. Thrice-daily walk-in ramp inspection programme. 3. ...
Safety indicator values	<ol style="list-style-type: none"> 1. <i>[Number]</i> events of unauthorized vehicles on the taxiways at 5 <i>[State]</i> international airports. 2. <i>[Number]</i> FOD events on the apron at 5 <i>[State]</i> international airports. 3. ...

Prescription

State	Will comply with all applicable international Standards.
-------	--

Figure 6-9. SMS — Prescription combined with performance

Chapter 7

INTRODUCTION TO SAFETY MANAGEMENT SYSTEMS (SMS)

7.1 OBJECTIVE AND CONTENTS

This chapter describes the basic features of safety management 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 discusses the relationship between SMS and quality management systems (QMS). The chapter includes the following topics:

- a) Introductory concepts;
- b) SMS features;
- c) System description;
- d) Gap analysis;
- e) SMS and QMS;
- f) SSP/SMS and the accident investigation process;
- g) Integration of management systems;
- h) Clarifying terms; and
- i) The difference between safety slogans and safety principles.

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 in order to be able to control the safety risks of the consequences of the hazards it must face during the delivery of the services for which the organization is in business. In many cases the organization itself generates the hazards during service delivery. It is important to acknowledge that an SMS itself is neither a tool nor a process. An SMS is the 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 to provide a toolbox that is appropriate, in size and complexity, to the size and complexity of the organization.

7.2.2 As a toolbox (Figure 7-1), an 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;



Figure 7-1. SMS — A toolbox

- b) the tools and task are properly related;
- c) the tools are commensurate with 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 an 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, an 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 of an airline), that might generate hazards. Safety management addresses all of the operational activities of the entire organization. The scope of an SMS 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 to service delivery, other organizational activities that support operational activities, such as finance, human resources and legal, as discussed in Chapter 3.

7.2.4 An SMS must start with 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 resources, just like any other core business function. 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 apprised of the role and objectives of the organization's SMS, or involved at an appropriate level in the organization's SMS, it will not have an appreciation of the extent of the threat that safety risks represent to the capabilities of the organization. Without such an 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 An SMS aims to make continuous improvements to the overall level of safety of an organization. In accordance with the nature of safety management as a core business function, an SMS involves non-stop, daily hazard identification, collection and analysis, safety risk estimation, and implementation of mitigation strategies. There is no specific point at which an SMS stops or slows down. An SMS is a constant, never-ending operation that aims at maintaining and, if possible, improving safety levels that are commensurate with the organization's strategic objectives and supporting core business functions. In this sense, an SMS is profoundly different from the traditional notion of accident investigation, which waited for an accident to occur, then extracted and distributed as many safety lessons as possible learned from the investigation in order to prevent similar accidents. An SMS actively looks for hazards, continuously assesses safety risks, to contain them before they result in an accident.

7.2.6 All aviation stakeholders play a role in SMS and, again, for very concrete reasons. It is important to identify and involve aviation system stakeholders to ensure that their input and knowledge relevant to safety risk decisions are taken into consideration before such decisions are taken.

7.2.7 Furthermore, given the broad-ranging nature of SMS activities, input from multiple sectors to the safety risk decision-making process is essential. The following is a list of stakeholders that may be called upon to assist in, or provide input to, the decision-making process on safety risks:

- a) aviation professionals;
- b) aircraft owners and operators;
- c) manufacturers;
- d) aviation regulatory authorities;
- e) industry trade associations;
- f) regional air traffic service providers;
- g) professional associations and federations;
- h) international aviation organizations;
- i) investigative agencies; and
- j) the flying public.

7.2.8 Stakeholders can assist organizational decision makers by ensuring that communication about the safety risks 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 characterize an SMS. It is:

- 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 of hazards under control is developed, approved, implemented and operated on a non-stop, daily basis. As a consequence of their systematic and strategic nature, SMS activities aim at gradual but constant improvement, as opposed to instant dramatic change. The systematic nature of an 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 an 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 in 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 an adverse event is experienced, and then reverting to “sleep mode” until the next adverse event is experienced and repair action is re-engaged. In order to sustain effective hazard identification, constant monitoring is conducted of operational activities necessary for the provision of services. This in turn allows for the 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 worse, 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. 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 between 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 activities. Potential safety vulnerabilities as a consequence of the interactions between people and other components of the operational context can specifically be characterized 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 with 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, is a hazard. While it is stored in underground tanks, untouched, the damaging potential of fuel as a hazard 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 a first and essential step, on the system description.

7.4.3 The example used in Chapter 2 to explain the interrelationship between 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 the service delivery, the tools and means that they will utilize, and the features of the environment constitute 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 characterized 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 activities, the first step in identifying such mismatches is to describe the system in terms of its components and their interactions.

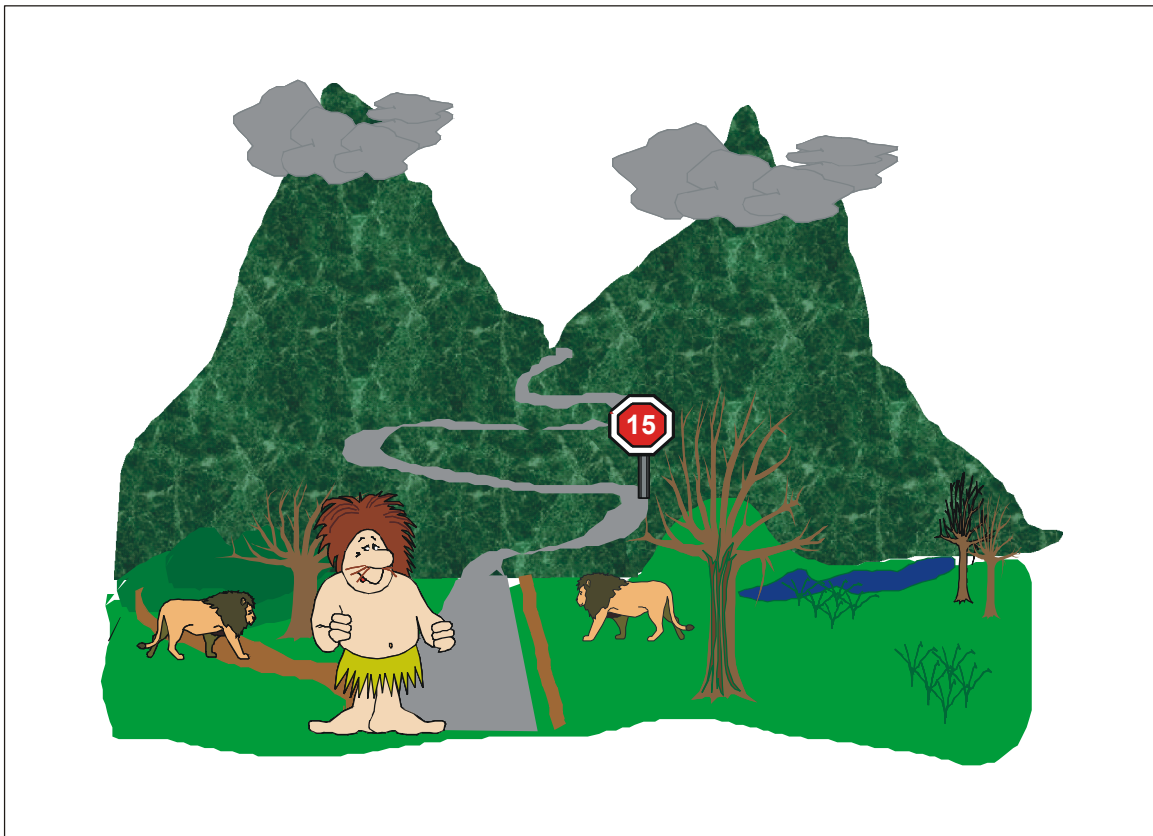


Figure 7-2. System description

7.4.5 A description of this system in term of its components and their interactions, utilizing the SHELL model discussed in Chapter 2, 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 of 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 to the other side of the mountain).

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

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

7.4.7 Appendix 1 to this chapter provides guidance on 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 these safety vulnerabilities, specified as hazards in the interfaces between people and other components of the system, through an analysis of the resources already present in the system. The analysis has two objectives. The first objective is to identify eventual mismatches in the interfaces between the different components identified through the system description. These mismatches are the safety vulnerabilities. The second objective is to identify whatever additional resources might be considered necessary to smooth rough interfaces, to assist people involved in the delivery of services in safely and efficiently discharging their tasks. This analysis is known as gap analysis.

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

7.5.3 Returning to Figure 7-2, and keeping in mind that the service provided by the system is the delivery, by people, of small packages to the other side of the mountains, 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 this question must address both safety (i.e. are personnel properly equipped to deliver the service safely?) and efficiency (i.e. are personnel properly equipped to deliver the service efficiently?).

7.5.4 The SHEL model, discussed in Chapter 2, is a useful tool to reply to the question and guide the gap analysis (see Figure 7-3). The caveman is the Liveware (L). The road, the STOP sign, 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 the caveman 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:

- a) The caveman must travel through the mountains, on 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).
- b) 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 the caveman (L) and the clouds (E).

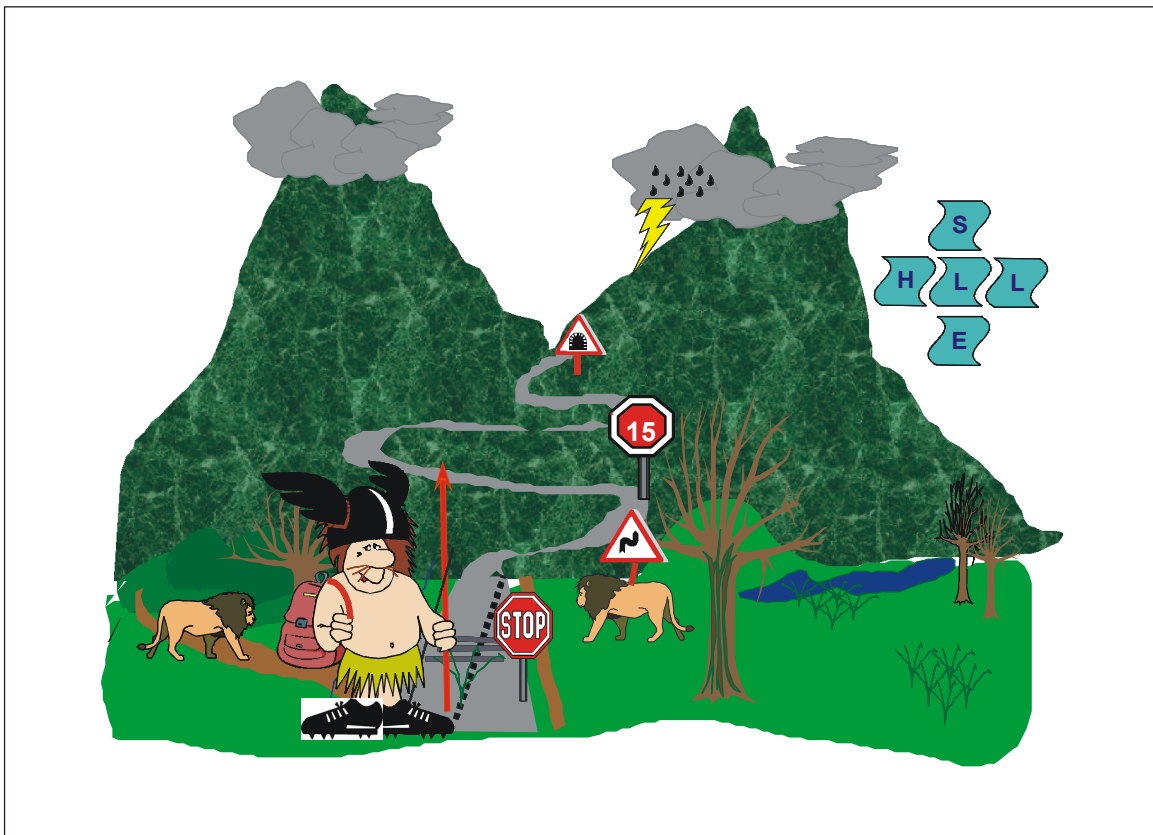


Figure 7-3. Gap analysis

- c) 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. Providing a spear for the caveman would therefore address a mismatch between the caveman (L) and the lions (E).
- d) In addition to the STOP sign, yellow “hold” lines painted on 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).
- 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 on 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).
- f) There is a speed sign that indirectly alerts travellers at the beginning of the winding road. The speed sign does not convey an unequivocal message about the upcoming road conditions. A dedicated and obvious alerting sign would be an additional resource to address a mismatch in the interface between the caveman (L) and the road (E).
- g) There is no warning that the pass at the top of the mountain is through a tunnel. An alerting sign would be an additional resource to address a mismatch in the interface between the caveman (L) and the road (E).

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 the 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 once 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 itself, 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 in ensuring the necessary standardization of processes to achieve the overarching objective of managing the safety risks of the consequences of the hazards the organization must confront during its 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 are nurtured by quality principles, the potential for misperceptions and misunderstandings about the relationship between SMS and QMS is real. It is thus essential to define this relationship from a synergistic rather than an 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 consequences of the 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 the understanding of human performance, organizational factors and their impact on 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 an end in themselves: the objective of hanging a banner with an ISO accreditation at the entrance of a corporate headquarters may distract the organization 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:

- a) SMS focuses on the safety, human and organizational aspects of an organization (i.e. safety satisfaction); while
- b) QMS focuses on the products and services 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:

- a) SMS builds partly upon QMS principles;
- b) SMS should include both safety and quality policies and practices; and
- c) 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 the complementary contributions of each system to the attainment of the organization's safety goals:

- a) SMS results in the design and implementation of organizational processes and procedures to identify safety hazards and their consequences and bring the associated safety risks in aviation operations under the control of the organization;
- b) 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 the 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 SARPs included in Annexes 1, 6, 8, 11 and 14 and discussed in Chapter 6 are limited to SMS. There are no ICAO requirements in the aforementioned Annexes with regard to QMS, with the sole exception of 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 As with the relationship between SMS and QMS, the relationship between the SSP or the 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 focused on the relationship between the 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 complementarity and synergy. Accident investigation is an essential tool of the 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 the organization's SMS. An accident (or serious incident) represents the ultimate failure of the SSP or the SMS (or both), as the managerial systems guiding the activities necessary for managing safety in a State or in an organization respectively. When such ultimate failure occurs, the accident investigation process is set in motion to find out the reasons for the failure of the safety management activities, and to generate the necessary countermeasures so failure is not repeated. Thus, in a safety management environment, the accident investigation process has a distinct role. It is the ultimate custodian of safety in the aviation system, which deploys when all safety defences, barriers, checks and counterbalances in the system have failed.

7.8 INTEGRATION OF MANAGEMENT SYSTEMS

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:

- a) quality management system (QMS);
- b) environment management system (EMS);
- c) occupational health and safety management system (OHSMS);
- d) safety management system (SMS); and
- e) 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 to such integration:

- a) reduction of duplication and therefore of costs;
- b) reduction of overall organizational risks and an increase in 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 organization. Aviation organizations should be encouraged to integrate their quality, safety, security, occupational health and safety, and environmental protection management systems. This integration, however, is presently beyond the scope of the harmonized ICAO safety management SARPs and of this manual.

7.9 CLARIFYING TERMS

It is important to develop a common understanding of the terminology used in relation to the different safety management activities carried out under the responsibility of service providers and/or the civil aviation oversight authorities. When the following terms are used in this manual, they have the following meanings:

- a) **Safety oversight** is what the State performs with regard to the SMS of the operators/service providers;
- b) **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
- c) **Safety audit** is what the State performs with regard to the structure of its SSP and the operators and 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 THE DIFFERENCE BETWEEN SAFETY SLOGANS AND SAFETY PRINCIPLES

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 enunciates precise guidance which is based on sound knowledge and provides all-encompassing statements on how to conduct a particular endeavour. The former articulates oblique references which are 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 an SSP/SMS based on "sloganeering". However, the potential does exist. This section reviews and sets forth to discredit, mostly by applying the basic safety and safety management concepts discussed in Chapters 2 and 3, five of aviation's most cherished safety slogans:

- a) In aviation, safety is first.
- b) Safety is everybody's responsibility.
- c) If ain't broke, why fix it?
- d) If you believe safety is expensive, try an accident.
- e) Seventy per cent of 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, in the case of 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, coordinated prioritization of production and protection goals, so that aviation organizations 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 dysfunctional organizations when caught by adverse events is that, notwithstanding evidence to the contrary, they cannot 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.

7.10.3 ***Safety is everybody's responsibility.*** This slogan is a puzzling one. When one feels sick; one visits a physician. When one needs legal counsel, one consults an attorney. If water does not come out of the faucet, one calls the plumber. However, when facing safety problems, everyone in aviation presumes to be subject-matter experts, particularly if they have some years of experience in the trade. The truth is that 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 unmanaged hazards and safety problems, but work on the documentation and description of the problems, as a prerequisite for the development of solutions. Chapter 8 develops these ideas in some depth.

7.10.4 ***If it ain't broke, why fix it?*** This slogan proposes 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 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 an 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 undertaking remedial action only after experiencing an accident are inevitably high, there are compelling economic and ethical reasons to fix the system before it breaks.

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 behaviour, 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. Once state-of-the-art structures and processes are in place, accidents, like illness and death, become ultimately a matter of statistical chance. While it is possible, and sensible, to perform proactive checks of system performance and engage in proactive endeavours, similar to the way humans visit family physicians and engage in fitness programmes, it is impossible to eliminate all hazards. 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. An efficient organization, manned by qualified personnel, equipped with resources commensurate with its production goals and with well-designed procedures can still have an accident, while a mismanaged, seriously under-resourced organization, with doubtfully-qualified personnel, substandard practices and a record of close-calls may manage to avoid an accident simply because of luck.

7.10.6 **Seventy per cent of accidents are caused by human error.** This slogan has been saved for the end because it epitomizes how misleading safety slogans can be. Consider the aviation system: humans conceive the blueprint of the system and, once they are satisfied with what they have 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 behaviour necessary to achieve the system's objectives, humans train other humans who 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 due to human error. From this perspective and depending upon the level of observation, one hundred per cent of accidents are arguably caused by human error.

Appendix 1 to Chapter 7

GUIDANCE ON SYSTEM DESCRIPTION

1. INTRODUCTION

1.1 A system description is the first prerequisite for the development of an SMS in an organization. Every system contains inherent potential safety vulnerabilities, which are characterized in terms of hazards. The hazard identification process can identify only 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 within the system, as well as the interfaces with the larger systems of which the system being assessed is a part.

1.2 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.

1.3 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 of an aerodrome is detailed below.

2. 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

1.1 Movement area access control

- a) Air
- b) Land
- c) Sea

- 1.2 Aerodrome emergency planning
 - a) Emergency procedures manual
 - b) Emergency simulation practices
- 1.3 Rescue and fire fighting
 - a) Capability
 - 1) Equipment
 - 2) Foam/water/dry powder discharge rate
 - b) Facility maintenance
 - c) Staff training and experience
 - d) Equipment mobilization plan
 - e) Reduction of capability (notice)
 - f) Water hydrant system
- 1.4 Movement area inspection and maintenance
 - a) Aerodrome manual
 - b) Inspection forms
 - c) Maintenance
- 1.5 Visual aids maintenance
 - a) Inspections
 - b) Schedule
- 1.6 Construction management
 - a) Control of works
 - b) Site management
- 1.7 Apron safety management, including vehicle traffic
 - a) Rules and regulation for airside operations
 - b) Airside management
 - 1) Airside vehicle management
 - 2) Airside vehicle licence
 - 3) Vehicle examination
 - 4) Safety specification
 - 5) Aircraft servicing coordination
 - c) Equipment parking
 - d) Apron discipline
 - e) Push-back operations
 - f) Traffic signs and markings
 - g) Stand allocation
 - h) Aircraft damage control
 - i) Fuel spillage control
 - j) Vehicle and equipment damage control
 - k) Apron safety checklists including ramp activity audit
 - l) Contracted and subcontracted activities

-
- 1.8 Wildlife hazard management
 - a) Bird control management
 - b) Observation
 - c) Bird strike report management
 - 1.9 Obstacle control
 - a) Airport boundary
 - b) Outside the airport
 - c) Runway strip
 - d) Regulation and survey
 - e) Approval of building construction under the flight path
 - 1.10 Disabled aircraft removal
 - a) Equipment compatible with aircraft type
 - b) Maintenance for readiness
 - c) Deployment scheme
 - d) Establishment of outsourcing procedures/contact
 - 1.11 Dangerous goods handling
 - a) Limitation of dangerous goods on aircraft
 - b) Storage and loading
 - c) Establishment of training programmes
 - d) Acceptance of dangerous goods by operators
 - e) Emergency response guidance for aircraft incidents involving dangerous goods
 - 1.12 Low visibility and adverse weather operations
 - a) Procedures
 - b) Coordination with air traffic services
 - c) Responsibility of organizations involved
 - 1.13 Radio navigation aids installations and maintenance
 - a) NOTAMS
 - 2. Aerodrome management
 - 2.1 Slots negotiation and allocation
 - 2.2 Flight dispatch
 - 2.3 Follow-me guidance and marshalling
 - 2.4 Movement area management and stand allocation
 - 2.5 Low visibility operations CAT II and CAT III
 - 2.6 Control of traffic rules and licensing regulations
 - 2.7 Cleaning, waste removal and pest control
 - 3. Passenger/terminal building management
 - 3.1 Management of passengers, baggage flow and facilities

- 3.2 Passengers and public information
 - 3.3 VIP and CIP assistance
 - 3.4 Left luggage
 - 3.5 Porter assistance
 - 3.6 Trolley management
 - 3.7 Cleaning and pest control
4. Air traffic and aeronautical information and communications services
- 4.1 Air traffic control (aerodrome control under low visibility operations)
 - 4.2 Flight information and alerting services
 - 4.3 Aeronautical information services (international NOTAM office and pre-flight information service)
 - 4.4 Aeronautical telecommunications services
5. Safety and security management
- 5.1 Implementation and monitoring of the SMS
 - a) Safety manager
 - b) Hazard identification and assessment of the consequences
 - c) Risks assessment, control and mitigation
 - d) Safety assurance
 - e) Safety action groups
 - f) Safety management systems manual (SMSM)
 - 5.2 Implementation and monitoring of the security programme
 - 5.3 Implementation and monitoring of the aerodrome emergency plan (AEP)
 - 5.4 Processing of 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

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 service providers and certified aerodromes, as applicable.

1. GAP ANALYSIS

1.1 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 of the service provider.

1.2 The gap analysis 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.

2. 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.

3. SMS GAP ANALYSIS FOR SERVICE PROVIDERS

The gap analysis checklist that follows 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 service provider’s system.

<i>ICAO reference</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
Component 1 — SAFETY POLICY AND OBJECTIVES			
Element 1.1 — Management commitment and responsibility			
Chapter 8	Is there a safety policy in place?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 3 and 8	Does the safety policy reflect organizational commitments regarding safety management?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 3 and 8	Does the safety policy include the safety reporting procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the safety policy clearly indicate which types of operational behaviours are unacceptable?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the safety policy include the conditions under which disciplinary action would not apply?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is the safety policy signed by the Accountable Executive?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is the safety policy communicated, with visible endorsement, throughout the [organization]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is the safety policy periodically reviewed to ensure it remains relevant and appropriate to the [organization]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is there a formal process to develop a coherent set of safety objectives?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Are the safety objectives linked to the safety performance indicators, safety performance targets and action plans?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Are the safety objectives publicized and distributed?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

ICAO reference	Aspect to be analysed or question to be answered	Answer	Status of implementation
Element 1.2 — Safety accountabilities			
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 and maintenance of the SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the Accountable Executive have direct responsibility for the conduct of the organization's affairs?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the Accountable Executive have final authority over operations authorized to be conducted under the operations certificate?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Are the safety responsibilities, accountabilities and authorities documented and communicated throughout the [organization]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Has the [organization] included a definition of the levels of management with authority to make decisions regarding safety risk tolerability?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 1.3 — Appointment of key safety personnel			
Chapter 8	Has the organization appointed a qualified person to manage and oversee the day-to-day operation of the SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the person overseeing the operation of the SMS fulfil the required job functions and responsibilities?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Are the safety authorities, responsibilities and accountabilities of personnel at all levels of the organization defined and documented?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 1.4 — Coordination of emergency response planning			
Chapter 8	Does the [organization] have an emergency response/contingency plan appropriate to the size, nature and complexity of the organization?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the [organization] have a process to distribute and communicate the coordination procedures to the personnel involved in such interaction?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
Element 1.5 — SMS documentation			
Chapters 4 and 8	Has the [organization] developed and does it maintain a safety library for appropriate hazard documentation and documentation management?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 4 and 8	Has the [organization] developed and does it maintain SMS documentation in paper or electronic form?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 8 and 10	Has the service provider developed an SMS implementation plan that ensures that the SMS meets the organization's safety objectives?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 8 and 10	Has the SMS implementation plan been developed by a person or a planning group which comprises an appropriate experience base?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is the SMS implementation plan endorsed by the senior management of the [organization]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is the SMS implementation plan regularly reviewed by the senior management of the [organization]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 8 and 10	Does the SMS implementation plan propose implementation of the SMS in phases?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the SMS implementation plan explicitly address the coordination between the service provider's SMS and the SMS of other organizations the [organization] must interface with during the provision of services?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Has the service provider developed a safety management systems manual (SMSM) as a key instrument for communicating the organization's approach to safety to the whole [organization]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the SMSM document all aspects of the SMS including, among others, the safety policy, objectives, procedures and individual safety accountabilities?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Does the SMSM clearly articulate the role of safety risk management as an initial design activity and the role of safety assurance as a continuous activity?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Are relevant portions of SMS-related documentation incorporated into approved documentation, such as company operations manual, maintenance control/policy manual and airport operations manual, as applicable?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 8	Is the service provider's records system in accordance with applicable regulatory requirements and industry best practices?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Component 2 — SAFETY RISK MANAGEMENT			
Element 2.1 — Hazard identification			
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 3, 4 and 9	Does the [organization] SDCPS include a combination of reactive, proactive and predictive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 3, 9 and 10	Does the [organization] have reactive processes that provide for the capture of information relevant to safety and risk management?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 9 and 10	Has the service provider developed training relevant to reactive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 9 and 10	Has the service provider developed communication relevant to reactive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is reactive reporting simple, accessible and commensurate with the size of the service provider?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 9 and 10	Are reactive reports reviewed at the appropriate level of management?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a feedback process to notify contributors that their reports have been received and to share the results of the analysis?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 9 and 10	Is there training relevant to proactive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 9 and 10	Has the service provider developed communication relevant to proactive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is proactive reporting simple, accessible and commensurate with the size of the service provider?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 9 and 10	Is there training relevant to predictive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Has the service provider developed communication relevant to predictive methods of safety data collection?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is the predictive safety data capture process commensurate with the size of the service provider?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
Element 2.2 — Safety risk assessment and mitigation			
Chapters 9 and 10	Has the [organization] developed and does it maintain a formal process that ensures analysis, assessment and control of the safety risks in the [organization] operations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 4, 9 and 10	Does the [organization] SMS documentation clearly articulate the relationship between hazards, consequences and safety risks?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 5 and 9	Is there a structured process for the analysis of the safety risks associated with the consequences of identified hazards, expressed in terms of probability and severity of occurrence?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 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)?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapters 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Component 3 — SAFETY ASSURANCE			
Element 3.1 — Safety performance monitoring and measurement			
Chapters 9 and 10	Has the [organization] implemented an internal process to verify the safety performance of the organization and to validate the effectiveness of safety risks controls?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Are the following tools included in those processes? Safety reporting systems <input type="checkbox"/> Yes <input type="checkbox"/> No Safety studies <input type="checkbox"/> Yes <input type="checkbox"/> No Safety reviews <input type="checkbox"/> Yes <input type="checkbox"/> No Safety audits <input type="checkbox"/> Yes <input type="checkbox"/> No Safety surveys <input type="checkbox"/> Yes <input type="checkbox"/> No Internal safety investigations <input type="checkbox"/> Yes <input type="checkbox"/> No		
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Are safety reports reviewed at the appropriate level of management?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a feedback process to notify contributors that their reports have been received and to share the results of the analysis?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Are corrective and preventive actions generated in response to hazard identification?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Are there procedures in place for the conduct of internal investigations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a process to ensure that occurrences and deficiencies reported are analysed to identify all associated hazards?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Does the service provider have a process for evaluating the effectiveness of the corrective/preventive measures that have been developed?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Does the service provider have a system to monitor the internal reporting process and the associated corrective actions?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
Chapter 9	Is there an audit function with the independence and authority required to carry out effective internal evaluations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Does the audit system cover all functions, activities and organizations within the service provider?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Are there selection/training processes to ensure the objectivity and competence of auditors as well as the impartiality of the audit process?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a procedure for reporting audit results and maintaining records?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a procedure outlining requirements for timely corrective and preventive action in response to audit results?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a procedure to record verification of action(s) taken and the reporting of verification results?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a process in place to monitor and analyse trends?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 3.2 — The management of change			
Chapter 9	Has the [organization] developed and does it maintain a formal process to identify changes within the organization which may affect established processes and services?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Does the formal process for the management of change analyse changes to operations or key personnel for safety risks?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Has the [organization] established arrangements to ensure safety performance prior to implementing changes?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 3.3 — Continuous improvement of the SMS			
Chapter 9	Has the [organization] developed and does it maintain a formal process to identify the causes of substandard performance of the SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Has the [organization] established a mechanism(s) to determine the implications of substandard performance of the SMS on operations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Has the organization established a mechanism(s) to eliminate or mitigate the causes of substandard performance of the SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Does the organization have a process for the proactive evaluation of facilities, equipment, documentation and procedures (through audits and surveys, etc.)?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Does the organization have a process for the proactive evaluation of an individual's performance, to verify the fulfilment of that individual's safety responsibilities?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Component 4 — SAFETY PROMOTION			
Element 4.1 — Training and education			
Chapter 9	Is there a documented process to identify training requirements so that personnel are trained and competent to perform their SMS duties?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
Chapter 9	Is the safety training appropriate to the individual's involvement in the SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is the safety training incorporated into indoctrination training upon employment?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there emergency response/contingency training for affected personnel?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a process that measures the effectiveness of training?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 4.2 — Safety communication			
Chapter 9	Are there communication processes in place within the [organization] that permit the safety management system to function effectively?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Are there communication processes (written, meetings, electronic, etc.) commensurate with the size and scope of the service provider?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is safety-critical information established and maintained in a suitable medium that provides direction regarding relevant SMS documents?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is safety-critical information disseminated throughout the [organization] and is the effectiveness of safety communication monitored?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 9	Is there a procedure that explains why particular safety actions are taken and why safety procedures are introduced or changed?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Chapter 8

SMS PLANNING

8.1 OBJECTIVE AND CONTENTS

This chapter describes the requirements associated with 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, this chapter discusses only the first component of the framework, safety policy and objectives; the other three components of the ICAO SMS framework (safety risk management, safety assurance and safety promotion) are discussed in Chapter 9. This chapter includes the following topics:

- a) The components and elements of an SMS;
- b) The ICAO SMS framework;
- c) Management commitment and responsibility;
- d) Safety accountabilities;
- e) Appointment of key safety personnel;
- f) Coordination of emergency response planning;
- g) SMS documentation; and
- h) SMS implementation plan.

8.2 THE COMPONENTS AND ELEMENTS OF AN SMS

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

- a) safety policy and objectives;
- b) safety risk management;
- c) safety assurance; and
- d) 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, ongoing activity aimed at:

- a) ensuring that the initial identification of hazards and assumptions in relation to the assessment of the consequences of safety risks, and the defences that exist in the system as a means of control, remain valid and applicable as the system evolves over time; and/or
- b) introducing 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 subprocesses, specific tasks or tools that the actual management system must engage or utilize in order to conduct the management of safety just as any other core business function or organizational process.

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

- a) management commitment and responsibility;
- b) safety accountabilities;
- c) appointment of key safety personnel;
- d) coordination of emergency response planning; and
- e) SMS documentation.

8.2.6 The safety risk management component is composed of two elements:

- a) hazard identification; and
- b) risk assessment and mitigation.

8.2.7 The safety assurance component is composed of three elements:

- a) safety performance monitoring and measurement;
- b) the management of change; and
- c) continuous improvement of the SMS.

8.2.8 The safety promotion component is composed of two elements:

- a) training and education; and
- b) safety communication.

8.3 THE ICAO SMS FRAMEWORK

Note.— Details of the ICAO SMS framework are contained in Appendix 1 to this chapter.

The four components, combined with the twelve elements discussed in section 8.2, comprise the ICAO SMS framework, intended as a principled guide for the development and implementation of a service provider's 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 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 responsibility 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:

- a) achieve the highest safety standards;
- b) observe all applicable legal requirements and international standards, and best effective practices;
- c) provide all appropriate resources;
- d) enforce safety as a primary responsibility of all managers; and
- e) ensure that the policy is understood, implemented and maintained at all levels.

8.4.3 Once developed, senior management must communicate the safety policy, with visible endorsement, 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 organizational behaviour to be measured vis-à-vis safety performance and therefore vis-à-vis 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 action plans of the SMS, discussed in Chapter 6.

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:

- a) the chief executive officer (CEO);
- b) the chairperson of the board of directors;
- c) a partner; or
- d) 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 than who the Accountable Executive should be are what 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:

- a) full authority for human resources issues;
- b) authority for major financial issues;
- c) direct responsibility for the conduct of the organization's affairs;
- d) final authority over operations under certificate; and
- e) final responsibility for all safety issues.

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, while delivering our services.

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 as a 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 such 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** that 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

8.4.7 Chapter 2 discusses the allocation of resources as a fundamental organizational process. Allocation of resources is therefore one of the primordial functions of management. Paragraph 8.4.1 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: 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 places the designated person in a position in which the person does not have the essential attributes to fulfil such a 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) discussed later 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 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 a management system for ensuring safe operations. Safe operations are unlikely unless a balanced and realistic allocation of resources between protection and production goals, which 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 materialized through the organization of the SMS itself, and particularly through one specific element of the SMS: the definition of the 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 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 person responsible for a functional unit), of the responsibilities regarding the operation of the SMS, to the appropriate extent, in addition to the specific responsibilities for the operation of the department/functional unit. Under the perspective of the management of safety as a core business function, every departmental head or person 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 persons 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 the 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.

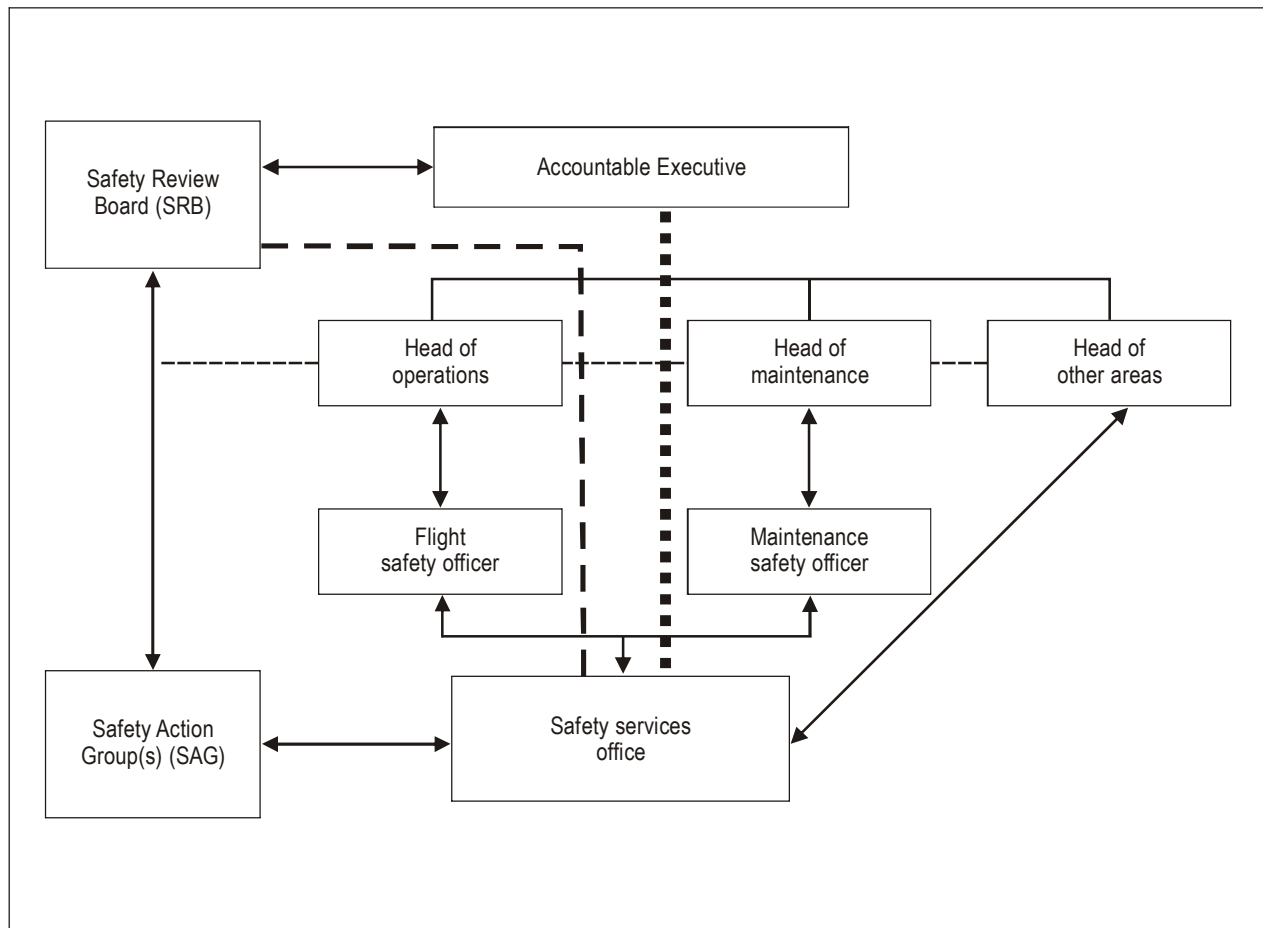


Figure 8-2. Safety accountabilities

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. This 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 The safety services office is at the heart of the functional chart. 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 in terms of the processes and decisions made regarding the delivery of services by the line managers of operational units. In an SMS environment, the safety services office fulfils four essential corporate functions:

- a) manages and oversees the hazard identification system;
- b) monitors safety performance of operational units directly involved in service delivery;

- c) advises senior management on safety management matters; and
- d) assists line managers with safety management matters.

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 the accident prevention officer, was the person in charge 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 to 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.

8.5.8 The intention behind this widespread practice was two-fold. 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 was intended to generate neutrality by removing those in charge of managing operational activities directly related to service delivery (line managers) from the assessment and resolution of safety concerns. The perspective was that there was a strong likelihood that line managers could, to varying degrees, be 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 to remove this perceived conflict of interest.

8.5.9 Clearly well-intentioned, this practice presented two serious downsides. First, by putting ownership of the safety process entirely in the safety office, it removed line managers from safety decision making. This nurtured the perception that “safety problems were the line manager’s problem; safety problems belonged to the safety office and the safety officer”. The line of accountability was effectively reduced to a two-party dialogue between the CEO and the safety officer. Given the workload of a CEO, this dialogue had all the potential to become a monologue. Second, and most importantly, it neglected the valuable input, 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 has been changed to safety services office, to reflect that it provides a service to the organization, to senior managers and to line managers, with regard to the management of safety as a core business process. The axiom “one cannot manage what one cannot measure” discussed in Chapter 3 is addressed 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 best able to design effective and efficient solutions and implement them. Furthermore, line managers can take the last step in the safety data analysis process, by turning safety information into safety intelligence and by providing a 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 are directly confronted, where deficiencies in organizational processes contribute to unleashing 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 has been delivered to the appropriate line managers, 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 managers in question, the safety services office will present new safety information about the safety

concern under consideration to the line managers of the areas to which the safety concern pertains. The safety information will indicate if the mitigation solutions implemented by the line managers have 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 are 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 resolved. Throughout this process, the line managers do not report to the safety services office, but to the Accountable Executive, as the person with final responsibility for the organization's SMS, through any of the organization's two formal safety bodies discussed in section 8.6.

8.6 APPOINTMENT OF KEY SAFETY PERSONNEL

8.6.1 Key to the effective implementation and functioning of a safety services office is the appointment of the person in charge of the daily operation of that office. This person will be identified by different names in different organizations, but for the purposes of this manual the generic term safety manager is retained.

8.6.2 The safety manager, in most organizations, will be the person to 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's functions include, but are not necessarily limited to:

- a) managing the SMS implementation plan on behalf of the Accountable Executive;
- b) performing/facilitating hazard identification and safety risk analysis;
- c) monitoring corrective actions and evaluating their results;
- d) providing periodic reports on the organization's safety performance;
- e) maintaining records and safety documentation;
- f) planning and organizing staff safety training;
- g) providing independent advice on safety matters;
- h) monitoring safety concerns in the aviation industry and their perceived impact on the organization's operations aimed at service delivery;
- i) coordinating and communicating (on behalf of the Accountable Executive) with the State's oversight authority and other State agencies as necessary on issues relating to safety; and
- j) coordinating and communicating (on behalf of the Accountable Executive) with international agencies on issues relating to safety.

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 a particular area, that safety officer will be the first point of contact for the safety manager.

8.6.4 Under normal circumstances, the safety manager accesses and/or communicates with the Accountable Executive through two channels: the Safety Action Group and, through it, the Safety Review Board, or directly through the Safety Review Board. These groups are discussed later in this chapter. In exceptional or urgent circumstances, the safety manager must have a direct emergency access to the Accountable Executive, as depicted by the dotted line connecting the respective boxes in Figure 8-2. This 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 manager is the person responsible for the collection and analysis of safety data on hazards, and the distribution, to line managers, of safety information on hazards and the safety risks of the consequences of hazards. As such, the safety manager will often be the bearer of bad news. For this reason the selection criteria for a safety manager acquires special significance and should include, but not be limited to, the following:

- a) operational management experience;
- b) technical background to understand the systems that support operations;
- c) people skills;
- d) analytical and problem-solving skills;
- e) project management skills; and
- f) oral and written communications skills.

Note.— A sample job description for a safety manager 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 directly available to line managers. Oftentimes additional resources are required, the allocation of which may not be within the authority of the line manager, 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 of senior managers, including line managers responsible for functional areas. The safety manager participates in the SRB in an advisory capacity only. The SRB is eminently strategic, deals with high-level issues in relation to policies, resource allocation and organizational performance monitoring, and meets infrequently, unless exceptional circumstances dictate otherwise. The SRB:

- a) monitors the effectiveness of the SMS implementation plan;
- b) monitors that any necessary corrective action is taken in a timely manner;
- c) monitors safety performance against the organization's safety policy and objectives;

- d) monitors the effectiveness of the organization's safety management processes which support the declared corporate priority of safety management as another core business process;
- e) monitors the effectiveness of the safety supervision of subcontracted operations;
- f) ensures that appropriate resources are allocated to achieve safety performance beyond that required by regulatory compliance; and
- g) gives strategic direction to the SAG.

8.6.8 Once a strategic direction has been developed by the SRB, concerted implementation of strategies across the organization must take place, in a coordinated manner. This is the primary role of the Safety Action Group (SAG). SAG is a high-level committee, composed of line managers and representatives of front-line personnel, and chaired in turn by designated line managers. The safety manager is the secretary of the SAG. The SAG is eminently tactical and deals with implementation issues to satisfy the strategic directives of the SRB. While the SAG deals with "grass roots" 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 those issues, to ensure consistency with the strategic direction provided by the SRB. The SAG:

- a) oversees operational safety performance within the functional areas and ensures that hazard identification and safety risk management are carried out as appropriate, with staff involvement as necessary to build up safety awareness;
- b) coordinates the resolution of mitigation strategies for the identified consequences of hazards and ensures that satisfactory arrangements exist for safety data capture and employee feedback;
- c) assesses the impact of operational changes on safety;
- d) coordinates the implementation of corrective action plans and convenes meetings or briefings as necessary to ensure that ample opportunities are available for all employees to participate fully in management for safety;
- e) ensures that corrective action is taken in a timely manner;
- f) reviews the effectiveness of previous safety recommendations; and
- g) oversees safety promotion and ensures that appropriate safety, emergency and technical training of personnel is carried out that meets or exceeds minimum regulatory requirements.

8.7 COORDINATION OF EMERGENCY RESPONSE PLANNING

8.7.1 An emergency response planning (ERP) outlines in writing what actions should be taken following an accident and who is responsible for each action. The purpose of an ERP is to ensure that there is an orderly and efficient transition from normal to emergency operations, including delegation of emergency authority and assignment of emergency responsibilities. Authorization for action by key personnel 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 the 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 airline operations overlap, it stands to reason that these plans should be compatible. The coordination of these plans should be described in the SMS manual.

8.8 SMS DOCUMENTATION

8.8.1 As discussed in Chapter 7, one explicit feature of an SMS is that all safety management activities are required to be documented and visible. It follows that documentation is an essential element of an SMS.

8.8.2 SMS documentation must include and make reference to, as appropriate, all relevant and applicable national and international regulations. It must also include SMS-specific records and documentation, such as hazard reporting forms, lines of accountability, responsibility and authority regarding the management of operational safety, and the structure of the safety management organization. It must furthermore document explicit guidelines for records 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:

- a) scope of the safety management system;
- b) safety policy and objectives;
- c) safety accountabilities;
- d) key safety personnel;
- e) documentation control procedures;
- f) coordination of emergency response planning;
- g) hazard identification and risk management schemes;
- h) safety assurance;
- i) safety performance monitoring;
- j) safety auditing;
- k) management of change;
- l) safety promotion; and
- m) contracted activities.

8.9 SMS IMPLEMENTATION PLAN

8.9.1 The SMS implementation plan defines the organization's approach to managing safety. As such, it is 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 an 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's 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 timescale.

8.9.2 Depending on the size of the organization and the complexity of its 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 be allocated resources (including time for meetings), commensurate with the task at hand.

8.9.3 Typical contents of an SMS implementation plan include:

- a) safety policy and objectives;
- b) system description;
- c) gap analysis;
- d) SMS components;
- e) safety roles and responsibilities;
- f) hazard reporting policy;
- g) means of employee involvement;
- h) safety performance measurement;
- i) safety communication;
- j) safety training; and
- k) management review of safety performance.

8.9.4 Once completed, senior management must endorse the SMS implementation plan. A typical implementation time frame for an SMS is one to four years. SMS implementation, including a phased approach, is discussed in Chapter 10, and guidance on the methodology for developing an SMS implementation plan and associated time frame is included in Appendix 2 to that chapter.

Appendix 1 to Chapter 8

FRAMEWORK FOR SAFETY MANAGEMENT SYSTEMS (SMS)

An SMS is a management tool for the management of safety by an organization. This appendix introduces a framework for the implementation and maintenance of a safety management system (SMS) by an organization. The implementation of the framework shall be commensurate with the size of the organization and the complexity of the services provided. The framework includes the following four components and twelve elements, representing the minimum requirements for SMS implementation.

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 disciplinary action would not apply. 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 risk 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. The [organization] shall develop and maintain SMS documentation describing 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 risk 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 substandard performance of the SMS, determine the implications of substandard 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.

Appendix 2 to Chapter 8

SAMPLE JOB DESCRIPTION FOR A 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 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's 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 organization's Safety Action Group (SAG) and within the safety services office (SSO).

Ambassador

- Represents the organization on government, international organization and industry committees (e.g. ICAO, IATA, CAA, AIB, etc.).

Analyst

- Analyses technical data for trends related to hazards, events and occurrences.

Process management

- Effectively utilizes applicable processes and procedures to fulfil roles and responsibilities.
- Investigates opportunities to increase the efficiency of processes.
- 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 because 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) ability to relate to all levels, both inside and outside the organization;
- g) organizational ability;

- h) ability to work unsupervised;
- i) good analytical skills;
- j) leadership skills and an authoritative approach; and
- k) worthy of respect from 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 of 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

This chapter describes the requirements associated with the operation of an SMS, using as reference the ICAO SMS framework. The first component of the ICAO SMS framework was dealt with in Chapter 8. This chapter discusses the three remaining components of the framework. The chapter includes the following topics:

- a) Safety risk management — General;
- b) Hazard identification;
- c) Risk assessment and mitigation;
- d) Safety assurance — General;
- e) Safety performance monitoring and measurement;
- f) Protection of sources of safety information;
- g) The management of change;
- h) Continuous improvement of the SMS;
- i) The relationship between safety risk management (SRM) and safety assurance (SA);
- j) Safety promotion — Training and education; and
- k) Safety promotion — Safety communication.

9.2 SAFETY RISK MANAGEMENT — GENERAL

9.2.1 An organizations manages 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 in which appropriate safety risk controls to eliminate or mitigate 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 an air 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 the system's functions as the basis for hazard identification (see Chapter 7). In the system description, the system components and their interfaces with the system's operational environment are analysed for the presence of hazards, as well as to identify those safety risk controls already existing in the system or the absence thereof (a process known as gap analysis, also discussed in Chapter 7). Hazards are analysed 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 conducted 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 the 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:

- a) **Worst case.** The most unfavourable conditions expected, e.g. extremely high levels of traffic and extreme weather disruption.
- b) **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 appendices 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 into two components — the probability of occurrence of a damaging event or condition, and the 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 definition and final construction of the matrix should be left to the service provider's organization to design, and be subject to agreement by 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 through 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 have been designed, but before the system is placed "online," an assessment must be made of whether the controls 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, utilizes auditing, analysis, review and similar techniques, in line with those utilized 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 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. Once 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 that of 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 on the assurance that safety risk controls are in place, being practised, 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-related 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 organization's choice of title — "quality" or "safety" — for the assurance process 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" in 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 risks 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 the 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, the process by which the safety performance of the organization is verified in comparison with the safety policy and approved safety objectives. Safety assurance control is conducted by monitoring and measuring the outcomes of activities that operational personnel must engage in 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 emphasis is placed on human error and 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 for the delivery of services. It is for this reason also that the SHELL 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 gap analysis.

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:

- a) **Responsibility.** Who is accountable for management of the operational activities (planning, organizing, directing, controlling) and its ultimate accomplishment.
- b) **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.
- c) **Procedures.** Specified ways to carry out operational activities and that translate the "what" (objectives) into "how" (practical activities).
- d) **Controls.** Elements of the system, including, hardware, software, special procedures or procedural steps, and supervisory practices designed to keep operational activities on track.
- e) **Interfaces.** 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.
- f) **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 input 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 should be or what they should "look like" should be left at an operational level, allowing individual organizations to tailor them to the scope and scale appropriate for the size and type of organization. Information sources for safety performance monitoring and measurement include:

- a) hazard reporting;
- b) safety studies;
- c) safety reviews;
- d) audits;
- e) safety surveys; and
- f) internal safety investigations.

9.6.5 Hazard reporting and hazard reporting systems are essential elements in hazard identification. Nobody knows actual system performance better than operational personnel. An organization that 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:

- a) mandatory reporting systems;
- b) voluntary reporting systems; and
- c) 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 and/or organizations may offer an incentive to report. For example, enforcement action may be waived for events that are reported underlining errors or unintentional violations. 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, and any identifying information about the reporter is known only to “gatekeepers” in order to allow for follow-up or “fill in voids” in the reported event(s). 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 systems are standardized, the actual reporting requirements may vary among States and organizations. It is also important to note, in order to ensure the success of the reporting systems, 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 in 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 to ensure an effective safety reporting environment. Typical qualities of successful safety reporting systems include:

- a) the reports are easy to make;
- b) there are no disciplinary actions as a result of the reports;
- c) the reports are confidential; and
- d) 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 such 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 a structural change in operations. Safety reviews are a fundamental component of the management of change, discussed in section 9.8. They have a clearly 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 at 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:

- a) hazard identification and safety risk assessment/mitigation;
- b) safety measurement;
- c) management accountabilities;
- d) operational personnel skills;
- e) technical systems; and
- f) abnormal operations.

9.6.12 Once performance of each safety management activity under the proposed changes is reviewed, the SAG produces a list of hazard 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 on 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 to 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 safety management functions, activities and resources of line units. Audits are used to ensure that the structure of the SMS is sound in terms of staffing, compliance with approved procedures and instructions, levels of competency and training to operate equipment and facilities and maintain required 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 are subjective, verification may be needed before corrective action can be taken. 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 the State, although in some instances organizations may conduct internal investigations notwithstanding the

fact that the event in question is being 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 safety performance and monitoring information sources to an organization's SMS can be summarized as follows:

- a) hazard reporting is a primary source of information on hazards in operations;
- b) safety studies are a source of information on generic safety concerns and/or systemic safety deficiencies;
- c) safety reviews are linked to the management of change and ensure safety performance under changing operational conditions;
- d) audits ensure the integrity of SMS structures and processes;
- e) safety surveys sample expert opinion and perceptions on specific problem areas in daily operations; and
- f) 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, are vital to an SMS and generate information that is used to implement corrective safety actions and ongoing 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, the vast majority of which 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. It has also been

admitted as evidence in judicial proceedings, which has resulted in criminal charges being brought against individuals involved in such occurrences. Laying criminal charges in aviation occurrences resulting from inadvertent operational errors may hinder the development and free exchange of safety information which is essential to improve aviation safety.

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 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 Assembly 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.

9.7.8 The ensuing legal guidance (contained in Attachment E to Annex 13 — *Aircraft Accident and Incident Investigation*) aims to assist States to 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:

- a) 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;
- b) It is not the purpose of protecting safety information to interfere with the proper administration of justice in States;
- c) 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;
- d) National laws and regulations protecting safety information should prevent its inappropriate use; and
- e) 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:

- a) 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;

- b) The protection should be specific for each SDCPS, based upon the nature of the safety information it contains;
- c) A formal procedure should be established to provide protection to qualified safety information, in accordance with specified conditions;
- d) Safety information should not be used in a way different from the purposes for which it was collected; and
- e) 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:

- a) 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;
- b) 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
- c) 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, 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:

- a) disclosure of the safety information is necessary to correct conditions that compromise safety and/or to change policies and regulations;
- b) disclosure of the safety information does not inhibit its future availability in order to improve safety;
- c) disclosure of relevant personal information included in the safety information complies with applicable privacy laws; and
- d) 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:

- a) the custodian of the safety information has the consent of the originator of the information for disclosure; or
- b) 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:

- a) 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
- b) 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 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 in 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:

- a) **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 being 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 an aircraft’s 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. Equipment 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.
- b) **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 the direct control of the organization, it 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.

- c) **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 the 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 the system evolves, seemingly small, incremental changes in the system (or the environment which provides the context for the system operation) can accumulate over time, which 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 ongoing 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 (i.e. a specialist safety or quality assurance department or another sub-organization as directed by senior management). The internal evaluation function also requires auditing and evaluation of 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 the delivery of services. It is here where hazards are most directly encountered, where deficiencies in activities contribute to safety risks, and where direct supervisory control and resource allocation can mitigate the safety risks to ALARP. While internal audits are often thought of as a test or “grading” of an organization’s activities, they are an essential tool for safety assurance, to help managers in charge of activities supporting the delivery of services to control that, once safety risk controls have been implemented, they continue to perform and 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. Continuous improvement is achieved through internal evaluations, internal and external audits and applies to:

- a) proactive evaluation of facilities, equipment, documentation and procedures, for example, through internal evaluations;
- b) proactive evaluation of an individual's performance, to verify the fulfilment of that individual's safety responsibilities, for example, through periodic competency checks (form of evaluation/audit); and
- c) 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 a conclusion, continuous improvement can occur only when the organization displays constant vigilance regarding the effectiveness of its technical operations and its corrective actions. Indeed, without ongoing monitoring of safety controls and mitigation actions, there is no way of telling whether the safety management process is achieving 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 of the relationship 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 practised as intended and that 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 on the organization 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 risks to ALARP. It also supports safety decisions in relation to these activities. Once in 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 the 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 on customer satisfaction, SMS requirements are safety requirements and are based on 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 assures (i.e. gives confidence) that organizational controls are being practised 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 concept in visual format.

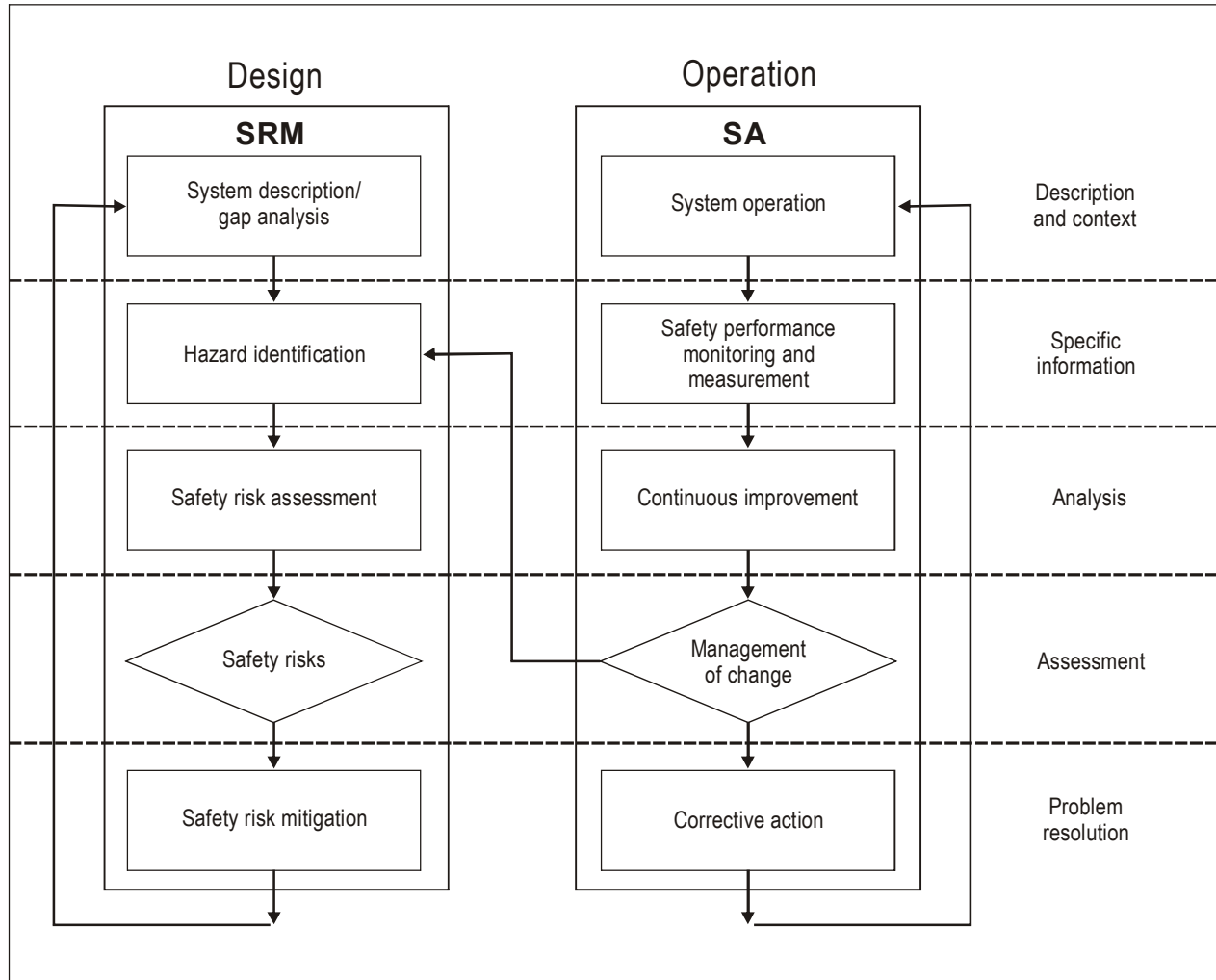


Figure 9-1. The relationship between safety risk management and safety assurance

9.11 SAFETY PROMOTION — TRAINING AND EDUCATION

9.11.1 An organizational safety effort cannot succeed by mandate or strictly through 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:

- a) training and education, including safety competency; and
- b) 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) a documented process to identify training requirements;
- b) a validation process that measures the effectiveness of training;
- c) initial (general safety) job-specific training;
- d) indoctrination/initial training incorporating SMS, including Human Factors and organizational factors; and
- e) 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 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 safety training responsibilities, including contents, 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 should include the organization's safety policy and SMS fundamentals and overview. The contents should 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 include 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 include safety assurance and safety promotion, safety roles and responsibilities, and establishing acceptable levels of safety (Figure 9-2).

9.11.10 Lastly, safety training should include special safety training for the Accountable Executive. This training session should be reasonably brief (it should not exceed one-half day), and it should 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.

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 the 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. 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:

- a) ensure that all staff are fully aware of the SMS;
- b) convey safety-critical information;
- c) explain why particular actions are taken;
- d) explain why safety procedures are introduced or changed; and
- e) convey "nice-to-know" information.

9.12.2 Examples of organizational communication include:

- a) safety management systems manual (SMSM);
- b) safety processes and procedures;
- c) safety newsletters, notices and bulletins; and
- d) websites or email.

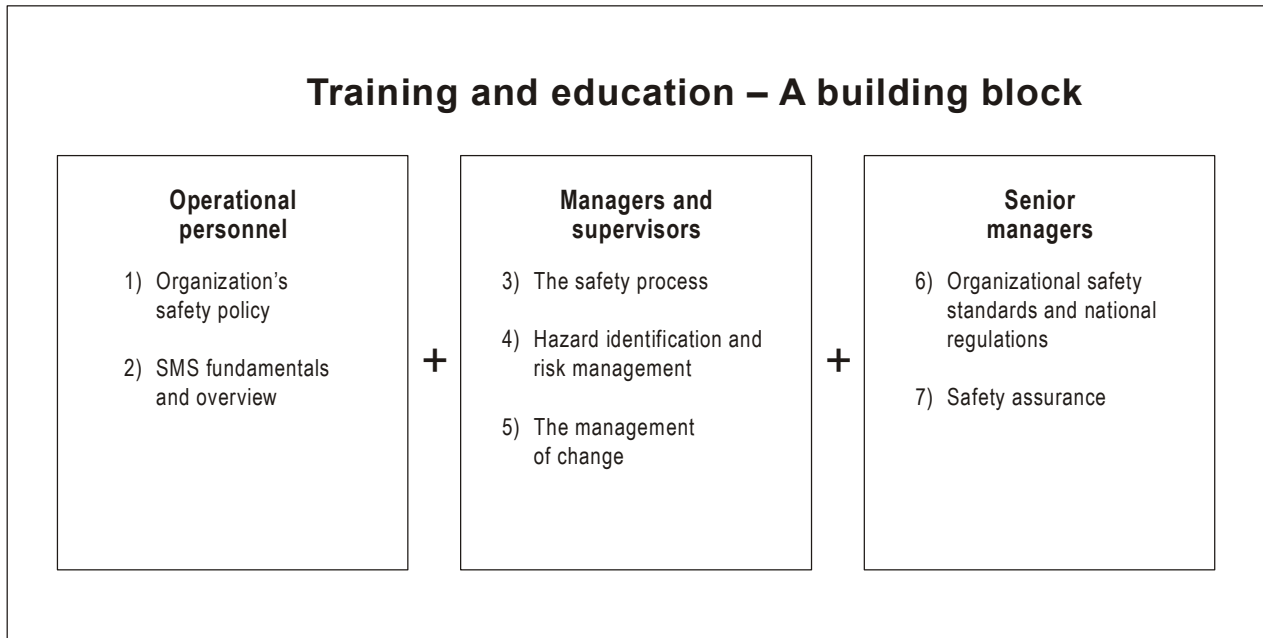


Figure 9-2. Safety training

Chapter 10

PHASED APPROACH TO SMS IMPLEMENTATION

10.1 OBJECTIVE AND CONTENTS

The objective of this chapter is to introduce a proposal for the implementation of an SMS in phases. The chapter includes the following topics:

- a) Why adopt a phased approach to SMS implementation;
- b) Phase I — Planning SMS implementation;
- c) Phase II — Reactive safety management processes;
- d) Phase III — Proactive and predictive safety management processes; and
- e) Phase IV — Operational safety assurance.

10.2 WHY ADOPT A PHASED APPROACH TO SMS 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, service providers' knowledge regarding SMS, 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 require only 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 or smaller allocation 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, two reasons that justify why a phased approach to SMS implementation is proposed are:

- a) it provides a manageable series of steps to follow in implementing an SMS, including allocation of resources; and
- b) it effectively manages the workload associated with SMS implementation.

10.2.3 A third reason, quite distinct from the previous two, but equally important, is to avoid "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 to the demands and requirements of a civil aviation oversight authority. In other words, a situation referred to as "ticking the

appropriate boxes” might develop, as a result of unreasonably demanding implementation requirements. Should such be the case, the resulting SMS, although complete and compliant on paper, would be nothing more than an empty shell. By providing a series of small, incremental and, most importantly, measurable steps, cosmetic compliance and “ticking the appropriate boxes” are 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 to successive phases involving safety management processes of greater complexity.

10.2.4 In summary, the proposal for a phased implementation of SMS aims to:

- a) provide a manageable series of steps to follow in implementing an SMS, including allocation of resources;
- b) effectively manage the workload associated with SMS implementation; and
- c) provide a robust SMS and not merely an empty shell (i.e. “ticking the appropriate boxes”).

10.2.5 Four implementation phases are proposed for an SMS. Each phase is associated with a component of the ICAO SMS framework introduced in Chapter 8. The implementation of each phase is based on 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 objective of Phase I of SMS implementation is to provide a blueprint on how the SMS requirements will be met and integrated into 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 Phase I is the gap analysis. From the gap analysis, an organization can determine the current status of its safety management processes and can begin detailed planning for the development of further safety management processes. 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 finalized in such a manner that meets the expectations of the civil aviation oversight authority, as set forth in relevant requirements and guidance material:

- a) Identify the Accountable Executive and the safety accountabilities of managers. This activity is based on Elements 1.1 and 1.2 of the ICAO SMS framework and is discussed in Chapter 8.
- b) Identify the person (or planning group) within the organization responsible for implementing the SMS. This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapter 8.
- c) 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 service providers and certified aerodromes). This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapter 7. Guidance on a system description is provided in Appendix 1 to Chapter 7.
- d) Conduct a gap analysis of the organization’s existing resources compared with the national and international requirements for establishing an SMS. This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapter 7. Guidance on an SMS gap analysis for a service provider is provided in Appendix 2 to Chapter 7.

- e) 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 on Element 1.5 of the ICAO SMS framework and is discussed in Chapter 8.
- f) Develop documentation relevant to safety policy and objectives. This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapter 8, which also includes an example of a safety policy statement.
- g) Develop and establish means for safety communication. This activity is based on Element 4.2 of the ICAO SMS framework and is discussed in Chapter 9.

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 yet exist. 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 finalized in such a manner that meets the expectations of the civil aviation oversight authority, as set forth in relevant requirements and guidance material:

- a) Implement those aspects of the SMS implementation plan that involve safety risk management based on reactive processes. This activity is based on Elements 2.1 and 2.2 of the ICAO SMS framework and is discussed in Chapters 3 and 8.
- b) Deliver training relevant to the SMS implementation plan components and to safety risk management based on reactive processes. This activity is based on Element 4.1 of the ICAO SMS framework and is discussed in Chapters 3, 8 and 9.
- c) Develop documentation relevant to the SMS implementation plan components and to safety risk management based on reactive processes. This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapters 3, 8 and 9.
- d) Develop and maintain formal means for safety communication. This activity is based on Element 4.2 of the ICAO SMS framework and is discussed in Chapter 9.

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 III, 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 finalized in such a manner that meets the expectations of the civil aviation oversight authority, as set forth in relevant requirements and guidance material:

- a) Implement those aspects of the SMS implementation plan that refer to safety risk management based on proactive and predictive processes. This activity is based on Elements 2.1 and 2.2 of the ICAO SMS framework and is discussed in Chapters 3 and 8.
- b) Develop training relevant to the SMS implementation plan components and to safety risk management based on proactive and predictive processes. This activity is based on Element 4.1 of the ICAO SMS framework and is discussed in Chapters 3, 8 and 9.
- c) Develop documentation relevant to the SMS implementation plan components and to safety risk management based on proactive and predictive processes. This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapters 3, 8 and 9.
- d) Develop and maintain formal means for safety communication. This activity is based on Element 4.2 of the ICAO SMS framework and is discussed in Chapter 9.

10.6 PHASE IV — OPERATIONAL SAFETY ASSURANCE

10.6.1 Phase IV is the final phase of the SMS. In this phase operational safety assurance is assessed through the implementation of periodic monitoring, 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 during periods of change in the operational environment.

10.6.2 At the completion of Phase IV, the following activities should be finalized in such a manner that meets the expectations of the civil aviation oversight authority, as set forth in relevant requirements and guidance material:

- a) Develop and agree on safety performance indicators, safety performance targets and SMS continuous improvement. This activity is based on Elements 1.1, 3.1, 3.2 and 3.3 of the ICAO SMS framework and is discussed in Chapters 6 and 9.
- b) Develop training relevant to operational safety assurance. This activity is based on Element 4.1 of the ICAO SMS framework and is discussed in Chapter 9.
- c) Develop documentation relevant to operational safety assurance. This activity is based on Element 1.5 of the ICAO SMS framework and is discussed in Chapter 9.
- d) Develop and maintain formal means for safety communication. This activity is based on Element 4.2 of the ICAO SMS framework and is discussed in Chapter 9.

10.6.3 A summary of the different phases of SMS implementation and their corresponding elements is shown in Figure 10-1.

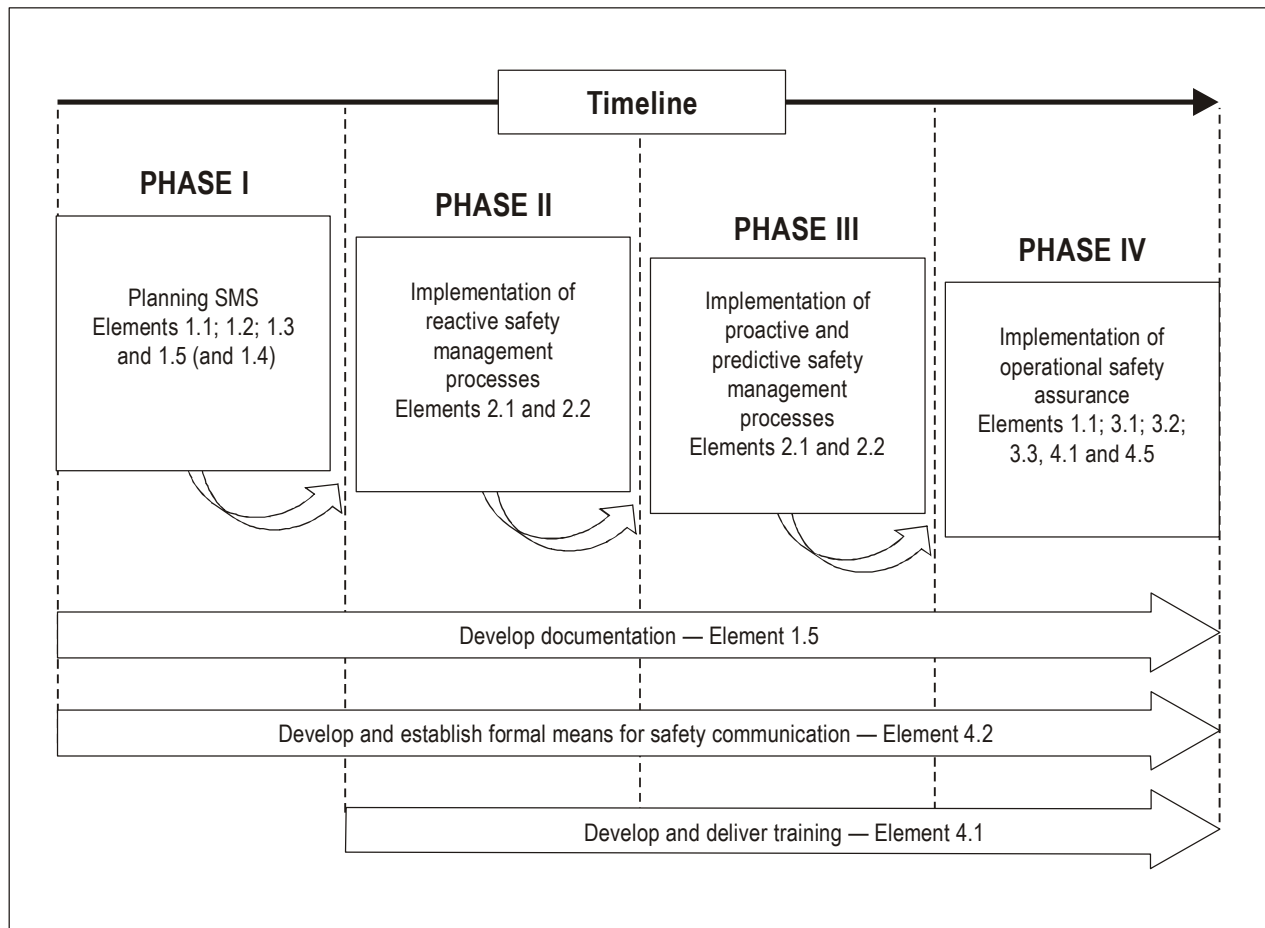


Figure 10-1. Summary of the different phases of SMS implementation

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's 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 regulation 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 service 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 subcontracted 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 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's 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 procedures 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 of the State]*.

4. DEFINITIONS

Note.— This list is 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

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.

6.1.9 A service provider shall establish safety objectives for the SMS.

6.1.10 The safety objectives should be linked to the safety performance indicators, safety performance targets and action plans 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 of, adherence to 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 someone from management to be the safety manager, the individual and focal point responsible 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 plan shall ensure the orderly and efficient transition from normal to emergency operations and the return to normal operations.

6.3.3 The coordination of the emergency response plan shall include, *inter alia*, the:

- 6.3.3.1 delegation of emergency authority;
- 6.3.3.2 assignment of emergency responsibilities during the coordinated activities;
- 6.3.3.3 coordination of efforts to cope with the emergency; and
- 6.3.3.4 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.

6.4.2 A service provider shall, as part of the SMS documentation, complete a system description.

6.4.3 The system description shall include the following:

- 6.4.3.1 the system interactions with other systems in the air transportation system;
- 6.4.3.2 the system functions;
- 6.4.3.3 required human performance considerations of the system operation;
- 6.4.3.4 hardware components of the system;
- 6.4.3.5 software components of the system;
- 6.4.3.6 related procedures that define guidance for the operation and use of the system;
- 6.4.3.7 operational environment; and
- 6.4.3.8 contracted, subcontracted and purchased products and/or services.

6.4.4 A service provider shall, as part of the SMS documentation, complete a gap analysis, in order to:

6.4.4.1 identify the safety arrangements and structures that may already exist in its organization; and

6.4.4.2 determine additional safety arrangements required to implement and maintain the organization's SMS.

6.4.5 A service provider shall, as part of the SMS documentation, develop, adhere to and maintain an SMS implementation plan.

6.4.6 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.

6.4.7 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.

6.4.8 The SMS implementation plan shall include the following:

6.4.8.1 safety policy and objectives;

6.4.8.2 system description;

6.4.8.3 gap analysis;

6.4.8.4 SMS components;

6.4.8.5 safety roles and responsibilities;

6.4.8.6 hazard reporting policy;

6.4.8.7 means of employee involvement;

6.4.8.8 safety performance measurement;

6.4.8.9 safety training;

6.4.8.10 safety communication; and

6.4.8.11 management review of safety performance.

6.4.9 The SMS implementation plan shall be endorsed by senior management of the organization.

6.4.10 A service provider shall, as part of the SMS documentation, develop and maintain a safety management systems manual (SMSM), to communicate the organization's approach to safety throughout the organization.

6.4.11 The SMSM shall document all aspects of the SMS, and its contents shall include the following:

6.4.11.1 scope of the safety management system;

6.4.11.2 safety policy and objectives;

6.4.11.3 safety accountabilities;

- 6.4.11.4 key safety personnel;
- 6.4.11.5 documentation control procedures;
- 6.4.11.6 coordination of emergency response planning;
- 6.4.11.7 hazard identification and safety risk management schemes;
- 6.4.11.8 safety performance monitoring;
- 6.4.11.9 safety auditing;
- 6.4.11.10 procedures for the management of change;
- 6.4.11.11 safety promotion; and
- 6.4.11.12 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 storage of 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 risk controls developed as a consequence of the hazard identification and safety risk management activities in 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 are 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 the 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 establish arrangements to ensure safety performance prior to implementing changes; and

8.3.2.3 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 substandard performance of the SMS, determine the implications on its operations, and rectify situations involving substandard performance in order to ensure continuous improvement of the SMS.

8.4.2 Continuous improvement of the service provider's 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 individual's performance, to verify the fulfilment of safety responsibilities.

9. SAFETY PROMOTION

9.1 General

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 their 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 are 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

A service provider shall ensure that the organization's 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's SMS, which encompasses four phases as described in 11.2 through 11.5.

11.2 **Phase I** — Planning should provide a blueprint on how the SMS requirements will be met and integrated into 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 (ATOs, air operators, AMOs, organizations responsible for type design and/or manufacture of aircraft, ATC service 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 II** — 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 safety 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 III** — 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 safety 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:
 - 11.4.3.1 SMS implementation plan components; and
 - 11.4.3.2 safety risk management (proactive and predictive processes).
- 11.5 **Phase IV** — Operational safety assurance should put into practice operational safety assurance:

- 11.5.1 development of 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;
- 11.5.4 documentation relevant to operational safety assurance; and
- 11.5.5 develop and maintain formal means for safety communication.

Appendix 2 to Chapter 10

GUIDANCE ON THE DEVELOPMENT OF AN SMS IMPLEMENTATION PLAN FOR SERVICE PROVIDERS

BACKGROUND

1. This appendix provides guidance to assist service providers in developing an SMS implementation plan that defines their 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.
2. The development of an SMS implementation plan will also:
 - a) assist service providers in preparing a realistic strategy for the implementation of an SMS that will meet the organization's safety objectives;
 - b) provide a manageable series of steps to follow in implementing an SMS; and
 - c) provide an accountability framework for the implementation of the SMS.
3. A phased approach is proposed to assist in effectively managing the workload associated with SMS implementation. Each phase is based upon the introduction of specific elements of the ICAO SMS framework.
4. 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 service providers and certified aerodromes, as applicable.

SMS Implementation Plan

1. PHASE I — PLANNING SMS IMPLEMENTATION

1.1 **The Accountable Executive**

- Identify the Accountable Executive and the person or planning group to develop the SMS implementation plan (discussed in Chapter 8).

1.2 **System description and gap analysis** (discussed in Chapter 7).

System description

- Perform the system description, which is the first prerequisite activity for the development of an SMS in an organization. It should include the interfaces within the system, as well as the interfaces with other systems in the air transportation system. Guidance on a system description is included in Appendix 1 to Chapter 7.

Gap analysis

- Perform a gap analysis, against the four components and twelve elements of the ICAO SMS framework, to identify existing safety arrangements within the organization and those that are missing. Guidance on the development of an SMS gap analysis is contained in Appendix 2 to Chapter 7.
- 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.

1.3 **Safety policy and objectives** (discussed in Chapter 8)

Safety policy

- Develop a safety policy.
- Have the Accountable Executive sign the safety policy.
- Communicate the safety policy, 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 can be found in Chapter 8.

Safety objectives

- Establish safety objectives for the SMS, by developing safety performance standards in terms of:

- safety performance indicators;
- safety performance targets; and
- action plans.
- Establish the SMS requirements for subcontractors:
 - establish a procedure to write SMS requirements into the contracting process; and
 - establish the SMS requirements in the bidding documentation.

1.4 **Safety accountabilities and appointment of key safety personnel**

(discussed in Chapter 8 of this manual)

SMS organizational structure

- Establish the safety services 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 services office and the Accountable Executive, the Safety Action Group (SAG) and the Safety Review Board (SRB).
- Ensure that the functional lines of communication are 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 appropriate strategic functions to the SRB.
- Establish the Safety Action Group (SAG).
- Appoint line managers and representatives of front-line personnel to the SAG.
- Assign appropriate tactical functions to the SRB.
- 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 risk tolerability.
- Develop a schedule of meetings for the safety services office to meet with the SRB and SAG as needed.

1.5 **Coordination of the emergency response plan (ERP)** (discussed in Chapter 8)

Internal coordination

- Review the outline of the ERP related to the delegation of authority and assignment of emergency responsibilities.
- Establish coordination procedures for action by key personnel 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.
- Incorporate the coordination among different ERPs in the organization's safety management systems manual (SMSM).

1.6 **SMS documentation** (discussed in Chapter 8)*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 records management that includes the SMS implementation plan and the SMSM.

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 the tasks at hand.
- Include significant items of the SMS implementation plan in the business plan of the organization.
- Identify the costs associated with the training and planning required for SMS implementation.
- Allocate time for the development and deployment of the SMS implementation plan among the different management layers of the organization.
- Draft a budget for SMS implementation.
- Approve the 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.
- Expand, review and amend the contents of the SMSM (which is a living document) as the phased approach of the SMS evolves.

1.7 **Safety promotion — Training** (discussed in Chapter 9)

Safety training

- Develop a documented process to identify training requirements.
- Develop 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 with training.
- Organize and set up schedules for appropriate training for all staff according to their individual responsibilities and involvement in the SMS.
- Develop training files for each employee, including management.

1.8 **Safety promotion — Safety communication** (discussed in Chapter 9)

- Establish a means to convey organizational information on Phase I, including:
 - safety newsletters, notices and bulletins;
 - websites;
 - email.

1.9 **Time frame for implementation, and deliverables**

The estimated time frame for implementation of Phase I 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.

2. PHASE II — REACTIVE SAFETY MANAGEMENT PROCESSES

2.1 **Hazard identification and analysis based on reactive processes** (discussed in Chapters 3, 4 and 9)

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.

2.2 **Safety risk management based on reactive processes** (discussed in Chapters 5 and 9)

Safety risk assessment

- Develop and adopt a safety risk matrix relevant to the organization's operational environment.
- Develop safety risk matrix instructions and include them in the training programme.

2.3 **Training** (discussed in Chapter 9)

- Develop a safety training programme for front-line personnel, managers and supervisors on:
 - the relevant SMS implementation plan components;
 - hazard identification and safety risk management based on reactive processes (front-line personnel are trained on identification and reporting of hazards from triggering events, and supervisors are trained on hazard and safety risk management);
 - the hazard reporting form/template.

2.4 **Documentation on reactive processes** (discussed in Chapters 4 and 9)

- Establish a safety library.
- Add information on reactive safety risk management processes to the SMSM. (Information on reactive safety risk management processes will be used at a later phase to establish safety performance indicators and targets.)
- Write requirements for hazard identification and safety risk management based on reactive processes into the bid documentation for contractors, if necessary, and notify contractors and subcontractors in writing.

2.5 **Safety promotion — Safety communication** (discussed in Chapter 9)

- Establish a means to convey organizational information on Phase II:
 - safety newsletters, notices and bulletins;
 - websites;
 - email.

2.6 **Time frame for implementation, and deliverables**

The estimated time frame for implementation of Phase II 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 based on safety data captured from reactive processes distributed to the organization.

3. PHASE III — PROACTIVE AND PREDICTIVE SAFETY MANAGEMENT PROCESSES

3.1 **Hazard identification and analysis based on proactive and predictive processes**
(discussed in Chapters 3, 4 and 9)

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.

3.2 **Safety risk management based on proactive and predictive processes**
(discussed in Chapters 5 and 9)

Safety risk assessment

- Develop and adopt a safety risk matrix relevant to the organization's operational environment.
- Develop safety risk matrix instructions and include them in the training programme.

3.3 **Training** (discussed in Chapter 9)

- Train staff of the safety services office on specific proactive and predictive means of collecting safety-related data.
- Brief supervisors and front-line 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 safety risk management based on proactive and predictive processes (front-line personnel are trained on identification and reporting of hazards from less serious triggering events or during real-time normal operations, and supervisors are trained on hazard and safety risk management based on proactive and predictive processes).

3.4 **Documentation on proactive and predictive processes**

(discussed in Chapters 4 and 9 of this manual)

- Store information from safety risk management based on proactive and predictive processes in the safety library.
- Add information on proactive and predictive safety risk management processes to the SMSM.
- Develop safety performance indicators and safety performance targets.
- Write requirements for hazard identification and safety risk management based on proactive and predictive processes into the bid documentation for contractors, if necessary, and notify contractors and subcontractors in writing.

3.5 **Safety promotion — Safety communication** (discussed in Chapter 9)

- Establish a means to convey organizational information on Phase III:
 - safety newsletters, notices and bulletins;
 - websites;
 - email.

3.6 **Time frame for implementation, and deliverables**

The estimated time frame for implementation of Phase III 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 based 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.

4. PHASE IV — OPERATIONAL SAFETY ASSURANCE

4.1 **Safety performance of the SMS** (discussed in Chapter 9)

- Establish safety performance indicators.
- Establish safety performance targets.
- Establish action plans.
- Define measures of reliability, availability and/or accuracy related to action plans, as required.
- Agree on safety performance measurement with the State oversight authority.

4.2 **Safety performance monitoring and measurement** (discussed in Chapter 9)

- Define and develop information sources for safety performance and monitoring.

4.3 **The management of change** (discussed in Chapter 9)

- 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 implementing changes, define arrangements to ensure safety performance.

4.4 **Continuous improvement of the SMS** (discussed in Chapter 9)

- Develop forms for internal evaluations and ensure independence from technical processes being evaluated.
- Define an internal audit process.
- Define an external audit process.

- Define a schedule for proactive evaluation of facilities, equipment, documentation and procedures, to be completed through audits and surveys.
- Define a schedule for proactive evaluation of an individual's performance.
- Develop documentation relevant to operational safety assurance.

4.5 **Training** (discussed in Chapter 9)

- Develop training relevant to operational safety assurance for staff involved in the safety assurance phase.

4.6 **Safety promotion — Safety communication** (discussed in Chapter 9)

- Establish a means to convey organizational information on Phase IV:
 - safety newsletters, notices and bulletins;
 - websites;
 - email.

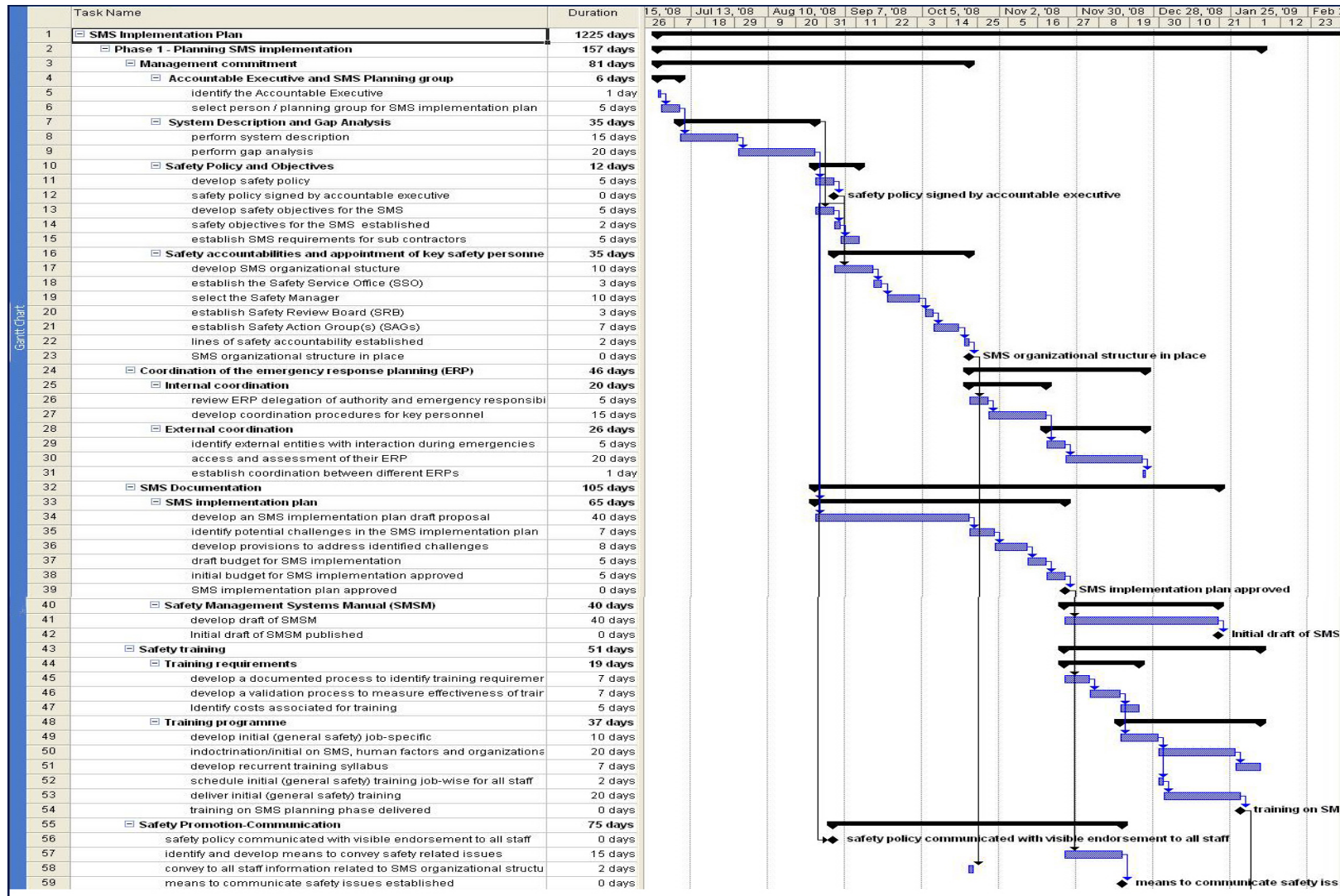
4.7 **Time frame for implementation and deliverables**

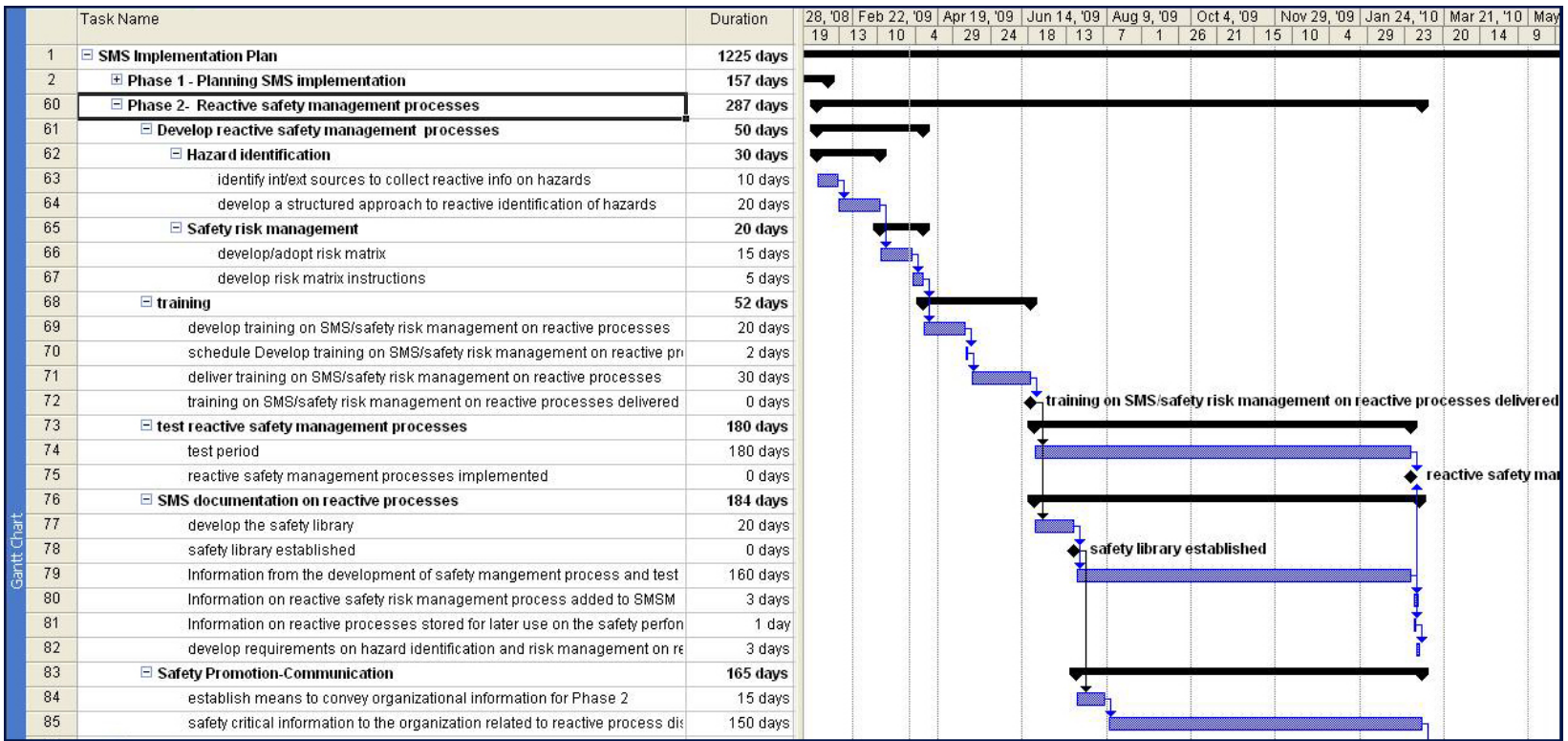
The estimated time frame for implementation of Phase IV could take from 9 to 12 months, depending on the size of the organization and complexity of the services provided.

Deliverables

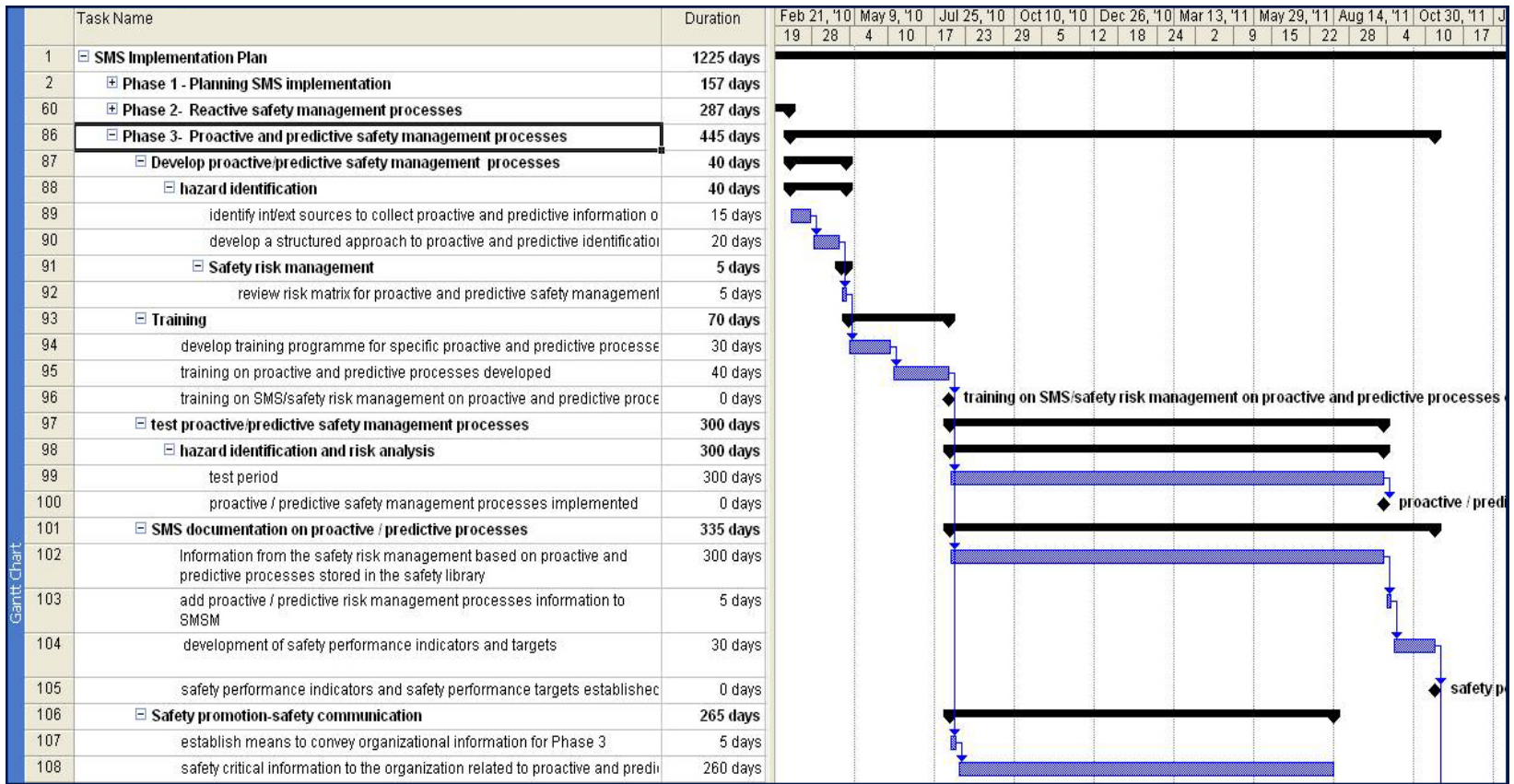
- 1) Agreement reached with the State oversight authority on safety performance indicators and safety performance targets.
- 2) Training on safety assurance for operational personnel, managers and supervisors completed.
- 3) Documentation relevant to operational safety assurance placed in the safety library.

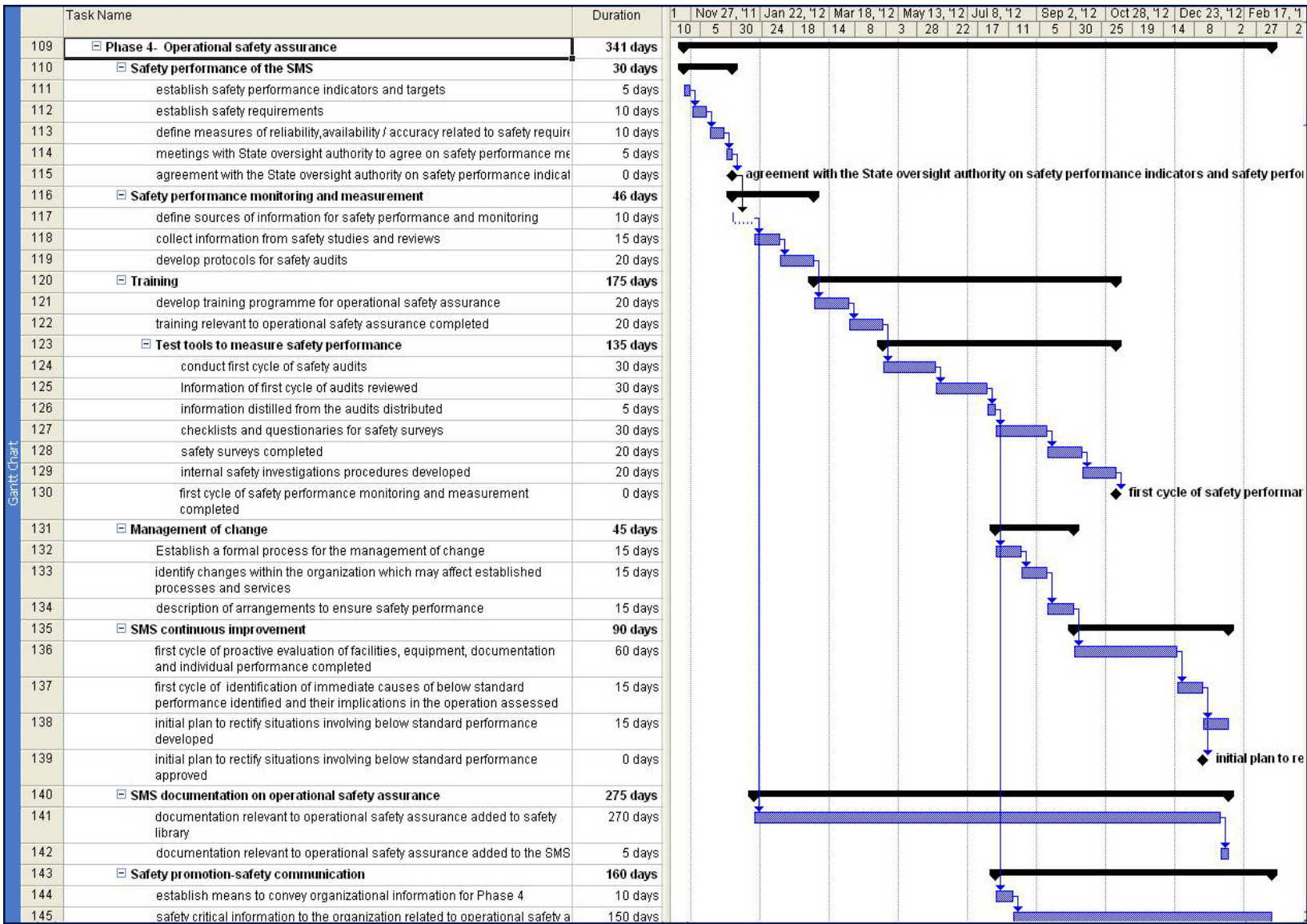
Gantt Chart — SMS Implementation Plan





Gantt Chart





Gantt Chart

Chapter 11

STATE SAFETY PROGRAMME (SSP)

11.1 OBJECTIVES AND CONTENTS

This chapter introduces a framework for development and implementation of a State safety programme (SSP) that combines elements of both prescriptive and performance-based approaches to the management of safety. This chapter also discusses the importance of a realistic implementation of an SSP as a prerequisite for the implementation of an SMS by service providers. The chapter includes the following topics:

- a) The components and elements of an SSP;
- b) The ICAO SSP framework;
- c) SSP development;
- d) SSP implementation; and
- e) The role of the SSP in supporting 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 elements of civil aviation functions in the State.

11.2.2 There are four components of an SSP, which 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:

- a) State safety policy and objectives;
- b) State safety risk management;
- c) State safety assurance; and
- d) State safety promotion.

11.2.3 From the point of view of safety interventions and mitigation strategies, the two core operational activities of an SSP are 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. Most of the equivalent components of an SMS presented in Chapter 8, 8.2 and 8.3 also apply to the SSP. There is, however, one difference: under the SSP, the accident and serious incident investigation process, although formally considered 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 of areas of greater concern (State safety assurance).

11.2.4 The four components discussed in 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 utilize in order to conduct the management of safety in a manner that combines prescriptive and performance-based approaches and supports the implementation of SMS by service providers.

11.2.5 The State safety policy and objectives component is composed of four elements:

- a) State safety legislative framework;
- b) State safety responsibilities and accountabilities;
- c) accident and incident investigation; and
- d) enforcement policy.

11.2.6 The State safety risk management component is composed of two elements:

- a) safety requirements for the service provider's SMS;
- b) agreement on the service provider's safety performance.

11.2.7 The State safety assurance component is composed of three elements:

- a) safety oversight;
- b) safety data collection, analysis and exchange; and
- c) safety-data-driven targeting of oversight of areas of greater concern or need.

11.2.8 The State safety promotion component is composed of two elements:

- a) internal training, communication and dissemination of safety information; and
- b) 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 service 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, comprise 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 the service provider's SMS
 - 2.2 Agreement on the service provider's 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 of 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 requirements, responsibilities and accountabilities of the different State organizations 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 be effectively implemented only 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 State safety policy and objectives component provides management and personnel explicit policies, procedures, management controls, documentation and corrective action processes that keep the safety management efforts of the State's civil aviation authority on track. This component is also essential in generating confidence in the State's ability to provide safety leadership in 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 of 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 provider's SMS operates, as well as agreement on the safety performance of the service provider's SMS.

11.4.5 Safety management principles affect most activities of a State's civil aviation authority, starting with rulemaking and policy development. Rather than pursuing only the causes of the most recent accident, 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 the service provider's 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 provider's SMS follow established controls (regulatory compliance), how realistic implementation of the SSP (ALoS) will be achieved, though a combination of safety measurement by the State and safety performance measurement by service providers, and how the actual performance of the service provider's 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.** SSP oversight activities, beyond rulemaking, are supported by analysis, and the resource allocation priorities of the State's civil aviation authority are 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 the service provider's 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 in regulations within the service provider's specific operational environment. The State safety assurance processes are used to obtain confidence in the service provider's safety management capability as demonstrated in assessments of its 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 take place. Under an SSP, this is a dual-track promotion; both within the State's 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 the State's regulations and standards, or the requirement for State civil aviation personnel to possess high levels of knowledge and skills. On 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 of the SSP by the State and the SMS by service providers. An SSP developed from, and based upon, safety management principles bridges the gap that would otherwise inevitably develop between the internal and external safety processes within the State's civil aviation organizations and the internal safety processes of service providers (see Figure 11-1). As part of the SSP, the State promulgates SMS requirements for service providers requiring them 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.

11.5 SSP IMPLEMENTATION

11.5.1 SSP implementation is facilitated by identifying the processes associated with 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 the SSP developed 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 UK CAA 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 an SMS by service providers. The service provider's SMS cannot perform effectively 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. A service provider's SMS can flourish only under the enabling umbrella provided by an SSP. The SSP is therefore a fundamental enabler of the implementation of an effective SMS by service providers. For this reason, within the scope of the overall implementation of an SSP presented in Appendix 5, four steps, two globally and two specifically, aim at supporting SMS implementation by service providers.



Figure 11-1. SMS bridges the gap between the safety processes of the State and those of the service provider

11.6.2 The first step, overall, to be taken by a State in implementing its SSP is to conduct a gap analysis, in order to ascertain the existence and status of maturity, 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 personnel of the State authority. The training programme should have two basic objectives. The first objective is to provide knowledge of safety management concepts, including the ICAO SARPs contained in Annexes 1, 6, 8, 11, 13 and 14, and related guidance material. This aspect of 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 national regulations and relevant ICAO SARPs. This aspect of 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 guidance material for the implementation of SMS. Guidance on the development of a State's regulation on SMS is included in Appendix 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 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 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 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 are at the heart of the interactive nature of the SSP and the SMS discussed in 11.4.10.

11.6.7 During the course of normal safety management activities under the SSP and SMS, respectively, the State and 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 provider's SMS processes. If the civil aviation oversight authority's response to these data 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 revise its enforcement policy to ensure continuous flow and exchange of proactive and predictive safety management data with service providers who operate in an SMS environment. The following guidelines are proposed for such revision:

- a) service providers should be allowed to deal with certain safety concerns internally, within the context of their SMS;
- b) 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;
- c) the mitigation plan should include timelines, so that the State can monitor satisfactory progress of mitigation activities; and
- d) gross negligence, reckless conduct and wilful deviations should be dealt with through established enforcement procedures.

Appendix 4 to this chapter presents guidance on the development of a State's enforcement policy and enforcement procedures in an SMS environment.

11.6.8 A summary of the role of the SSP in supporting SMS implementation and proposed actions is shown in Figure 11-2.

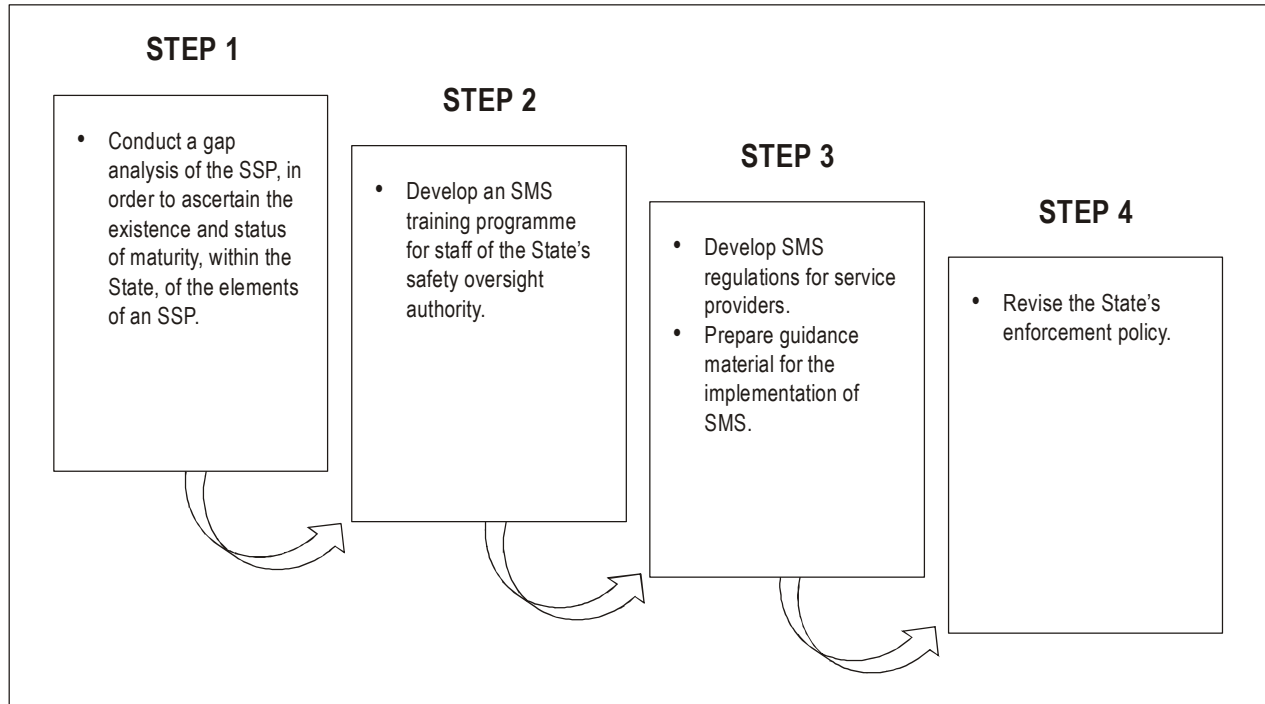


Figure 11-2. A summary of the role of the SSP in supporting SMS implementation

Appendix 1 to Chapter 11

FRAMEWORK FOR THE STATE SAFETY PROGRAMME (SSP)

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 service providers and certified aerodromes, as applicable.

This appendix introduces a framework for the implementation and maintenance of a State safety programme (SSP) by a State. The framework consists of the following four components and eleven elements:

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 of 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.

A brief description of each element follows.

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 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's 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 the service provider's 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 the service provider's 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 the service provider's safety performance

The State has agreed with individual service providers on the safety performance of their SMS. The agreed safety performance of an individual service provider's 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 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 provider's SMS, that they are being practised 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 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 of 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.

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 the 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 be required to demonstrate that their management systems adequately reflect an SMS approach. The expected result of this approach is improved safety management, and safety practices, including safety reporting within the civil aviation industry.

In [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 and personnel have the proper skills and are trained for discharging their responsibilities, both safety-related and otherwise;
- f) conduct both performance-based and 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 are encouraged to provide essential safety-related information on hazards, and there is a continuous flow and exchange of safety management data between [State] and service providers;

- l) establish and measure the realistic implementation of our SSP against safety indicators and safety targets which are clearly identified; and
- m) promulgate an enforcement policy that ensures that no information derived from any SDCPS established under the SSP or the SMS will be used as the basis for enforcement action, except in the case of 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

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 service providers and certified aerodromes, as applicable.

1. GAP ANALYSIS

1.1 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.

1.2 The gap analysis 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.

2. 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 the service provider's SMS
 - 2.2 Agreement on the service provider's 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 of 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.

3. STATE SAFETY PROGRAMME (SSP) GAP ANALYSIS

The gap analysis checklist that follows 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 the 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.

<i>ICAO reference (Doc 9859)</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
Component 1 — STATE SAFETY POLICIES AND OBJECTIVES			
Element 1.1 — State safety legislative framework			
Chapter 11	Has [State] promulgated a national safety legislative framework and specific regulations that define the management of safety in the State?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Has [State] defined the specific activities related to the management of safety in the State in which each [State] aviation organization must participate?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Has [State] established requirements, responsibilities and accountabilities regarding the management of safety in [State] by its aviation organizations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are the legislative framework and specific regulations periodically reviewed to ensure that they remain relevant and appropriate to the State?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are [State] legislative framework and specific regulations periodically reviewed to ensure that they are up to date with respect to international standards?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Has [State] established a safety policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is [State] safety policy signed by the [State] SSP Accountable Executive or a high authority within [State]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is [State] safety policy reviewed periodically?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Has [State] developed documentation that describes the SSP, including the interrelationship between its components and elements?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference (Doc 9859)</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 1.2 — State safety responsibilities and accountabilities			
Chapter 11	Has [State] identified and defined the State requirements, responsibilities and accountabilities regarding the establishment and maintenance of the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Do the requirements include directives and activities to plan, organize, develop, control and continuously improve the SSP in a manner that meets [State] safety objectives?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Do the requirements include a clear statement about the provision of the necessary resources for the implementation and maintenance of the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Has [State] identified and appointed an Accountable Executive as the qualified person having direct responsibility for the implementation, operation and supervision of the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does the [State] SSP Accountable Executive fulfil the required job functions and responsibilities?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does the [State] SSP Accountable Executive coordinate, as appropriate, the activities of the different State aviation organizations under the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does the [State] SSP Accountable Executive have control of the necessary resources required for the proper execution of the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does the [State] SSP Accountable Executive verify that all personnel of [State] aviation organizations understand their authorities, responsibilities and accountabilities with regard to the SSP and all safety management processes, decisions and actions?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are safety responsibilities and accountabilities, at all levels, defined and documented?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 1.3 — Accident and incident investigation			
Chapter 11	Has [State] established, as part of the management of 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does [State] maintain the independence of the accident and incident investigation organization from other State aviation organizations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 1.4 — Enforcement policy			
Chapter 11	Has [State] promulgated an enforcement policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference (Doc 9859)</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
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's safety management system (SMS), and to the satisfaction of the appropriate State authority?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does the enforcement policy establish the conditions and circumstances under which to deal with safety deviations through established enforcement procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Component 2 — STATE SAFETY RISK MANAGEMENT			
Element 2.1 — Safety requirements for the service provider's SMS			
Chapter 11	Has [State] established the controls which govern how service providers will identify hazards and manage safety risks?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Do those controls include requirements, specific operating regulations and implementation policies for the service provider's SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are requirements, specific operating regulations and implementation policies based on identified hazards and analysis of the safety risks of the consequences of the hazards?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are requirements, specific operating regulations and implementation policies periodically reviewed to ensure they remain relevant and appropriate to the service providers?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is there a [State] policy in place that ensures effective safety reporting of safety deficiencies, hazards or occurrences?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 2.2 — Agreement on the service provider's safety performance			
Chapter 11	Has [State] individually agreed with service providers on the safety performance of their SMS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is the agreed safety performance commensurate with the complexity of the individual service provider's specific operational context?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does the agreed safety performance consider the individual service provider's resources to address safety risks?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is the agreed safety performance expressed by multiple safety indicators and safety targets, as opposed to a single one, as well as by action plans?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is the agreed safety performance periodically reviewed to ensure it remains relevant and appropriate to the service provider?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

ICAO reference (Doc 9859)	Aspect to be analysed or question to be answered	Answer	Status of implementation
Component 3 — STATE SAFETY ASSURANCE			
Element 3.1 — Safety oversight			
Chapter 11	Has [State] established mechanisms to ensure an effective safety oversight function?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Do established mechanisms include inspections, audits and surveys to ensure that regulatory safety risk controls are appropriately integrated into the SMS of service providers?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Do established mechanisms ensure that regulatory safety risk controls are practised as designed?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Do established mechanisms ensure that regulatory safety risk controls have the intended effect on safety risks?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are regular and periodic reviews conducted regarding [State] ALoS?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are regular and periodic reviews conducted to assess if [State] SSP and its ALoS remain appropriate to the scope and complexity of the aviation operations in the State?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is there a process to evaluate the effectiveness of changes related to the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 3.2 — Safety data collection, analysis and exchange			
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Has [State] established an acceptable level of safety (ALoS) related to its SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Does [State] ALoS related to the SSP combine elements of safety measurement and safety performance measurement?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is [State] ALoS commensurate with the complexity of aviation activities within [State]?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is there a formal process within [State] to develop and maintain a set of parameters to measure the realistic implementation of the SSP?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 3.3 — Safety-data-driven targeting of oversight of areas of greater concern or need			
Chapter 11	Has [State] developed procedures to prioritize inspections, audits and surveys towards those areas of greater safety concern or need?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

<i>ICAO reference (Doc 9859)</i>	<i>Aspect to be analysed or question to be answered</i>	<i>Answer</i>	<i>Status of implementation</i>
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Component 4 — STATE SAFETY PROMOTION			
Element 4.1 — Internal training, communication and dissemination of safety information			
Chapter 11	Does [State] provide internal training, awareness and two-way communication of safety-relevant information within [State] aviation organizations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are there communication processes in place within [State] to ensure that information about the SSP functions and products is made available to [State] aviation organizations in a timely manner?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
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?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are communication processes (written, meetings, electronic, etc.) commensurate with the size and scope of the [State] aviation organizations?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are safety information and information about the SSP functions and products maintained in a suitable medium?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Element 4.2 — External training, communication and dissemination of safety information			
Chapter 11	Does the [State] provide external education, awareness of safety risks and two-way communication of safety-relevant information?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are there communication processes in place within [State] that allow the SSP to be promoted nationally and internationally?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Is there a formal process for the external dissemination of safety information to [State] service providers and a means of monitoring the effectiveness of this process?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are there communication processes in place within [State] to ensure that information about the SSP functions and products is made available to [State] service providers in a timely manner?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are communication processes (written, meetings, electronic, etc.) commensurate with the size and scope of [State] service providers?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Chapter 11	Are safety information and information about the SSP functions and products established and maintained in a suitable medium?	<input type="checkbox"/> Yes <input type="checkbox"/> No	

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. 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)].

2. PRINCIPLES

2.1 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.

2.2 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.

2.3 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's 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.

2.4 The second general principle is that no information derived from safety data collection and processing systems (SDCPS) established under SMS shall be used as the basis for enforcement action.

3. SCOPE

3.1 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*; Annex 11 — *Air Traffic Services*; and Annex 14 — *Aerodromes, Volume I — Aerodrome Design and Operations*.

3.2 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 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 service providers and certified aerodromes, as applicable.

4. GENERAL

4.1 [Service provider] will establish, maintain and adhere to an SMS that is commensurate with the size, nature and complexity of the operations authorized to be conducted under its operations certificate and to the hazards and safety risks related to these operations.

4.2 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.

4.3 When a service provider operating under an SMS unintentionally 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, analyse 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.

5. 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 the 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.

6. 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:

- a) counselling;
- b) remedial training; or
- c) variation, suspension and cancellation of authorizations.

7. IMPARTIALITY OF ENFORCEMENT ACTIONS

Enforcement decisions must not be influenced by:

- a) personal conflict;
- b) considerations such as gender, race, religion, political views or affiliation; or
- c) personal, political or financial power of those involved.

8. PROPORTIONALITY OF RESPONSES

Enforcement decisions must be proportional to the identified breaches and the safety risks they underlie, based on two principles:

- a) [State's CAA] will take action against those who consistently and deliberately operate outside Civil Aviation Regulations; and
- b) [State's CAA] will seek to educate and promote training or supervision of those who show commitment to resolving safety deficiencies.

9. NATURAL JUSTICE AND ACCOUNTABILITY

Enforcement decisions must:

- a) be fair and follow due process;
- b) be transparent to those involved;
- c) take into account the circumstances of the case and the attitude/actions of the service provider when considering action;
- d) be consistent actions/decisions for like/similar circumstances; and
- e) be subject to appropriate internal and external review.

10. EXCEPTIONS

10.1 This policy is not applicable if there is evidence of a deliberate effort to conceal non-compliance.

10.2 This policy is not applicable if the service provider fails to provide confidence in its means of hazard identification and safety risk management.

10.3 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.

10.4 In such circumstances, the penalty matrix (or applicable measurement) of the established enforcement procedures will be applicable.

(Signed) _____
State Accountable Executive

Enforcement Procedures in an SMS environment

1. GENERAL

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 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

2.1 These procedures apply to contraventions that may have been committed by persons or service providers conducting activities under an SMS.

2.2 These procedures are effective as of [date]. They replace and supersede previous procedures identified in [State's Civil Aviation Regulations].

2.3 Where service providers have demonstrated their willingness to conduct their operations under an SMS, SMS enforcement procedures may be used with respect to contraventions by those service providers that, although they do not have an accepted SMS, have some essential core components of an SMS in place and are in the process of full implementation.

2.4 [State's CAA] will not apply SMS enforcement procedures to 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" similar to the one outlined in [State's CAA] published advisory material [AM-xxx] — Implementation Procedures Guide for SMS.

2.5 Where service providers have not demonstrated they are operating in an SMS environment, the enforcement actions may apply without the advantages of the procedures explained in paragraph 3.

3. PROCEDURES

3.1 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 the 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.

3.2 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 this list available to aviation enforcement will assist the investigators in making a decision regarding the use of the SMS enforcement procedures.

3.3 During the “phased approach” 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.

3.4 [State’s CAA] will require, as a minimum, that the three following conditions be met before SMS enforcement procedures may be applied:

- a) The service provider has an effective internal hazard reporting programme supported by upper management;
- b) The service provider has a proactive event analysis process commensurate with the size and complexity of its operations and adequate for determining causal factors and developing corrective measures;
- c) The information derived from the process referred to in paragraph 3, appropriately protected so as not to endanger SDCPS, is communicated, upon request, to the principal inspector assigned to the specific service provider.

Initial report of violation

3.5 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.

Preliminary analysis

3.6 The following questions should be considered based on the information received:

- a) Are there reasonable grounds to believe that a person or organization conducting activities under an SMS may have committed a contravention?
- b) Is the event of such a serious nature that enforcement action should be considered?
- c) Is there any perishable evidence that should be secured for enforcement action?

Providing effective support

3.7 When the three questions are answered in the affirmative, the principal inspector shall be notified. The information shall identify the event and the contravention.

3.8 When requested, aviation enforcement investigators will provide effective support to the Accountable Executive by advising on the appropriate response to the contravention, in order to ensure that if enforcement action is taken, it will be successful. Support for the Accountable Executive includes collecting and securing perishable evidence.

Initiating an enforcement investigation

3.9 An enforcement investigation shall be initiated only upon the request of the principal inspector, not the enforcement investigators.

Immunity

3.10 No information derived from an 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, follow the requirements and guidance set forth by the International Civil Aviation Organization (ICAO) and meet the conditions in paragraph 3.

Appendix 5 to Chapter 11

GUIDANCE ON THE DEVELOPMENT OF AN SSP IMPLEMENTATION PLAN

1. BACKGROUND

1.1 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, in a sequential, principled manner, the processes, procedures and means that will allow the State to discharge its responsibilities associated with the management of safety in civil aviation.

1.2 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 elements of civil aviation functions in the State. This guidance is intended as a reference and may need to be tailored to meet the particular needs of States.

1.3 The development of an SSP implementation plan will allow States to:

- a) formulate an overarching strategy for the management of safety in the State;
- b) coordinate the processes executed by the different State aviation organizations under the SSP;
- c) establish the controls that govern how the service provider's safety management system (SMS) will operate;
- d) ensure that the operation of the service provider's SMS follows established controls; and
- e) support the interaction between the SSP and the operation of the service provider's SMS.

1.4 When the State is responsible for the provision of specific services (e.g. aerodrome services, air navigation services) the organization providing the service should develop and implement an SMS (refer to the SMS implementation plan 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 service providers and certified aerodromes, as applicable.

2. SSP GAP ANALYSIS

2.1 In order to develop an SSP implementation plan, a gap analysis of the 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.

2.2 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 of 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
 - 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 the service provider's SMS
 - 2.2 Agreement on the service provider's 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 of 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.

3. SSP IMPLEMENTATION PLAN

3.1 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 with 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.

3.2 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.

1. STATE SAFETY POLICY AND OBJECTIVES

1.1 State safety legislative framework

- a) 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.
- b) Establish a national-level group within the State in the form of a 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.
- c) Establish a time frame to periodically review the safety legislation and specific operating regulations to ensure they remain relevant and appropriate to the State.

1.2 State safety responsibilities and accountabilities

- a) 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 of and continuously improve the SSP in a manner that meets the State's safety objectives. Include a clear statement about the provision of the necessary resources for the implementation of the SSP.
- b) Identify and appoint the Accountable Executive of the State SSP who shall have *inter alia*:
 - 1) ultimate responsibility and accountability, on behalf of the State, for the implementation and maintenance of the SSP;
 - 2) full authority on human resources issues related to the State aviation organization that has been designated as placeholder for the SSP;
 - 3) full authority on major financial issues related to State aviation organization that has been designated as placeholder for the SSP;
 - 4) final authority over service provider's certificate management aspects; and
 - 5) final responsibility for the resolution of all aviation safety issues of the State.
- c) Establish the SSP implementation team.
- d) Assign the time required for each task associated with the implementation of the SSP among the different management levels of the State aviation organizations.
- e) Introduce all staff to SSP concepts at a level commensurate with their involvement in the SSP.
- f) Develop and implement a State safety policy that includes but is not necessarily limited to:
 - 1) 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;
 - 2) the development and promulgation of a national safety legislative framework and applicable operating regulations for the management of safety in the State;

- 3) the commitment to allocate the necessary resources to State aviation organizations to allow their personnel to discharge their responsibilities, both safety-related and otherwise;
 - 4) the support of the management of safety in the State through an effective hazard reporting and communication system;
 - 5) the establishment of provisions for the protection of safety data collection and processing systems (SDCPS);
 - 6) the commitment to effective interaction with service providers in the resolution of safety concerns;
 - 7) the commitment to communicate the State safety policy, with visible endorsement, to all staff; and
 - 8) an enforcement policy that reflects service provider's operations in an SMS environment.
- g) Establish the necessary means to ensure that the State safety policy is understood, implemented and observed at all levels within State aviation organizations.

1.3 Accident and incident investigation

- a) 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.
- b) Develop and establish the necessary arrangements to ensure the independence of the accident and incident investigation authority from other aviation organizations of the State.

1.4 Enforcement policy

- a) 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's 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.
- b) 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.

1.5 SSP documentation

- a) 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's acceptable level of safety (ALoS) related to 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 the Accountable Executive.
4. State safety and enforcement policies distributed within the aviation organizations of the State and among service providers under oversight.
5. Independent accident and incident investigation process in place.
6. SSP organizational structure in place.

Milestones

1. Accountable Executive identified.
2. Proposed safety policy drafted.
3. Lines of safety responsibility and accountability established.
4. Proposed SSP organizational structure approved.
5. 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.

2. STATE SAFETY RISK MANAGEMENT

2.1 Safety requirements for the service provider's SMS

- a) Establish the requirements, specific operating regulations and implementation policies for the service provider's SMS (SMS regulatory framework, advisory circulars, etc.) as the controls which govern how service providers will identify hazards and manage and control safety risks.
- b) Establish a time frame for consultation with service providers on those requirements.
- c) Establish a time frame to periodically review the requirements and specific operating regulations to ensure they remain relevant and appropriate to the service providers.

2.2 Agreement on the service provider's safety performance

- a) Develop and establish a procedure for agreement on the safety performance of an individual service provider's SMS based on:

- 1) safety performance indicator values;
 - 2) safety performance target values; and
 - 3) action plans.
- b) Include within the agreed procedure that the service provider's safety performance should be commensurate with:
- 1) the complexity of the individual service provider's specific operational contexts; and
 - 2) the availability of the individual service provider's resources to address safety risks.
- c) Measure the safety performance of the service provider's 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.
- d) Develop a means to assess lower-level outcomes and most frequent processes among different service providers.
- e) Determine measurable performance outcomes within different SMS.

Deliverables

1. SMS regulations promulgated.
2. Guidance material on implementation of SMS distributed to service providers.
3. First annual review of the agreed safety performance of service providers 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. Training of State technical personnel in hazard identification and safety risk management completed.
4. Procedure for agreement on the safety performance of service providers completed.

3. STATE SAFETY ASSURANCE**3.1 Safety oversight**

- a) Establish mechanisms to ensure an effective safety oversight function.
- b) Establish mechanisms that guarantee that the identification of hazards and the management of safety risks by service providers follow established regulatory controls.

- c) Establish mechanisms that guarantee that safety risk controls are integrated into the service provider's SMS.
- d) Develop an internal SSP audit.

3.2 Safety data collection, analysis and exchange

- a) Develop and establish a means of collecting, analysing and storing data about hazards and safety risks at the State level:
 - 1) establish a mandatory hazard reporting system;
 - 2) establish a confidential hazard reporting system;
 - 3) develop a State hazard database;
 - 4) establish a mechanism to develop information from the stored data;
 - 5) establish a means to collect hazards at both the aggregate State level and at the individual service provider's level; and
 - 6) establish a means to implement corrective action plans.
- b) Ensure that the 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 provider's SMS, including, but not necessarily limited to:
 - 1) inspections;
 - 2) audits; and
 - 3) surveys.
- c) Observe the following sequence for implementation:
 - 1) regulatory safety risk controls integrated into the service provider's SMS;
 - 2) oversight activities to ensure the service provider's hazard identification and safety risk management processes follow established regulatory requirements; and
 - 3) oversight activities to verify that safety risk controls are practised by service providers.
- d) Establish the acceptable level of safety (ALoS) related to the SSP, comprising a combination of safety measurement and safety performance measurement:
 - 1) 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 and regulatory compliance.
 - 2) Safety performance measurement includes the quantification of the outcomes of low-level, low-consequence processes that provides a measure of the realistic implementation of an individual SSP beyond accident rates and/or regulatory compliance.

3.3 Safety-data-driven targeting of oversight of areas of greater concern or need

- a) Establish procedures to prioritize inspections, audits and surveys, based on analysis of hazards and safety risks.

Deliverables

1. State mandatory and confidential hazard reporting system in place.
2. First annual review of the safety policy and objectives conducted.
3. First annual review of the enforcement policy conducted.
4. ALoS established.

Milestones

1. Data storage and processing of hazards and safety risks at the State level.
2. Information on hazards and safety risks at both the aggregate State level and the individual service provider's level collected.

4. STATE SAFETY PROMOTION

4.1 Internal training, communication and dissemination of safety information

- a) Identify internal training requirements.
- b) Develop and provide generic safety training to all staff.
- c) Develop a training programme on key components of an SSP and an SMS for staff that includes:
 - 1) indoctrination/initial safety training;
 - 2) on-the-job (OJT) safety training;
 - 3) recurrent safety training.
- d) Establish a means to measure the effectiveness of the training.
- e) Develop a means to communicate safety-related issues internally, including:
 - 1) safety policies and procedures;
 - 2) newsletters;
 - 3) bulletins; and
 - 4) a website.

4.2 External training, communication and dissemination of safety information

- a) Establish the means to provide two-way communication of safety-relevant information to support SMS implementation among service providers, including small operators.
- b) Develop training and guidance material on implementation of SMS for service providers.
- c) Establish the means to communicate safety-related issues externally including:
 - 1) safety policies and procedures;
 - 2) newsletters;
 - 3) bulletins; and
 - 4) a website.

Deliverables

- 1. First cycle of generic safety training for staff completed.
- 2. Training programme on key components of an SSP and an SMS for technical and support staff completed.
- 3. Guidance material on SMS distributed to service providers, including small operators.
- 4. First cycle of training for service providers on implementation of SMS completed.
- 5. Means to communicate safety-related information, internally and externally, established.

Milestones

- 1. Minimum knowledge and experience requirements for technical personnel performing safety oversight functions established.
 - 2. Guidance material on SMS developed and published.
 - 3. Training programmes on SMS for State aviation organizations 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 certificated take-off mass of over 2 250 kg. ICAO also gathers information on aircraft incidents involving aircraft over 5 700 kg. 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.

LIST OF EXAMPLES OF SERIOUS INCIDENTS

The term “serious incident” is defined in Annex 13, Chapter 1, as follows:

Serious incident. An incident involving circumstances indicating that an accident nearly occurred.

The incidents listed are typical examples of incidents that are likely to be serious incidents. The list is not exhaustive and only serves as guidance to the definition of serious incident.

- Near collisions requiring an avoidance manoeuvre to avoid a collision or an unsafe situation or when an avoidance action would have been appropriate.
- Controlled flight into terrain only marginally avoided.
- Aborted take-offs on a closed or engaged runway, on a taxiway¹ or unassigned runway.
- Take-offs from a closed or engaged runway, from a taxiway¹ or unassigned runway.
- Landings or attempted landings on a closed or engaged runway, on a taxiway¹ or unassigned runway.
- Gross failures to achieve predicted performance during take-off or initial climb.
- Fires and smoke in the passenger compartment, in cargo compartments or engine fires, even though such fires were extinguished by the use of extinguishing agents.
- Events requiring the emergency use of oxygen by the flight crew.
- Aircraft structural failures or engine disintegrations not classified as an accident.

1. Excluding authorized operations by helicopters.

- Multiple malfunctions of one or more aircraft systems seriously affecting the operation of the aircraft.
 - Flight crew incapacitation in flight.
 - Fuel quantity requiring the declaration of an emergency by the pilot.
 - Runway incursions classified with severity A. The *Manual on the Prevention of Runway Incursions* (Doc 9870) contains information on the severity classifications.
 - Take-off or landing incidents. Incidents such as under-shooting, overrunning or running off the side of runways.
 - System failures, weather phenomena, operations outside the approved flight envelope or other occurrences which could have caused difficulties controlling the aircraft.
 - Failures of more than one system in a redundancy system mandatory for flight guidance and navigation.
-

Attachment B

EMERGENCY RESPONSE PLANNING

1. INTRODUCTION

1.1 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 response 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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.

2. ICAO REQUIREMENTS

2.1 Any organization conducting or supporting flight operations should have an emergency response plan. For example:

- a) 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 *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 on accidents involving company aircraft, guidance should also be provided on 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 *Airport Services Manual* (Doc 9137), Part 7 — *Airport Emergency Planning* gives guidance to both airport authorities and aircraft operators on pre-planning for emergencies, as well as on coordination between the different airport agencies, including the operator.

2.2 To be effective, an ERP should:

- 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.

3. ERP 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:

- a) **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.
- b) **Organization.** The ERP should outline management's intentions with respect to the responding organizations by:
 - 1) designating who will lead and who will be assigned to the response teams;
 - 2) defining the roles and responsibilities for personnel assigned to the response teams;
 - 3) clarifying the reporting lines of authority;
 - 4) setting up a crisis management centre (CMC);
 - 5) establishing procedures for receiving a large number of requests for information, especially during the first few days after a major accident;

- 6) designating the corporate spokesperson for dealing with the media;
- 7) defining what resources will be available, including financial authorities for immediate activities;
- 8) designating the company representative to any formal investigations undertaken by State officials;
and
- 9) defining a call-out plan for key personnel, etc.

An organization chart could be used to show organizational functions and communication relationships.

c) **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:

- 1) management;
- 2) State authorities (search and rescue, regulatory authority, accident investigation board, etc.);
- 3) local emergency response services (airport authorities, fire fighters, police, ambulances, medical agencies, etc.);
- 4) relatives of victims (a sensitive issue that, in many States, is handled by the police);
- 5) company personnel;
- 6) media; and
- 7) legal, accounting, insurers, etc.

d) **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:

- 1) Who should lead the initial response team?
- 2) Who should be included on the initial response team?
- 3) Who should speak for the organization at the accident site?
- 4) What would be required by way of special equipment, clothing, documentation, transportation, accommodation, etc.?

e) **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:

- 1) acting as passengers in crash exercises;
- 2) handling survivors;
- 3) dealing with next of kin, etc.

- f) **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:
- 1) staffing (perhaps for 24 hours a day, 7 days per week, during the initial response period);
 - 2) communications equipment (telephones, fax, Internet, etc.);
 - 3) documentation requirements, maintenance of emergency activity logs;
 - 4) impounding related company records;
 - 5) office furnishings and supplies; and
 - 6) reference documents (such as emergency response checklists and procedures, company manuals, airport emergency plans and telephone lists).

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.

- g) **Records.** In addition to the organization's need to maintain logs of events and activities, the organization will also be required to provide information to any State investigation team. The ERP should provide the following types of information to investigators:
- 1) all relevant records about the aircraft, the flight crew and the operation;
 - 2) lists of points of contact and any personnel associated with the occurrence;
 - 3) notes of any interviews (and statements) with anyone associated with the event;
 - 4) any photographic or other evidence.
- h) **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:
- 1) nominating a senior company representative at the accident site if:
 - at home base;
 - away from home base;
 - offshore or in a foreign State.
 - 2) management of surviving passengers;
 - 3) needs of relatives of victims;
 - 4) security of wreckage;
 - 5) handling of human remains and personal property of the deceased;

- 6) preservation of evidence;
 - 7) provision of assistance (as required) to the investigation authorities;
 - 8) removal and disposal of wreckage; etc.
- i) **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:
- 1) what information is protected by statute (FDR data, CVR and ATC recordings, witness statements etc.);
 - 2) 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);
 - 3) direction regarding a prepared statement for immediate response to media queries;
 - 4) what information may be released (what should be avoided);
 - 5) the timing and content of the company's initial statement;
 - 6) provisions for regular updates to the media.
- j) **Formal investigations.** Guidance for company personnel dealing with State accident investigators and police should be provided.
- k) **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:
- 1) State requirements for the provision of family assistance services;
 - 2) travel and accommodation arrangements to visit the accident location and survivors;
 - 3) programme coordinator and point(s) of contact for each family;
 - 4) provision of up-to-date information;
 - 5) grief counselling, etc.;
 - 6) immediate financial assistance to victims and their families;
 - 7) memorial services, etc.

Some States define the types of assistance to be provided by an operator.

- l) **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.
- m) **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.

4. AIRCRAFT OPERATOR'S RESPONSIBILITIES

4.1 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. As part of their emergency response planning, aircraft operators in conjunction with the airport operator are expected to:

- 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 coordinate fulfilment 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.).

4.2 In the event of an aircraft accident at or near the airport, operators will be expected to take such actions as:

- a) report to the 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.

5. 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 manual or emergency response manual. To be effective, checklists must be regularly:

- a) reviewed and updated (for example, currency of call-out lists and contact details); and
- b) tested through realistic exercises.

6. 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 call-out 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

MANUALS

Advanced Surface Movement Guidance and Control Systems (A-SMGCS) Manual (Doc 9830)

Aerodrome Design Manual (Doc 9157)

Airport Services Manual (Doc 9137)

Airworthiness Manual (Doc 9760)

Global Air Navigation Plan (Doc 9750)

Global Air Traffic Management Operational Concept (Doc 9854)

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)

Manual Concerning Interception of Civil Aircraft (Doc 9433)

Manual Concerning Safety Measures Relating to Military Activities Potentially Hazardous to Civil Aircraft Operations
(Doc 9554)

Manual of Aircraft Accident and Incident Investigation (Doc 9756)

Part I — *Organization and Planning*

Part III — *Investigation*¹

Part IV — *Reporting*

Manual of Aircraft Ground De-icing/Anti-icing Operations (Doc 9640)

Manual of All-Weather Operations (Doc 9365)

Manual of Civil Aviation Medicine (Doc 8984)

1. In preparation

Manual of Procedures for Operations Inspection, Certification and Continued Surveillance (Doc 8335)

Manual of Radiotelephony (Doc 9432)

Manual on Airspace Planning Methodology for the Determination of Separation Minima (Doc 9689)

Manual on Air Traffic Management System Requirements (Doc 9882)

Manual on Certification of Aerodromes (Doc 9774)

Manual on Global Performance of the Air Navigation System (Doc 9883)

Manual on ICAO Bird Strike Information Systems (IBIS) (Doc 9332)

Manual on Implementation of a 300 m (1 000 ft) Reduced Vertical Separation Minimum Between FL 290 and FL 410 Inclusive (Doc 9574)

Manual on Required Communication Performance (RCP) (Doc 9869)

Manual on Simultaneous Operations on Parallel or Near-Parallel Instrument Runways (SOIR) (Doc 9643)

Manual of Surface Movement Guidance and Control Systems (SMGCS) (Doc 9476)

Normal Operations Safety Survey (NOSS) (Doc 9910)

Performance-based Navigation Manual (Doc 9613)

Preparation of an Operations Manual (Doc 9376)

Safety Oversight Audit Manual (Doc 9735)

Safety Oversight Manual (Doc 9734)

CIRCULARS

Assessment of ADS-B to Support Air Traffic Services and Guidelines for Implementation (Cir 311)¹

A Unified Framework for Collision Risk Modelling in Support of the Manual on Airspace Planning Methodology with further applications (Cir 319)¹

Guidance on Assistance to Aircraft Accident Victims and Their Families (Cir 285)

Hazards at Aircraft Accident Sites (Cir 315)

Human Factors Digest No 15 — Human Factors in Cabin Safety (Cir 300)

Human Factors Digest No. 16 — Cross-cultural Factors in Aviation Safety (Cir 302)

1. In preparation

Human Factors Digest No. 17 — Threat and Error Management (TEM) in Air Traffic Control (Cir 314)

Operation of New Larger Aeroplanes at Existing Aerodromes (Cir 305)

Training Guidelines for Aircraft Accident Investigators (Cir 298)

MISCELLANEOUS

ADREP reporting (<http://www.icao.int/anb/aig/Reporting.html>)

— END —