

Doc 9859
AN/474



Safety Management Manual (SMM)

Approved by the Secretary General
and published under his authority

Third Edition — 2013

International Civil Aviation Organization

www.icao.int/publications

.....



Doc 9859
AN/474



Safety Management Manual (SMM)

**Approved by the Secretary General
and published under his authority**

Third Edition — 2013

International Civil Aviation Organization

Published in separate English, Arabic, Chinese, 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.

First edition 2006
Second edition 2009
Third edition 2013

Doc 9859, Safety Management Manual (SMM)

Order Number: 9859

ISBN 978-92-9249-214-4

© ICAO 2013

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.

AMENDMENTS

Amendments are announced in the supplements to the *Catalogue of ICAO Publications*; the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

[illegible][illegible]

TABLE OF CONTENTS

	<i>Page</i>
Glossary	(ix)
Acronyms and abbreviations	(ix)
Definitions.....	(xii)
Chapter 1. Overview of the Manual	1-1
1.1 General.....	1-1
1.2 Objective	1-1
1.3 Structure.....	1-2
Chapter 2. Safety Management Fundamentals	2-1
2.1 The concept of safety	2-1
2.2 The evolution of safety	2-1
2.3 Accident causation	2-2
2.4 People, context and safety	2-6
2.5 Errors and violations.....	2-8
2.6 Safety culture	2-10
2.7 The management dilemma.....	2-13
2.8 Change management.....	2-14
2.9 Integration of management systems.....	2-15
2.10 Safety reporting and investigation	2-16
2.11 Safety data collection and analysis	2-18
2.12 Safety indicators and performance monitoring	2-23
2.13 Hazards.....	2-23
2.14 Safety risk.....	2-26
2.15 Safety risk management.....	2-30
2.16 Prescriptive and performance-based requirements.....	2-32
Appendix 1 to Chapter 2. Organization Safety Culture (OSC)/Organization Risk Profile (ORP) Assessment Checklist — Air Operators	2-App 1-1
Appendix 2 to Chapter 2. Example of a Safety Risk Mitigation Worksheet.....	2-App 2-1
Appendix 3 to Chapter 2. Illustration of a Hazard Prioritization Procedure	2-App 3-1
Chapter 3. ICAO Safety Management SARPS	3-1
3.1 Introduction.....	3-1
3.2 State safety management requirements.....	3-1

	Page
3.3 Service providers' safety management requirements.....	3-2
3.4 New Annex 19 — <i>Safety Management</i>	3-4
Chapter 4. State Safety Programme (SSP)	4-1
4.1 Introduction.....	4-1
4.2 SSP framework	4-1
SSP Component 1. State safety policy and objectives	4-2
SSP Element 1.1 State safety legislative framework	4-2
SSP Element 1.2 State safety responsibilities and accountabilities	4-3
SSP Element 1.3 Accident and incident investigation	4-4
SSP Element 1.4 Enforcement policy	4-4
SSP Component 2. State safety risk management	4-5
SSP Element 2.1 Safety requirements for the service provider's SMS	4-5
SSP Element 2.2 Agreement on the service provider's safety performance	4-5
SSP Component 3. State safety assurance	4-6
SSP Element 3.1 Safety oversight	4-6
SSP Element 3.2 Safety data collection, analysis and exchange	4-7
SSP Element 3.3 Safety-data-driven targeting of oversight of areas of greater concern or need	4-8
SSP Component 4. State safety promotion	4-9
SSP Element 4.1 Internal training, communication and dissemination of safety information.....	4-9
SSP Element 4.2 External training, communication and dissemination of safety information.....	4-10
4.3 SSP implementation planning	4-10
4.3.1 General.....	4-10
4.3.2 Regulatory system description.....	4-11
4.3.3 Gap analysis.....	4-11
4.3.4 SSP implementation plan	4-11
4.3.5 Safety indicators	4-11
4.4 SSP implementation — Phased approach	4-13
Phase 1	4-14
Phase 2	4-17
Phase 3	4-18
Phase 4	4-19
Appendix 1 to Chapter 4. Guidance on the development of a State safety policy statement.....	4-App 1-1
Appendix 2 to Chapter 4. Guidance on a State's voluntary and confidential reporting system.....	4-App 2-1
Appendix 3 to Chapter 4. Example of a State's mandatory reporting procedure	4-App 3-1
Appendix 4 to Chapter 4. SSP safety performance indicators	4-App 4-1
Appendix 5 to Chapter 4. Safety information protection	4-App 5-1
Appendix 6 to Chapter 4. Guidance on accident and incident notification and reporting	4-App 6-1

	<i>Page</i>
Appendix 7 to Chapter 4. SSP gap analysis checklist and implementation plan	4-App 7-1
Appendix 8 to Chapter 4. Sample contents of an SSP document	4-App 8-1
Appendix 9 to Chapter 4. Example of a State SMS Regulation	4-App 9-1
Appendix 10 to Chapter 4. Sample State enforcement policy	4-App 10-1
Appendix 11 to Chapter 4. Guidance on State enforcement procedures in an SSP-SMS environment	4-App 11-1
Appendix 12 to Chapter 4. Example of an SMS regulatory acceptance/assessment checklist	4-App 12-1
 Chapter 5. Safety Management System (SMS).....	 5-1
5.1 Introduction.....	5-1
5.2 Scope	5-1
5.3 SMS framework	5-2
SMS Component 1. Safety policy and objectives	5-3
SMS Element 1.1 Management commitment and responsibility	5-3
SMS Element 1.2 Safety accountabilities	5-7
SMS Element 1.3 Appointment of key safety personnel	5-9
SMS Element 1.4 Coordination of emergency response planning	5-12
SMS Element 1.5 SMS documentation	5-12
SMS Component 2. Safety risk management.....	5-14
SMS Element 2.1 Hazard identification.....	5-14
SMS Element 2.2 Safety risk assessment and mitigation	5-18
SMS Component 3. Safety assurance.....	5-21
SMS Element 3.1 Safety performance monitoring and measurement	5-22
SMS Element 3.2 The management of change	5-23
SMS Element 3.3 Continuous improvement of the SMS.....	5-24
SMS Component 4. Safety promotion	5-25
SMS Element 4.1 Training and education.....	5-25
SMS Element 4.2 Safety communication	5-27
5.4 SMS implementation planning.....	5-27
5.4.1 System description	5-27
5.4.2 Integration of management systems.....	5-28
5.4.3 Gap analysis.....	5-29
5.4.4 SMS implementation plan.....	5-30
5.4.5 Safety performance indicators	5-30
5.5 Phased implementation approach	5-31
5.5.1 General.....	5-31
5.5.2 Phase 1	5-32
5.5.3 Phase 2	5-34
5.5.4 Phase 3	5-36
5.5.5 Phase 4	5-38
5.5.6 SMS elements progressively implemented throughout Phases 1 to 4.....	5-39
 Appendix 1 to Chapter 5. Electronic signatures.....	 5-App 1-1

	Page
Appendix 2 to Chapter 5. Sample job description for a safety manager	5-App 2-1
Appendix 3 to Chapter 5. Emergency response planning.....	5-App 3-1
Appendix 4 to Chapter 5. Guidance on the development of an SMS manual.....	5-App 4-1
Appendix 5 to Chapter 5. Voluntary and confidential reporting systems.....	5-App 5-1
Appendix 6 to Chapter 5. SMS safety performance indicators	5-App 6-1
Appendix 7 to Chapter 5. SMS gap analysis checklist and implementation plan.....	5-App 7-1
Attachment. Related ICAO guidance material	Att-1

Full document details: ICAO 9859 2013

GLOSSARY

ACRONYMS AND ABBREVIATIONS

AD	Airworthiness directive
ADREP	Accident/incident data reporting (ICAO)
AIB	Accident investigation board
AIR	Airworthiness
ALoSP	Acceptable level of safety performance
AMAN	Abrupt manoeuvring
AME	Aircraft maintenance engineer
AMO	Approved maintenance organization`
AMS	Aircraft maintenance schedule
ANS	Air navigation service
AOC	Air operator certificate
AOG	Aircraft on ground
ASB	Alert service bulletin
ATC	Air traffic control
ATM	Air traffic management
ATS	Air traffic service(s)
CAA	Civil aviation authority
CAN	Corrective action notice
CBA	Cost-benefit analysis
CEO	Chief executive officer
CFIT	Controlled flight into terrain
Cir	Circular
CM	Condition monitoring
CMA	Continuous monitoring approach
CMC	Crisis management centre
CNS	Communications, navigation and surveillance
CP	Command post
CRM	Crew resource management
CVR	Cockpit voice recorder
D&M	Design and manufacturing
DGR	Dangerous goods regulation
DMS	Document management system
DOA	Design organization approval
Doc	Document
EAD	Emergency airworthiness directive
EC	Escalation control
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems
EDTO	Extended diversion time operation
EF	Escalation factor
EMC	Emergency management centre

EMS	Environmental management system
ERP	Emergency response plan
FDR	Flight data recorder
FH	Flying hours
FIR	Flight information region
FL	Flight level
FMS	Financial management system
FRMS	Fatigue risk management systems
FTL	Flight time limitation
FTM	Fleet technical management
GAQ	Gap analysis questionnaire
H	Hazard
HF	Human factors
HIRA	Hazard identification and risk assessment
HIRM	Hazard identification and risk mitigation
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IFSD	In-flight shutdown
ILS	Instrument landing system
IMC	Instrument meteorological conditions
ISO	International Organization for Standardization
iSTARS	Integrated Safety Trend and Reporting System
ITM	Inventory technical management
kg	Kilogram(s)
LEI	Lack of effective implementation
LOC-I	Loss of control in flight
LOFT	Line-oriented flight training
LOS	Loss of separation
LOSA	Line operations safety audit
LRU	Line replaceable unit
LSI	Line station inspection
MCM	Maintenance control manual
MDR	Mandatory defect report
MEDA	Maintenance error decision aid
MEL	Minimum equipment list
MFF	Mixed fleet flying
MOR	Mandatory occurrence report
MPD	Maintenance planning document
MRM	Maintenance resource management
MRO	Maintenance repair organization
MSL	Mean sea level
N/A	Not applicable

OEM	Original equipment manufacturer
OHSMS	Occupational health and safety management system
OPS	Operations
ORP	Organization risk profile
OSC	Organization safety culture
OSHE	Occupational safety, health and environment
PC	Preventive control
PMI	Principal maintenance inspector
POA	Production organization approval
POI	Principal operations inspector
QA	Quality assurance
QC	Quality control
QM	Quality management
QMS	Quality management system
RAIO	Regional accident and incident investigation organization
RM	Recovery measure
RSOO	Regional safety oversight organization
SA	Safety assurance
SAG	Safety action group
SARPs	Standards and Recommended Practices (ICAO)
SB	Service bulletin
SCF-NP	System component failure — non-powerplant
SD	Standard deviation
SDCPS	Safety data collection and processing system
SeMS	Security management system
SHEL	Software/hardware/environment/liveware
SM	Safety management
SMM	Safety management manual
SMP	Safety Management Panel
SMS	Safety management system(s)
SOPs	Standard operating procedures
SPI	Safety performance indicator
SRB	Safety review board
SRC	Safety review committee
SRM	Safety risk management
SSO	Safety services office
SSP	State safety programme
STDEVP	Population standard deviation
TBD	To be determined
TOR	Terms of reference
UC	Ultimate consequence
UE	Unsafe event
USOAP	Universal Safety Oversight Audit Programme (ICAO)
WIP	Work in progress

DEFINITIONS

Note.— The following definitions were developed while new Annex 19 — Safety Management was being drafted. Once Annex 19 becomes applicable in November 2013, if there should be any differences in the definitions, the Annex 19 definitions shall prevail.

Acceptable level of safety performance (ALoSP). The minimum level of safety performance of civil aviation in a State, as defined in its State safety programme, or of a service provider, as defined in its safety management system, expressed in terms of safety performance targets and safety performance indicators.

Accountable executive. A single, identifiable person having responsibility for the effective and efficient performance of the State's SSP or of the service provider's SMS.

Change management. A formal process to manage changes within an organization in a systematic manner, so that changes which may impact identified hazards and risk mitigation strategies are accounted for, before the implementation of such changes.

Defences. Specific mitigating actions, preventive controls or recovery measures put in place to prevent the realization of a hazard or its escalation into an undesirable consequence.

Errors. An action or inaction by an operational person that leads to deviations from organizational or the operational person's intentions or expectations.

High-consequence indicators. Safety performance indicators pertaining to the monitoring and measurement of high-consequence occurrences, such as accidents or serious incidents. High-consequence indicators are sometimes referred to as reactive indicators.

Lower-consequence indicators. Safety performance indicators pertaining to the monitoring and measurement of lower-consequence occurrences, events or activities such as incidents, non-conformance findings or deviations. Lower-consequence indicators are sometimes referred to as proactive/predictive indicators.

Risk mitigation. The process of incorporating defences or preventive controls to lower the severity and/or likelihood of a hazard's projected consequence.

Safety management system. A systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.

Safety performance. A State's or service provider's safety achievement as defined by its safety performance targets and safety performance indicators.

Safety performance indicator. A data-based safety parameter used for monitoring and assessing safety performance.

Safety risk. The predicted probability and severity of the consequences or outcomes of a hazard.

State safety programme. An integrated set of regulations and activities aimed at improving safety.

Chapter 1

OVERVIEW OF THE MANUAL

1.1 GENERAL

1.1.1 This third edition of the ICAO *Safety Management Manual (SMM)* (Doc 9859) supersedes the second edition, published in 2009, in its entirety. It also supersedes the ICAO *Accident Prevention Manual* (Doc 9422), which is obsolete.

1.1.2 This manual is intended to provide States with guidance on the development and implementation 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*, Volume I — *Aerodrome Design and Operations*. It should be noted that SSP provisions will be incorporated into Annex 19 — *Safety Management*, which was still under development at the time this third edition was published. This manual also provides guidance material for the establishment of safety management system (SMS) requirements by States as well as for SMS development and implementation by affected product and service providers.

1.1.3 It should be noted that this manual is intended to be used in conjunction with other appropriate guidance material which can be used to complement or enhance the concepts or guidance in this document.

Note.— In the context of safety management, the term “service provider” or “product and service provider” refers to any organization providing aviation products and/or 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.

1.2 OBJECTIVE

The objective of this manual is to provide States and product and service providers with:

- a) an overview of safety management fundamentals;
- b) a summary of ICAO safety management SARPs contained in Annexes 1, 6, 8, 11, 13 and 14;
- c) guidance on how to develop and implement an SSP in compliance with the relevant ICAO SARPs, including a harmonized regulatory framework for the oversight of product and service providers' SMS; and
- d) guidance on SMS development, implementation and maintenance.

1.3 STRUCTURE

Chapter 1 presents an overview of the manual while Chapter 2 discusses the fundamental safety management concepts and processes. Chapter 3 provides a compilation of the ICAO safety management SARPs contained in Annexes 1, 6, 8, 11, 13 and 14. Finally, Chapters 4 and 5 outline a progressive approach to the development, implementation and maintenance of an SSP and an SMS. The last two chapters also contain appendices which provide practical guidance and illustrations. The Attachment to the manual provides a list of related ICAO guidance material.

Note.— In this manual, the use of the male gender should be understood to include both male and female persons.

Chapter 2

SAFETY MANAGEMENT FUNDAMENTALS

Note.— This chapter provides an overview of fundamental safety management concepts and practices applicable to implementation of State safety programmes as well as the implementation and oversight of safety management systems by product and service providers. The content of this chapter is provided for introductory purposes with further details on these topics found throughout subsequent chapters of this manual.

2.1 THE CONCEPT OF SAFETY

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

2.1.2 While the elimination of aircraft accidents and/or serious incidents remains the ultimate goal, it is recognized that the aviation system cannot be completely free of hazards and associated risks. Human activities or human-built systems cannot be guaranteed to be absolutely free from operational errors and their consequences. Therefore, safety is a dynamic characteristic of the aviation system, whereby safety risks must be continuously mitigated. It is important to note that the acceptability of safety performance is often influenced by domestic and international norms and culture. As long as safety risks are kept under an appropriate level of control, a system as open and dynamic as aviation can still be managed to maintain the appropriate balance between production and protection.

2.2 THE EVOLUTION OF SAFETY

The history of the progress in aviation safety can be divided into three eras.

- a) *The technical era — from the early 1900s until the late 1960s.* Aviation emerged as a form of mass transportation in which identified safety deficiencies were initially related to technical factors and technological failures. The focus of safety endeavours was therefore placed on the investigation and improvement of technical factors. By the 1950s, technological improvements led to a gradual decline in the frequency of accidents, and safety processes were broadened to encompass regulatory compliance and oversight.
- b) *The human factors era — from the early 1970s until the mid-1990s.* In the early 1970s, the frequency of aviation accidents was significantly reduced due to major technological advances and enhancements to safety regulations. Aviation became a safer mode of transportation, and the focus of safety endeavours was extended to include human factors issues including the man/machine interface. This led to a search for safety information beyond that which was generated by the earlier accident investigation process. Despite the investment of resources in error mitigation, human performance continued to be cited as a recurring factor in accidents (Figure 2-1). The application of human factors science tended to focus on the individual, without fully considering the operational and organizational context. It was not until the early 1990s that it was first acknowledged that individuals operate in a complex environment, which includes multiple factors having the potential to affect behaviour.

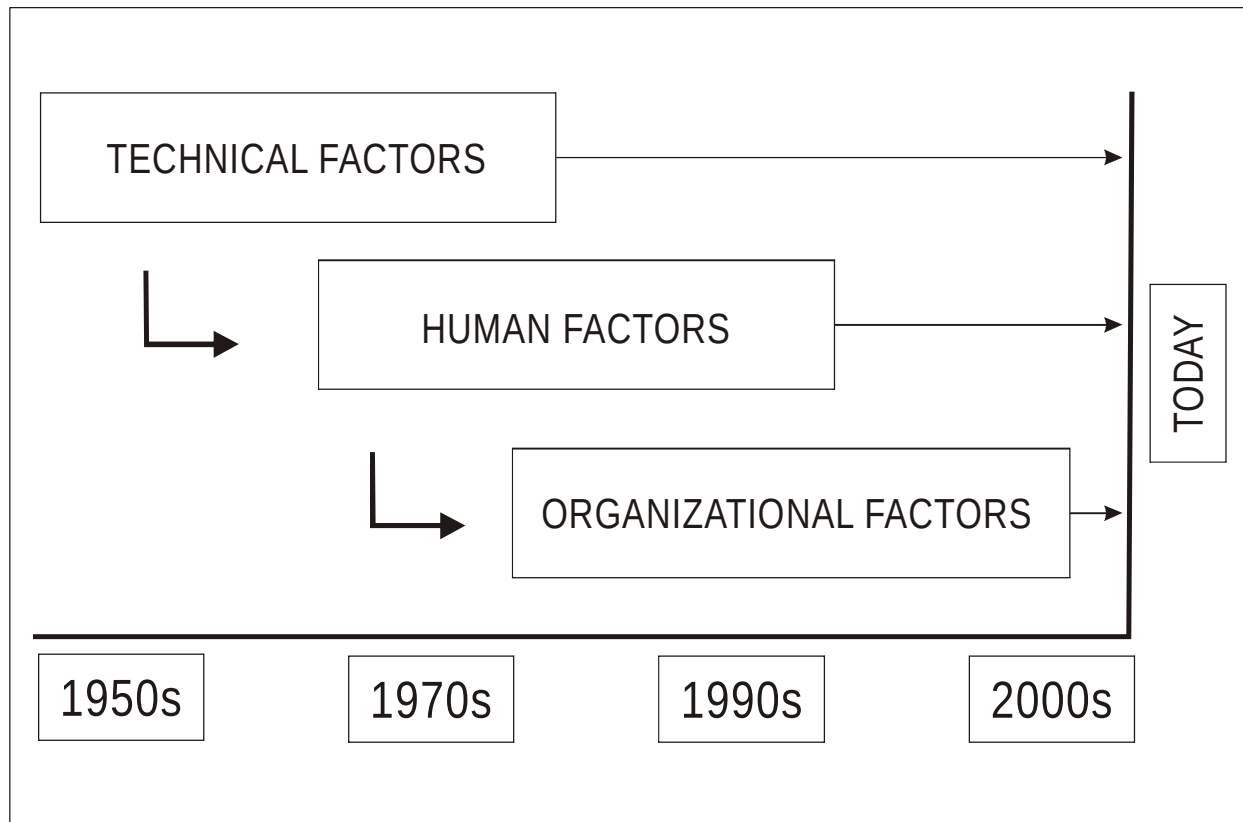


Figure 2-1. The evolution of safety

- c) *The organizational era — from the mid-1990s to the present day.* During the organizational era safety began to be viewed from a systemic perspective, which was to encompass organizational factors in addition to human and technical factors. As a result, the notion of the “organizational accident” was introduced, considering the impact of organizational culture and policies on the effectiveness of safety risk controls. Additionally, traditional data collection and analysis efforts, which had been limited to the use of data collected through investigation of accidents and serious incidents, were supplemented with a new proactive approach to safety. This new approach is based on routine collection and analysis of data using proactive as well as reactive methodologies to monitor known safety risks and detect emerging safety issues. These enhancements formulated the rationale for moving towards a safety management approach.

2.3 ACCIDENT CAUSATION

2.3.1 The “Swiss-Cheese” Model, developed by Professor James Reason, illustrates that accidents involve successive breaches of multiple system defences. These breaches can be triggered by a number of enabling factors such as equipment failures or operational errors. Since the Swiss-Cheese Model contends that complex systems such as aviation are extremely well defended by layers of defences, single-point failures are rarely consequential in such systems. Breaches in safety defences can be a delayed consequence of decisions made at the highest levels of the system, which may remain dormant until their effects or damaging potential are activated by specific operational

circumstances. Under such specific circumstances, human failures or active failures at the operational level act to breach the system's inherent safety defences. The Reason Model proposes that all accidents include a combination of both active and latent conditions.

2.3.2 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 harmful outcome.

2.3.3 Latent conditions are those that exist in the aviation system well before a damaging outcome is experienced. The consequences of latent conditions may remain dormant for a long time. Initially, these latent conditions are not perceived as harmful, but will 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. Latent conditions in the system may include those created by a lack of safety culture; poor equipment or procedural design; conflicting organizational goals; defective organizational systems or management decisions. The perspective underlying the organizational accident aims to identify and mitigate these latent conditions on a system-wide basis, rather than through localized efforts to minimize active failures by individuals.

2.3.4 Figure 2-2 shows how the Swiss-Cheese Model assists in understanding the interplay of organizational and managerial factors in accident causation. It illustrates that various defences are built into the aviation system to protect against fluctuations in human performance or decisions at all levels of the system. While these defences act to protect against the safety risks, breaches that penetrate all defensive barriers may potentially result in a catastrophic situation. Additionally, Reason's Model represents how latent conditions are ever present within the system prior to the accident and can manifest through local triggering factors.

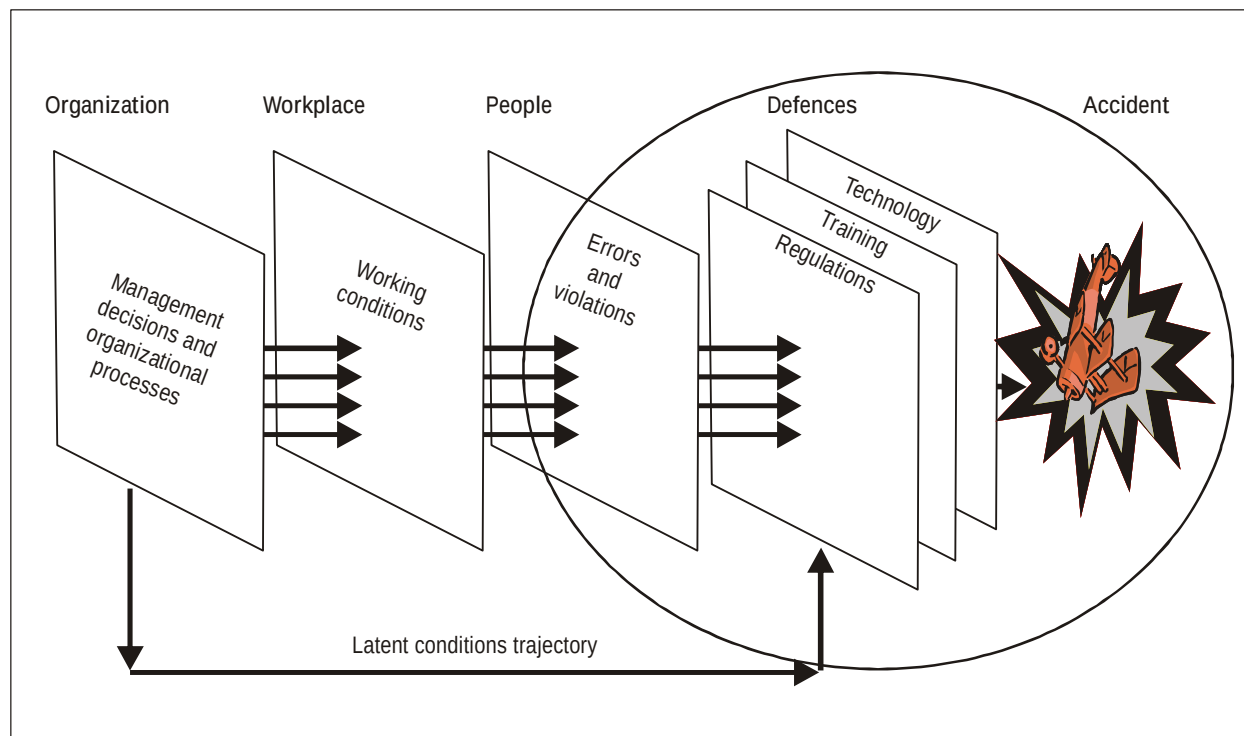


Figure 2-2. The concept of accident causation

The organizational accident

2.3.5 The notion of the organizational accident underlying Reason's Model can be best understood through a building-block approach, consisting of five blocks (Figure 2-3). 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, and supervision. 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.

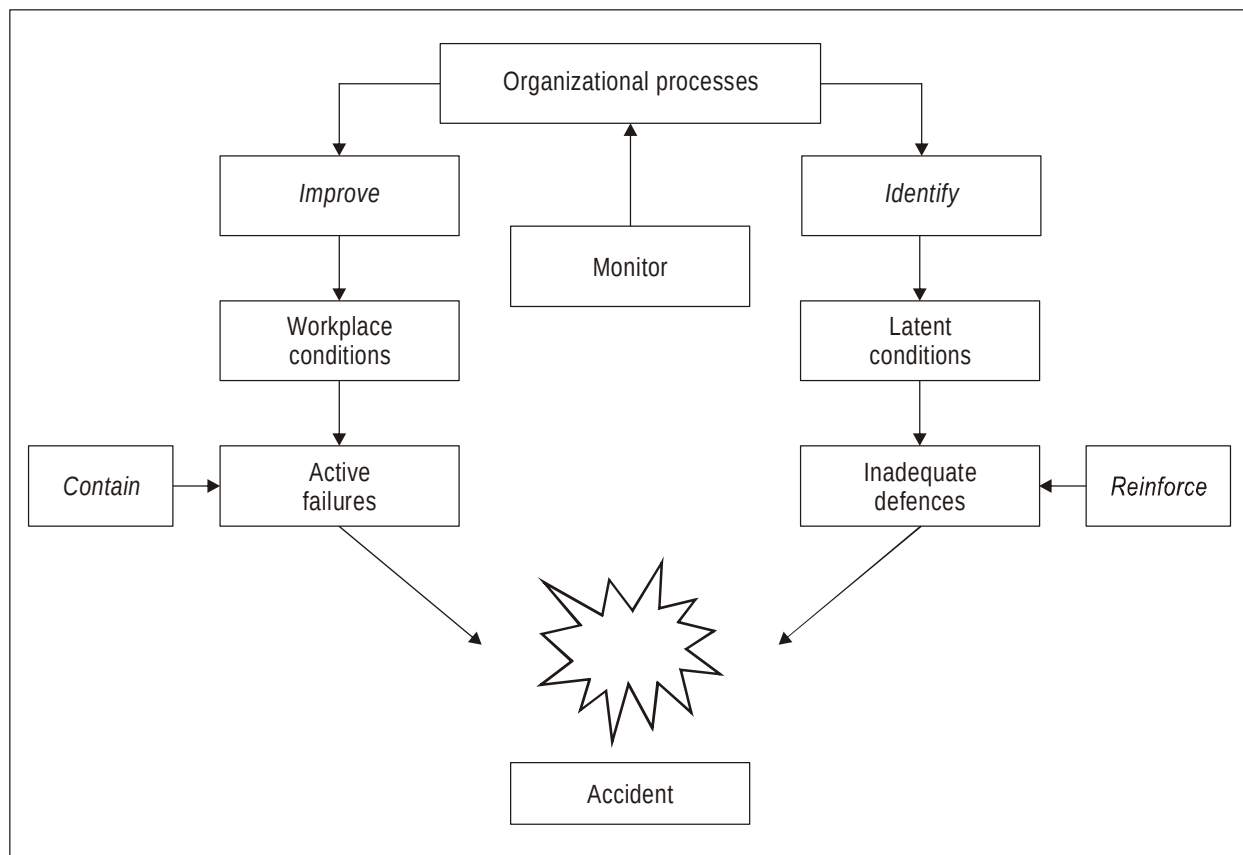


Figure 2-3 The organizational accident

2.3.6 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.

2.3.7 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.

2.3.8 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.

2.3.9 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.

2.3.10 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, while accomplishing a task, willingly deviates from rules, procedures or training received commits a violation. Thus, the basic difference between errors and violation is intent.

2.3.11 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 combination of all these factors that produces safety breakdowns.

The practical drift

2.3.12 Scott A. Snook's theory of practical drift is used as the basis to understand how, in aviation, the baseline performance of any system "drifts away" from its original design when the organization's processes and procedures cannot anticipate all situations that may arise in daily operations.

2.3.13 During the early stages of system design (e.g. ATC airspace, introduction of specific equipment, expansion of a flight operation scheme), operational interactions between people and technology, as well as the operational context, are taken into consideration to identify the expected performance limitations as well as potential hazards. The initial system design is based on three fundamental assumptions: the technology needed to achieve the system production goals is available, the people are trained to properly operate the technology, and the regulations and procedures will dictate system and human behaviour. These assumptions underlie the baseline (or ideal) system performance, which can be graphically presented as a straight line from the date of operational deployment until the system is decommissioned (Figure 2-4).

2.3.14 Once operationally deployed, the system performs as designed, following baseline performance most of the time. In reality, however, operational performance is different from baseline performance as a consequence of real-life operations and changes in the operational and regulatory environment. Since the drift is a consequence of daily practice, it is referred to as a "practical drift". The term "drift" is used in this context as the gradual departure from an intended course due to external influences.

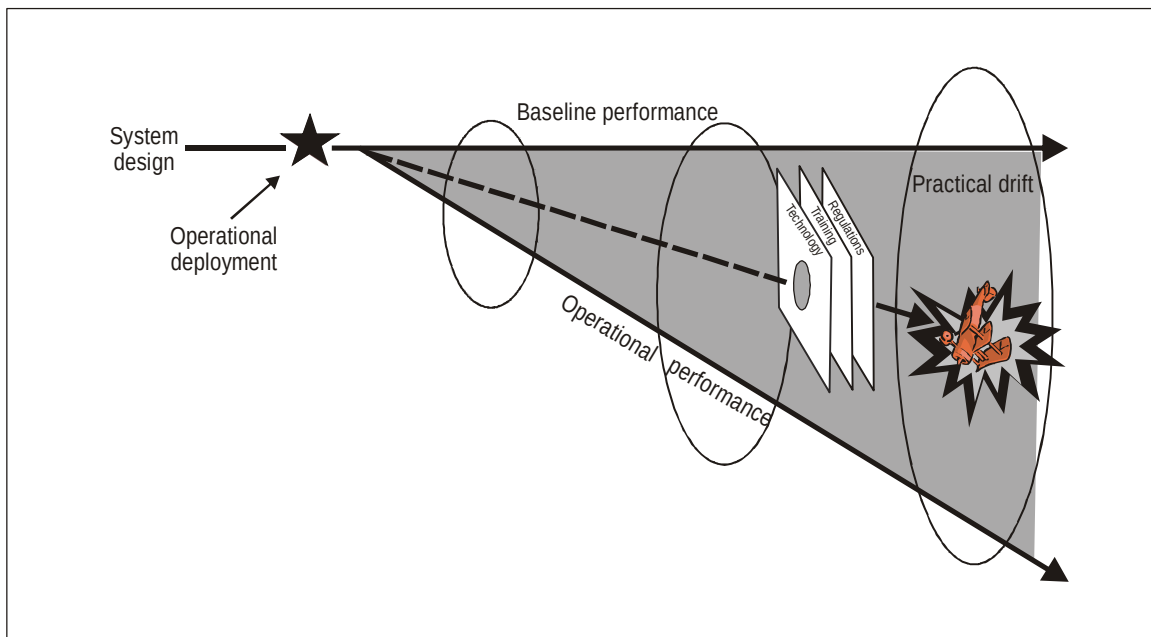


Figure 2-4. The practical drift

2.3.15 A practical drift from baseline performance to operational performance is foreseeable in any system, no matter how careful and well thought out its design planning may have been. Some of the reasons for the practical drift may include: technology that does not always operate as predicted; procedures that cannot be executed as planned under certain operational conditions; regulations that are not applicable within certain contextual limitations; introduction of changes to the system, including the addition of new components; the interaction with other systems; and so forth. The fact remains however that, despite all the system's shortcomings leading to the drift, people operating inside the practical drift make the system work on a daily basis, applying local adaptations (or workarounds) and personal strategies "beyond what the book says".

2.3.16 As explained in Figure 2-4, capturing and analysing the information on what takes place within the practical drift holds considerable learning potential about successful safety adaptations and, therefore, for the control and mitigation of safety risks. The closer to the beginning of the practical drift that the information can be systematically captured, the greater the number of hazards and safety risks that can be predicted and addressed, leading to formal interventions for re-design of or improvements to the system. However, the unchecked proliferation of local adaptations and personal strategies may lead the practical drift to depart too far from the expected baseline performance, to the extent that an incident or an accident becomes a greater possibility.

2.4 PEOPLE, CONTEXT AND SAFETY

2.4.1 The aviation system includes product and service providers and State organizations. It is a complex system that requires an assessment of the human contribution to safety and an understanding of how human performance may be affected by its multiple and interrelated components.

2.4.2 The SHELL Model is a conceptual tool used to analyse the interaction of multiple system components. Figure 2-5 provides a basic depiction of the relationship between humans and other workplace components. The SHELL Model contains the following four components:

- a) *Software (S)*: procedures, training, support, etc.;
- b) *Hardware (H)*: machines and equipment;
- c) *Environment (E)*: the working environment in which the rest of the L-H-S system must function; and
- d) *Liveware (L)*: humans in the workplace.

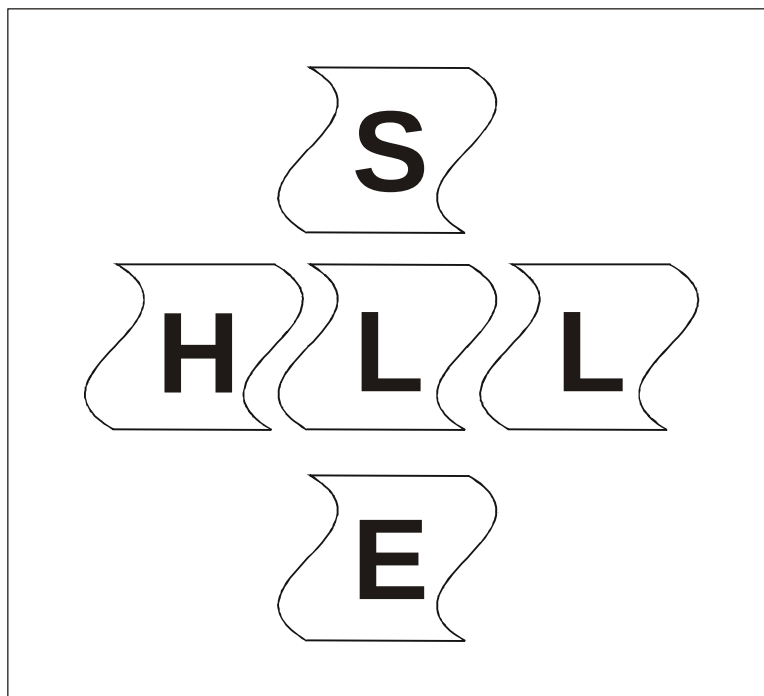


Figure 2-5. The SHELL model — components and interfaces

2.4.3 *Liveware*. In the centre of the SHELL 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 SHELL 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. The SHELL Model is useful in visualizing the following interfaces between the various components of the aviation system:

- a) *Liveware-Hardware (L-H)*. The L-H interface refers to the relationship between the human and the physical attributes of equipment, machines and facilities. The interface between the human and

technology is commonly considered with reference to human performance in the context of aviation operations, and there is a natural human tendency to adapt to L-H mismatches. Nonetheless, this tendency has the potential to mask serious deficiencies, which may become evident only 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 issues as recency of experience, accuracy, format and presentation, vocabulary, clarity and symbology.
- c) *Liveware-Liveware (L-L)*. The L-L interface is the relationship among persons in the work environment. Since flight crews, air traffic controllers, aircraft maintenance engineers and other operational personnel function in groups, it is important to recognize that communication and interpersonal skills, as well as group dynamics, play a role in determining human performance. The advent of crew resource management (CRM) and its extension to air traffic services (ATS) and maintenance operations has created a focus on the management of operational errors across multiple aviation domains. Staff/management relationships as well as overall organizational culture are also within the scope of this interface.
- 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 operational aspects such as weather factors, aviation infrastructure and terrain. This interface also involves the relationship between the human internal environment and its external environment. Psychological and physiological forces, including illness, fatigue, financial uncertainties, and relationship and career concerns, can be either induced by the L-E interaction or originate from external secondary sources. The aviation work environment includes disturbances to normal biological rhythms and sleep patterns. Additional environmental aspects may be related to organizational attributes that may affect decision-making processes and create pressures to develop "workarounds" or minor deviations from standard operating procedures.

2.4.4 According to the SHELL Model, a mismatch between the Liveware and the other four components contributes to human error. Thus, these interactions must be assessed and considered in all sectors of the aviation system.

2.5 ERRORS AND VIOLATIONS

2.5.1 Effective SMS implementation by the product or service provider as well as effective SMS oversight by the State are both dependent upon a clear, mutual understanding of errors and violations and the differentiation between the two. The difference between errors and violations lies in intent. While an error is unintentional, a violation is a deliberate act or omission to deviate from established procedures, protocols, norms or practices.

2.5.2 Errors or violations may result in non-compliance with regulations or approved operating procedures. Punitive measures taken in response to acts of non-compliance may lead to a reduction in the reporting of errors in the absence of other processes. Accordingly, the State and the product or service provider must consider whether acts of non-compliance are the result of a violation or inadvertent error when determining whether punitive action is appropriate, with the criteria normally being whether non-compliance is the result of wilful misconduct or gross negligence.

Errors

2.5.3 As indicated previously, an error is defined as “an action or inaction by an operational person that leads to deviations from organizational or the operational person’s intentions or expectations”. In the context of an SMS, both the State and the product or service provider must understand and expect that humans will commit errors regardless of the level of technology used, the level of training or the existence of regulations, processes and procedures. An important goal then is to set and maintain defences to reduce the likelihood of errors and, just as importantly, reduce the consequences of errors when they do occur. To effectively accomplish this task, errors must be identified, reported and analysed so that appropriate remedial action can be taken. Errors can be divided into the two following categories:

- a) *Slips and lapses* are failures in the execution of the intended action. Slips are actions that do not go as planned, while lapses are memory failures. For example, operating the flap lever instead of the (intended) gear lever is a slip. Forgetting a checklist item is a lapse.
- b) *Mistakes* are failures in the plan of action. Even if execution of the plan were correct, it would not have been possible to achieve the intended outcome.

2.5.4 Safety strategies must be put into place to control or eliminate errors. The strategies to control errors leverage the basic defences within the aviation system. These include the following:

- a) *Reduction strategies* provide direct intervention to reduce or eliminate the factors contributing to the error. Examples of reduction strategies include improvement of ergonomic factors and reduction of environmental distractions.
- b) *Capturing strategies* assume the error will be made. The intent is to “capture” the error before any adverse consequences of the error are felt. Capturing strategies are different from reduction strategies in that they utilize checklists and other procedural interventions rather than directly eliminating the error.
- c) *Tolerance strategies* refer to the ability of a system to accept that an error will be made but without experiencing serious consequences. The incorporation of redundant systems or multiple inspection processes are examples of measures that increase system tolerance to errors.

2.5.5 Since the performance of personnel is generally influenced by organizational, regulatory and environmental factors, safety risk management must include consideration of organizational policies, processes and procedures related to communication, scheduling of personnel, allocation of resources and budgeting constraints that may contribute to the incidence of errors.

Violations

2.5.6 A violation is defined as “a deliberate act of wilful misconduct or omission resulting in a deviation from established regulations, procedures, norms or practices”. Nonetheless, non-compliance is not necessarily the result of a violation because deviations from regulatory requirements or operating procedures may be the result of an error. To further complicate the issue, while violations are intentional acts, they are not always acts of malicious intent. Individuals may knowingly deviate from norms, in the belief that the violation facilitates mission achievement without creating adverse consequences. Violations of this nature are errors in judgement and may not automatically result in disciplinary measures depending on the policies in place. Violations of this type can be categorized as follows:

- a) *Situational violations* are committed in response to factors experienced in a specific context, such as time pressure or high workload.

- b) *Routine violations* become the normal way of doing business within a work group. Such violations are committed in response to situations in which compliance with established procedures makes task completion difficult. This may be due to practicality/workability issues, deficiencies in human-technology interface design and other issues that cause persons to adopt “workaround” procedures, which eventually become routine. These deviations, referred to as “drift,” may continue without consequence, but over time they may become frequent and result in potentially severe consequences. In some cases routine violations are well grounded and may result in the incorporation of the routine violation as an accepted procedure after a proper safety assessment has been conducted and it is shown that safety is not compromised.
- c) *Organizationally induced violations* may be considered as an extension of routine violations. This type of violation tends to occur when an organization attempts to meet increased output demands by ignoring or stretching its safety defences.

2.6 SAFETY CULTURE

2.6.1 Culture is characterized by the beliefs, values, biases and their resultant behaviour that are shared by members of a society, group or organization. An understanding of these cultural components, and the interaction between them, is important to safety management. The three most influential cultural components are organizational, professional and national cultures. A reporting culture is a key component of these different cultures. The mix of cultural components may vary greatly among organizations and can negatively influence effective hazard reporting, collaborative root-cause analysis and acceptable risk mitigation. Continuous improvement in safety performance is possible when safety becomes a value within an organization as well as a priority at the national or professional level.

2.6.2 A safety culture encompasses the commonly held perceptions and beliefs of an organization's members pertaining to the public's safety and can be a determinant of the behaviour of the members. A healthy safety culture relies on a high degree of trust and respect between personnel and management and must therefore be created and supported at the senior management level.

2.6.3 A healthy safety culture actively seeks improvements, vigilantly remains aware of hazards and utilizes systems and tools for continuous monitoring, analysis and investigation. It must exist in State aviation organizations as well as in product and service provider organizations. Other characteristics of a healthy safety culture include a shared commitment by personnel and management to personal safety responsibilities, confidence in the safety system, and a documented set of rules and policies. The ultimate responsibility for the establishment and adherence to sound safety practices rests with the management of the organization. A safety culture cannot be effective unless it is embedded within an organization's own culture.

2.6.4 *Organizational culture* refers to the characteristics and safety perceptions among members interacting within a particular entity. Organizational value systems include prioritization or balancing policies covering areas such as productivity versus quality, safety versus efficiency, financial versus technical, professional versus academic, and enforcement versus corrective action.

2.6.5 The greatest potential for the creation and maintenance of an effective, self-sustaining culture for the management of safety is at the organizational level. The organization is a major determinant of the behaviour in which persons will engage while performing management or operational activities during the delivery or oversight of aviation activities. Organizational culture sets the boundaries for accepted executive and operational performance by establishing the norms and limits. Thus, organizational culture provides a cornerstone for managerial and employee decision making.

2.6.6 Organizational culture has the potential to affect the following:

- a) interactions between senior and junior members of a group;
- b) interactions between industry and regulatory authority personnel;
- c) the degree to which information is shared internally and with the regulatory authorities;
- d) the prevalence of teamwork in the regulatory authority or industry organization;
- e) reactions of personnel under demanding operational conditions;
- f) the acceptance and utilization of particular technologies; and
- g) the tendency to take punitive measures in reaction to operational errors within a product or service provider or by the regulatory authorities.

2.6.7 Organizational culture is also affected by factors such as:

- a) business policies and procedures;
- b) supervisory behaviour and practices;
- c) safety improvement goals as well as minimum tolerance levels;
- d) management's attitude toward quality or safety issues;
- e) employee training and motivation;
- f) the relationship between the regulatory authorities and product and service providers; and
- g) policies on work/life balance.

2.6.8 The way in which management deals with day-to-day safety issues is also fundamental to improving organizational culture. Collaborative interaction between front-line personnel and their safety and quality counterparts, as well as the representatives of the regulatory authority, is indicative of a positive organizational culture. This relationship should be characterized by professional courtesy, while maintaining respective roles as necessary to ensure objectivity or accountability.

2.6.9 An effective way to promote safe operations is to ensure that an organization has developed an environment where all staff feel responsible for safety. This becomes evident when staff consider the impact on safety in everything they do, report all hazards, errors and threats and support the identification and management of all their associated risks. In addition, management must create an environment in which personnel are aware of safety risks, are given sufficient systems to protect themselves and are assured protection when they divulge safety information through the safety reporting system. An effective safety culture serves as a method to synchronize diverse national and professional cultures within the context of the organization.

2.6.10 *Professional culture* differentiates the characteristics of particular professional groups (i.e. the characteristic behaviour of pilots vis-à-vis that of air traffic controllers, civil aviation authority personnel or maintenance engineers). Through personnel selection, education, training, on-the-job experience and peer pressure, etc., professionals tend to adopt the value system and develop behaviour patterns consistent with their peers or predecessors. An effective professional culture reflects the ability of professional groups to differentiate between safety performance issues and contractual or industrial issues. A healthy professional culture may be characterized as the ability for all professional groups within the organization to collaboratively address safety performance issues.

2.6.11 *National culture* differentiates the characteristics of particular nations, including the role of the individual within society, the manner in which authority is distributed, and national priorities with respect to resources, accountabilities, morality, objectives and different legal systems. From a safety management perspective, national culture plays a large part in determining the nature and scope of regulatory enforcement policies, including the relationship between regulatory authority personnel and industry personnel, and the extent to which safety-related information is protected.

2.6.12 National culture forms an intrinsic component of personal beliefs that inherently shapes the safety perspectives of individuals prior to their membership within an organization. Organizational culture may therefore be significantly affected by the national cultures present among the members of its workforce.

2.6.13 When applying a safety management programme, managers should closely assess and consider the differences in the national cultures of their personnel. For instance, safety risk perceptions can differ greatly between different national cultures. Safety-related aspects, including communication and leadership styles as well as the interaction between supervisors and subordinates, may need to accommodate a multicultural workforce.

2.6.14 *Reporting culture* emerges from personnel beliefs about and attitudes toward the benefits and potential detriments associated with reporting systems and the ultimate effect on their acceptance or utilization of such systems. It is greatly influenced by organizational, professional and national cultures and is one criterion for judging the effectiveness of a safety system. A healthy reporting culture aims to differentiate between intentional and unintentional deviations and determine the best course of action for both the organization as a whole and the individuals directly involved.

2.6.15 The success of a reporting system depends upon the continuous flow of information from front-line personnel. Policies that distinguish wilful acts of misconduct from inadvertent errors, providing for an appropriate punitive or non-punitive response, are essential to assure the effective reporting of systemic safety deficiencies. Not only is an "absolute no blame" culture unreasonable, it is not even feasible. While management gains safety information, the system will be ineffective if it interferes with appropriate punitive actions. Conversely, a culture that fails to distinguish unintentional errors/mistakes from acts of wilful misconduct will inhibit the reporting process. If personnel avoid reporting for fear of punishment, management does not gain important safety information.

2.6.16 Overall, personnel must believe that they will be supported in any decisions made in the interest of safety but must also understand that intentional breaches of safety policy will not be tolerated. Therefore, a voluntary reporting system should be confidential and operated in accordance with appropriate non-punitive policies. The system should also provide feedback to personnel on safety improvements achieved as a result of the reports received. This objective requires secure and easy access to safety reporting systems, active safety data collection and management's proactive treatment of the data.

2.6.17 Safety information should be collected solely for the improvement of aviation safety, and information protection is essential in ensuring the continued availability of information. This may be realized through a safety reporting system that is confidential, voluntary and non-punitive. The benefits are twofold. Often personnel are the closest to safety hazards, so the reporting system enables them to actively identify these hazards. At the same time, management is able to gather pertinent safety hazard information and also build trust with personnel.

2.6.18 Once the data have been collected and stored, that information must be processed in order to substantiate the implementation of appropriate actions that should be communicated to front-line personnel in a timely manner.

Promotion and assessment of a safety culture

2.6.19 The effectiveness of a safety culture can indeed be measured and monitored through the use of tangible metrics. In a mature safety culture environment, it can be anticipated that organizations may be in a position to introduce

a mechanism to conduct an internal organization safety culture (OSC) assessment. Such an assessment may be further enhanced using the more technically involved and sector-specific organization risk profile (ORP) assessment. Concurrently, industry organizations and/or regulators may consider developing promotional schemes (e.g. a safety culture award) to encourage product and service providers to participate in a voluntary OSC/ORP assessment of their organizations. The parameters to be assessed in an OSC/ORP assessment should include organizational factors and outcomes that are beyond conventional regulatory requirements, but which are nevertheless pertinent to an organization's safety culture, and therefore have an impact on its safety performance. This is the main purpose of an OSC/ORP assessment. It serves to supplement traditional regulatory oversight by addressing organizational factors (latent conditions) that are otherwise beyond regulatory purview. An OSC assessment checklist would tend to be more generic in content while an ORP checklist would be more customized to the nature of the organization's operations. An illustration of a possible sector-specific OSC/ORP assessment checklist is provided in Appendix 1.

2.7 THE MANAGEMENT DILEMMA

2.7.1 Safety management processes identify hazards with the potential to adversely affect safety. These processes also provide effective and objective mechanisms to assess the risk presented by hazards and implement ways to eliminate these hazards or mitigate the risks associated with them. The result of these processes is to facilitate achievement of an acceptable level of safety while balancing the allocation of resources between production and protection. From a resource allocation perspective, the concept of a safety space is especially useful in describing how this balance is achieved.

Safety space

2.7.2 In any organization engaged in the delivery of services, production and safety risks are linked. As production increases, the safety risks may also increase if the necessary resources or process enhancements are not available. An organization must define its production and safety objectives by balancing output with acceptable safety risks. Also, when defining its production objectives, the organization needs to define defences in order to keep safety risks under control. For a product or service provider, the basic safety defences are technology, training and internal processes and procedures. For the State, the basic defences are similar, i.e. training of personnel, the appropriate use of technology, effective oversight and the internal processes and procedures supporting oversight. The safety space is the zone where an organization balances desired production while maintaining required safety protection through safety risk controls. For example, a manufacturer or air navigation service provider may wish to support anticipated growth through investment in new technologies. These technologies may simultaneously provide the necessary efficiency improvements as well as improved reliability and safety performance. Such decision making should involve an assessment of both the value added to the organization's product or service objectives as well as the safety risks involved. The allocation of excessive resources to protection or risk controls may result in the product or service becoming unprofitable, thus jeopardizing the viability of the organization.

2.7.3 On the other hand, excess allocation of resources for production at the expense of protection can have an impact on the safety performance of the product or service and can ultimately lead to an accident. It is therefore essential that a safety boundary be defined that provides early warning that an unbalanced allocation of resources exists or is developing. Therefore, the safety space boundaries should be defined by the management of the organization and reviewed continually to ensure that they accurately reflect the current situation. Refer to Figure 2-6 for an illustration of the boundaries of an organization's safety space.

2.7.4 The need to balance production and protection has become a readily understood and accepted requirement from a product and service provider perspective. This balance is equally applicable to the State's management of its SSP, given the requirement to balance resources required for State protective functions that include certification and surveillance.

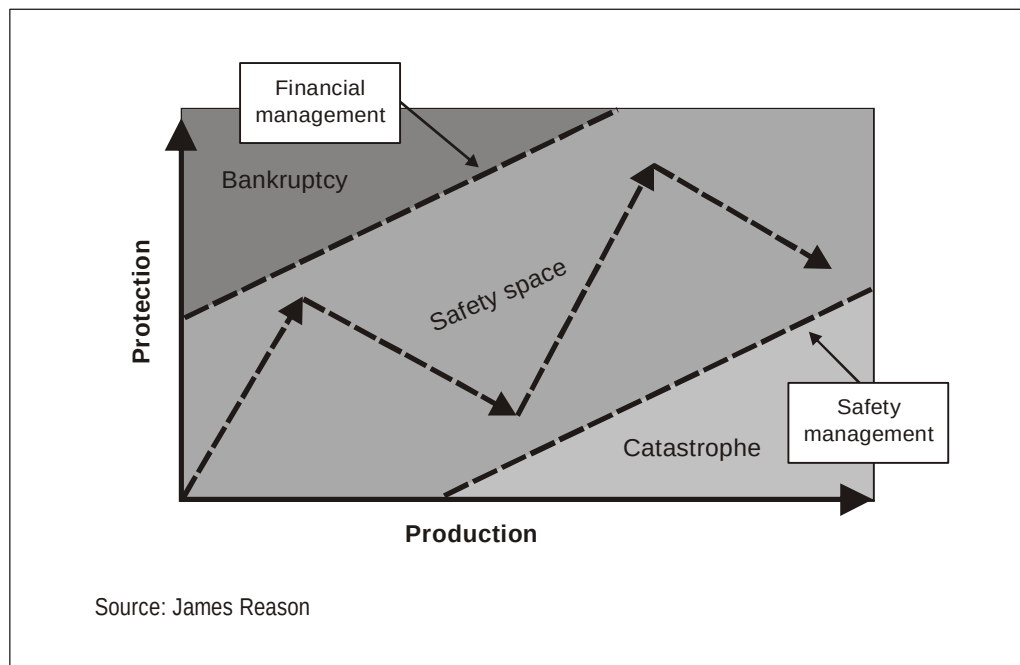


Figure 2-6. The safety space

2.8 CHANGE MANAGEMENT

2.8.1 Aviation organizations, including regulatory authorities, experience change due to expansion and contraction as well as changes to existing systems, equipment, policies, programmes, services and regulations. Hazards may inadvertently be introduced into the aviation system whenever change occurs. Existing baseline safety risk mitigation processes may also be impacted. Safety management practices require that hazards resulting from change be systematically identified, and strategies to manage the consequential safety risks be developed, implemented and subsequently evaluated. Sound management of safety risks associated with change is a critical requirement of the SSP and SMS.

2.8.2 The management of safety risks resulting from change should take into account the following three considerations:

- a) *Criticality of systems and activities.* Criticality relates to the potential consequences of safety risk, whether a consideration during the system design process or during a situation related to systemic change. Changes to equipment and activities associated with relatively high safety risks should be reviewed to make sure that necessary corrective actions can be taken to control potentially emerging safety risks.
- b) *Stability of systems and operational environments.* Changes may be planned and under the direct control of the organization. Planned changes may be associated with organizational growth or contraction as well as the introduction of new equipment, products or services. Unplanned changes, including those that are operational, political or economic in nature, may also create risks that require

a mitigating response by the organization. Instances in which frequent systemic or environmental changes occur dictate that managers update key risk assessments and related information more frequently than in more stable situations.

- c) *Past performance.* Past performance of critical systems may be a reliable indicator of future performance. 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, data analyses, investigations or reports, it is essential that such information be considered to assure the effectiveness of corrective actions.

2.9 INTEGRATION OF MANAGEMENT SYSTEMS

2.9.1 Aviation organizations vary greatly in terms of overall size and complexity. Each organization has a layered management system that is composed of multiple subsystems given direction through some type of governance system. The organization should integrate organizational management systems designed to achieve specific organizational goals, i.e. provide products and services to customers. A holistic organizational management system has often been referred to as an integrated management system or simply the organizational “management system”.

2.9.2 Typical management systems within an aviation organization may include:

- a) a quality management system (QMS);
- b) a safety management system (SMS);
- c) a security management system (SeMS);
- d) an environmental management system (EMS);
- e) an occupational health and safety management system (OHSMS);
- f) a financial management system (FMS); and
- g) a documentation management system (DMS).

2.9.3 Each management system is monitored by an “accountable leader”. Complex product or service provider organizations may have thirty-plus management systems that must be integrated into the enterprise. Examples of these systems include:

- a) a supplier management system;
- b) a marketing management system;
- c) a personnel management system;
- d) a facilities management system;
- e) a ground equipment management system;
- f) a production management system;

- g) a training management system;
- h) a flight operations management system;
- i) a cargo operations management system;
- j) an aircraft maintenance management system;
- k) a dispatch management system; and
- l) a fatigue risk management system (FRMS).

2.9.4 There is a developing tendency in civil aviation to integrate all of these management systems as functional components of the overarching enterprise management system. There are a number of 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; and
- d) elimination of potentially conflicting responsibilities and relationships.

2.9.5 Each organization will integrate these systems based on its unique production requirements. Risk management processes are essential features of the SMS, QMS, EMS, FMS, OSHSMS and SeMS. If the SMS were to operate in isolation of these other management systems, there may be a tendency to focus solely on safety risks without understanding the nature of quality, security or environmental threats to the organization.

2.9.6 While system integration is presently beyond the scope of the harmonized ICAO safety management SARPs and this manual, many civil aviation authorities and product or service providers have realized the benefits of integrating and aligning multiple management systems. For details on SMS and QMS integration, please refer to Chapter 5.

2.10 SAFETY REPORTING AND INVESTIGATION

Effective safety reporting

2.10.1 Accurate and timely reporting of relevant information related to hazards, incidents or accidents is a fundamental activity of safety management. The data used to support safety analyses are reported by multiple sources. One of the best sources of data is direct reporting by front-line personnel since they observe hazards as part of their daily activities. A workplace in which personnel have been trained and are constantly encouraged to report their errors and experiences is a prerequisite for effective safety reporting.

2.10.2 There are five basic characteristics that are universally associated with effective safety reporting systems (see Figure 2-7). Effective hazard reporting is a key component of safety management. Once reported, data on hazards can be analysed with other data sources to support the SRM and SA processes.

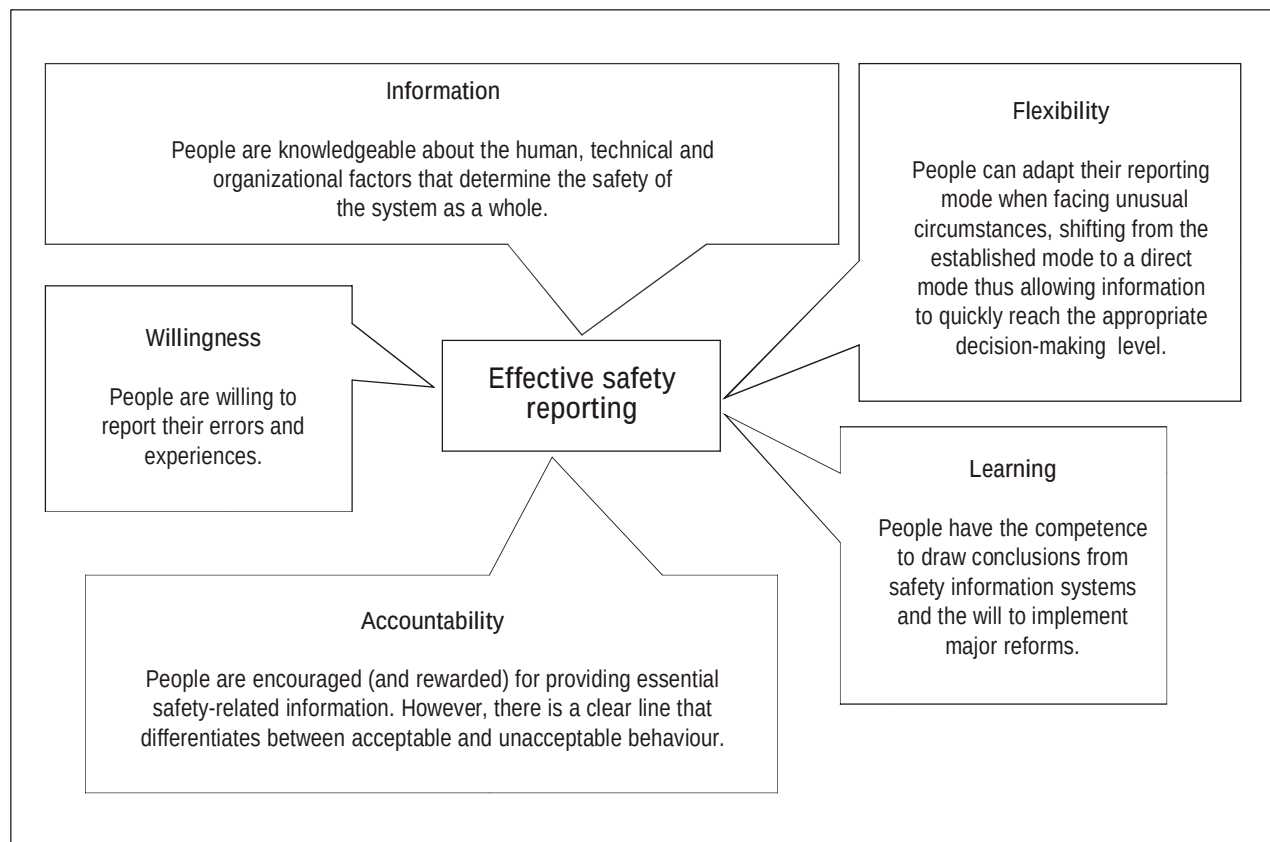


Figure 2-7. Effective safety reporting — five basic characteristics

2.10.3 Another source of data used to support SRM and SA processes is occurrence reporting. This may range from the highest-consequence occurrences (accidents, serious incidents) to lower-consequence events such as operational incidents, system/equipment failures or defects. While regulatory requirements for mandatory reporting of high-consequence occurrences (accidents, serious incidents) are common, a mature safety management environment will provide for the reporting of lower-consequence events as well. This will allow for the necessary monitoring mechanisms to address all potential high-consequence outcomes. The trend (rate of occurrence) of lower-consequence events is inevitably a precursor of higher-consequence outcomes to come.

2.10.4 Further guidance on State voluntary and mandatory incident reporting systems is provided in Appendices 2 and 3, respectively, to Chapter 4. Guidance on SMS voluntary reporting systems is provided in Appendix 5 to Chapter 5.

Investigation of accidents and incidents

2.10.5 When an accident or serious incident occurs, the accident investigation process is set in motion to find out any possible failure within the aviation system, the reasons therefor and to generate the necessary countermeasures to prevent recurrence. Thus, in a safety management environment, the accident investigation process has a distinct role, being an essential process that deploys when safety defences, barriers, checks and counterbalances in the system have failed.

2.10.6 Being an important reactive component of the elements contained in the SMS and SSP frameworks, accident investigations contribute to the continuous improvement of the aviation system by providing the root causes of accidents/incidents and lessons learned from analysis of events. This can support decisions regarding the development of corrective actions and corresponding allocation of resources and may identify necessary improvements to the aviation system including SMS, SSP as well as the State accident investigation process. While it is common for mandatory State-level investigations to be limited to accidents and serious incidents, a mature safety management environment may provide for the investigation of lower-consequence events as well.

2.10.7 Apart from establishing findings and the root causes of accidents/incidents, most investigation exercises also uncover hazards/threats. An effective and comprehensive investigation process includes the identification of and discrimination between an ultimate consequence, an unsafe event and hazards/threats that contribute to the accident/incident. This may include any systemic, latent or organizational factors within the entire aviation system framework. In today's proactive safety management environment, there is an important and necessary integration between an accident/incident investigation process and an organization's hazard reporting/identification process. Investigation reporting forms should have a clear provision that hazards/threats uncovered during the investigation process, which would require separate follow-up action by the organization's hazard identification and risk mitigation process, must be documented. It is common for some investigation reports to limit their "conclusion" and "action taken/recommended" to immediate or direct causes only. Thus, any secondary or indirect hazards/threats tend to be overlooked, unless this gap can be bridged by linking the accident/incident investigation and hazard identification processes.

2.11 SAFETY DATA COLLECTION AND ANALYSIS

Safety data collection and quality

2.11.1 Data-based decision making is one of the most important facets of any management system. The type of safety data to be collected may include accidents and incidents, events, non-conformance or deviations and hazard reports. The quality of the data that are used to enable effective decision making must be considered throughout SSP and SMS development and implementation. Unfortunately, many databases lack the data quality necessary to provide a reliable basis for evaluating safety priorities and the effectiveness of risk mitigation measures. Failure to account for the limitations of data used in support of safety risk management and safety assurance functions will result in flawed analysis results that may lead to faulty decisions and discredit the safety management process.

2.11.2 Given the importance of data quality, organizations must assess the data used to support safety risk management and safety assurance processes using the following criteria:

- a) *Validity.* Data collected are acceptable as per established criteria for their intended use.
- b) *Completeness.* No relevant data are missing.
- c) *Consistency.* The extent to which measurement of a given parameter is consistent can be reproduced and avoids error.
- d) *Accessibility.* Data are readily available for analysis.
- e) *Timeliness.* Data are relevant to the time period of interest and available promptly.
- f) *Security.* Data are protected from inadvertent or malicious alteration.
- g) *Accuracy.* Data are error-free.

By considering these seven criteria for data quality, safety data analyses will generate the most accurate information possible to be used in support of strategic decision making.

Safety database

2.11.3 In the context of safety data collection and analysis, the term “safety database” may include the following type of data or information which can be used to support safety data analysis:

- a) accident investigation data;
- b) mandatory incident investigation data;
- c) voluntary reporting data;
- d) continuing airworthiness reporting data;
- e) operational performance monitoring data;
- f) safety risk assessment data;
- g) data from audit findings/reports;
- h) data from safety studies/reviews; and
- i) safety data from other States, regional safety oversight organizations (RSOOs) or regional accident and incident investigation organizations (RAIOs), etc.

2.11.4 A safety database may refer to the State’s SSP-related database(s) or to a service provider’s internal SMS-related database(s), depending on the context. Voluntary reports may come from operational personnel (service providers, pilots, etc.), but also from passengers or the general public.

2.11.5 Much of the data in safety databases are in the form of reports related to complex events such as accidents and incidents. The reports in these types of databases typically answer a series of questions. Who was involved in the event? What happened that caused a report to be written? When did the event occur? Where did the event take place? Why did it happen? Other types of databases are related to relatively narrow topics such as flight information, weather and traffic volumes. These reports contain simple facts.

2.11.6 The safety databases are typically housed in various parts of an organization. Many organizations provide access to the databases through an interface that allows safety analysts to efficiently specify and extract reports of interest. Reports can be viewed individually or collectively through aggregation. Analytical tools allow safety analysts to view extracted data in multiple formats. Examples include spreadsheets, maps and various types of graphs.

2.11.7 To ensure that a database is understood and used appropriately, information related to the database (metadata) must be well documented and made available to users. Types of metadata include field definitions, changes made to the database over time, usage rules, the data collection form and references to valid values.

2.11.8 A large number of safety databases have been developed independently by many different organizations with very specific areas of responsibility and analysis needs. In order to provide aviation safety analysts with expanded views of safety issues, it is necessary to build safety information integration facilities that can extract information from multiple sources, apply common data standards, consolidate metadata and load the information onto a common platform housed in centralized data storage architecture.

2.11.9 Once the safety data have been processed, they are made accessible to safety analysts through a common interface and common set of analytical tools. If an analyst requires data from multiple databases, the application of common data standards makes it possible for database technicians to extract data from the required databases and construct an entirely new database. A schematic view of a State's safety data system is shown in Figure 2-8, indicating the inputs, processes and outputs related to safety data collection, analysis and exchange.

Inputs (Collection)	• accident and incidents reports; • voluntary incident reporting systems; • mandatory incident reporting systems; • operational data collection systems (provided directly from service providers); • safety oversight data collection systems.
Processes (Analysis)	• data collection tools and data management systems to capture and store data from: — accident and incident reporting systems; — operational data collection systems; — safety oversight data collection systems; — recommendations from investigations of accidents and serious incidents; • analysis methods to assess known and emerging risks from all available data sources; • safety indicators, target and alert levels (individual or aggregate level) to measure safety performance and detect undesirable trends; • development of risk-based safety surveillance processes, including the prioritization of inspections and audits.
Outputs (Exchange)	• safety recommendations issued by the relevant State authorities based on analysis of all safety data system inputs; • reports on safety indicators, targets and alerts (service provider and State level) generated through analysis of data inputs including: — comparative “benchmark” analyses; — historical trend analyses; — correlations between proactive indicators and safety outcomes (accidents and serious incidents); • reviews of State regulations and oversight processes including the prioritization of oversight activities according to areas of greatest risk; • administrative actions required for safety purposes; • the exchange of information regarding safety issues among State regulatory authorities and accident investigation authorities; • the exchange of information regarding safety issues among service providers, regulatory authorities as well as accident and incident investigation organizations, at the national, regional and international levels.

Figure 2-8. Schematic view of a State's safety data system

Safety data analysis

2.11.10 After collecting safety data through various sources, organizations should then perform the necessary analysis to identify hazards and control their potential consequences. Among other purposes, the analysis may be used to:

- a) assist in deciding what additional facts are needed;
- b) ascertain latent factors underlying safety deficiencies;
- c) assist in reaching valid conclusions; and
- d) monitor and measure safety trends or performance.

2.11.11 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 analysis methods.

2.11.12 Human judgement may be subject to some level of bias based on past experiences, which may influence the interpretation of analysis results or testing of 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

2.11.13 The following safety analysis methods may be used:

- a) *Statistical analysis.* This method can be used to assess the significance of perceived safety trends often depicted in graphical presentations of analysis results. While statistical analysis may yield powerful information regarding the significance of certain trends, data quality and analytical methods must be carefully considered to avoid reaching erroneous conclusions.
- b) *Trend analysis.* By monitoring trends in safety data, predictions may be made about future events. Trends may be indicative of emerging hazards.
- c) *Normative comparisons.* Sufficient data may not be available to provide a factual basis against which to compare the circumstances of potential events. In such cases, it may be necessary to sample real-world experience under similar operating conditions.
- d) *Simulation and testing.* In some cases, hazards may become evident through simulation as well as laboratory testing to validate the safety implications of existing or new types of operations, equipment or procedures.
- e) *Expert panel.* The views of peers and specialists can be useful in evaluating the diverse nature of hazards related to a particular unsafe condition. A multidisciplinary team formed to evaluate evidence of an unsafe condition can assist in identifying the best course of corrective action.
- f) *Cost-benefit analysis.* The acceptance of recommended safety risk control measures may be dependent on credible cost-benefit analysis. The cost of implementing the proposed measures are weighed against the expected benefits over time. Cost-benefit analysis may suggest that accepting the consequences of the safety risk is tolerable considering the time, effort and cost necessary to implement corrective action.

Management of safety information

2.11.14 Effective safety management is “data driven”. Sound management of the organization's databases is fundamental to ensuring effective and reliable safety analysis of consolidated sources of data.

2.11.15 The establishment and maintenance of a safety database provide an essential tool for personnel monitoring system safety issues. A wide range of relatively inexpensive electronic databases, capable of supporting the organization's data management requirements, are commercially available.

2.11.16 Depending on the size and complexity of the organization, system requirements may include a range of capabilities to effectively manage safety data. In general, the system should:

- a) include a user-friendly interface for data entry and query;
- b) have the capability to transform large amounts of safety data into useful information that supports decision making;
- c) reduce the workload for managers and safety personnel; and
- d) operate at a relatively low cost.

2.11.17 To take advantage of the potential benefits of safety databases, a basic understanding of their operation is required. While any information that has been grouped together in an organized manner can be considered to be a database, analysis of paper records maintained in a simple filing system will suffice only for small operations. Storage, recording, recall and retrieval using paper-based systems are cumbersome tasks. Safety data should preferably be stored in an electronic database that facilitates the query of records and generation of analysis output in a variety of formats.

2.11.18 The functional properties and attributes of different database management systems vary, and each should be considered before deciding on the most suitable system. 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 safety data with other organizations;
- g) monitor event investigations; and
- h) monitor the implementation of corrective actions.

Protection of safety data

2.11.19 Given the potential for misuse of safety data that have been compiled strictly for the purpose of advancing aviation safety, database management must include the protection of that 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” regulations vis-à-vis safety management requirements;
- b) organizational policies and procedures on the protection of safety data that limit access to those with a “need to know”;
- 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) prohibitions on unauthorized use of data.

Further information on safety data protection can be found in Appendix 5 to Chapter 4.

2.12 SAFETY INDICATORS AND PERFORMANCE MONITORING

2.12.1 The output from an organization's safety data collection and analysis system is normally depicted in the form of charts or graphs. Such charts and graphs, normally utilized in conventional quality/reliability management systems, typically show a “snapshot” of the data analysis resulting from a one-time query.

2.12.2 Figure 2-9 is a basic (screen shot) data analysis chart and shows the absolute number of mandatory occurrence report (MOR) incidents of an operator by fleet type for the year 2009. This basic chart does not reflect the number of aircraft for each fleet nor does it account for the number of flights by each fleet. Thus, there is limited usefulness to be derived from this type of chart. It would not be adequate for the purpose of a continuing safety performance indicator.

2.12.3 Analysis used to continuously monitor safety should be in the form of a periodic data extraction to generate a trend chart or graph, updated on a monthly or quarterly basis, as shown in Figure 2-10. This data chart provides information on the monthly reportable incident rate, taking into consideration the number of accumulated flying hours (FH) for the operator's fleet. A periodic (monthly) upload of the incident rate data will then allow the chart to serve as a continuous trend monitoring indicator. Once such a continuous trend monitoring indicator chart is in place, the next step is to transform it into a safety performance measurement indicator by setting target and alert levels within the chart. This step should preferably be done when historical data points have already been generated on the chart. These historical data points (historical performance) will be the basis for setting or defining unacceptable alert trend levels as well as any desired targeted improvement level to be achieved within a specified period. Further details on development of safety performance indicators and their associated target and alert settings are addressed in Chapter 4 (SSP) and Chapter 5 (SMS).

2.13 HAZARDS

2.13.1 Hazard identification is a prerequisite to the safety risk management process. Any incorrect differentiation between hazards and safety risks can be a source of confusion. A clear understanding of hazards and their related consequences is essential to the implementation of sound safety risk management.

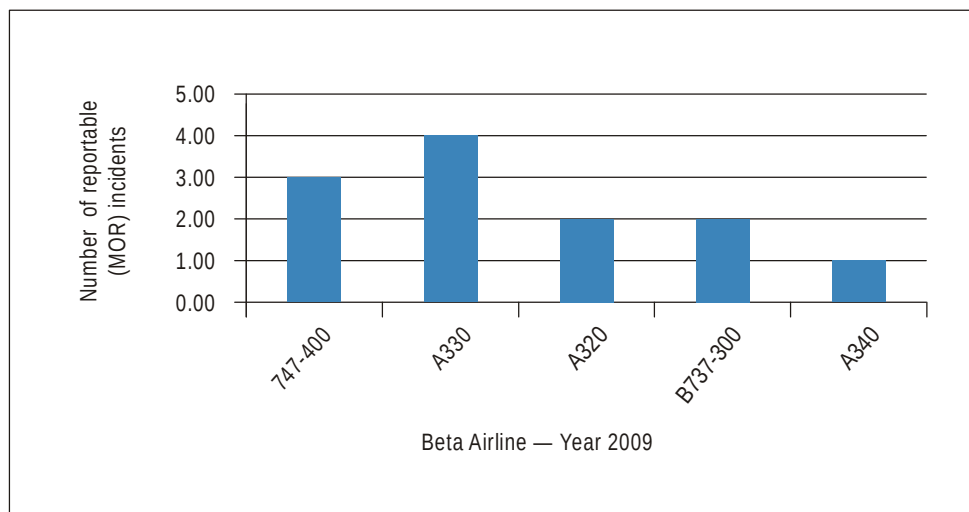


Figure 2-9. A basic (screen shot) data analysis chart

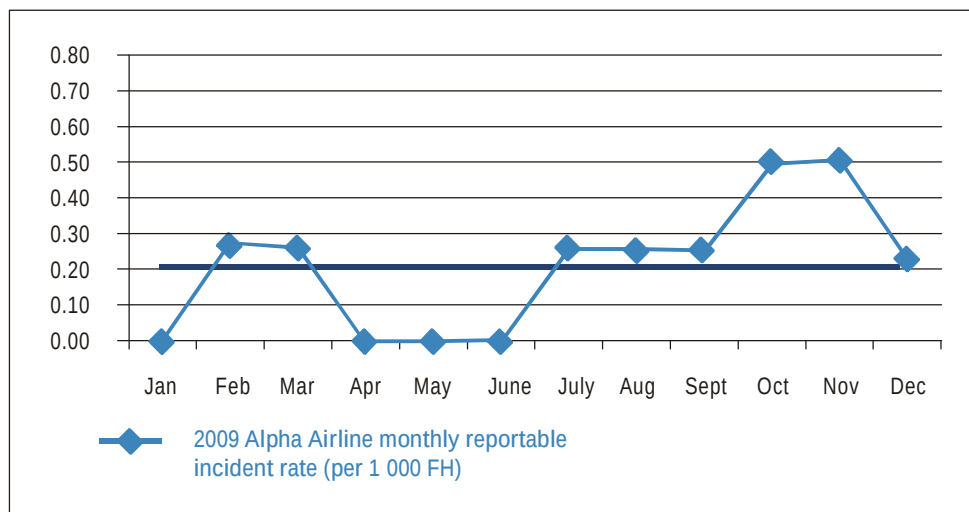


Figure 2-10. A continuous monitoring safety indicator chart

Understanding hazards and consequences

2.13.2 A hazard is generically defined by safety practitioners as a condition or an object with the potential to cause death, injuries to personnel, damage to equipment or structures, loss of material, or reduction of the ability to perform a prescribed function. For the purpose of aviation safety risk management, the term hazard should be focused on those conditions which could cause or contribute to unsafe operation of aircraft or aviation safety-related equipment, products and services. (Guidance on distinguishing hazards that are directly pertinent to aviation safety from other general/industrial hazards is addressed in 2.13.12 and 2.13.13).

2.13.3 Consider, for example, a fifteen-knot wind, which is not necessarily a hazardous condition. In fact, a fifteen-knot wind blowing directly down the runway improves aircraft take-off and landing performance. However, a fifteen-knot wind blowing in a direction ninety degrees across a runway of intended take-off or landing creates a crosswind condition that may be hazardous due to its potential to contribute to an aircraft operational occurrence, such as a lateral runway excursion.

2.13.4 Hazards are an inevitable part of aviation activities. However, their manifestation and possible consequences can be addressed through various mitigation strategies to contain the potential for a hazard to result in unsafe aircraft or aviation equipment operations.

2.13.5 There is a common tendency to confuse hazards with their consequences or outcomes. A consequence is an outcome that can be triggered by a hazard. For example, a runway excursion (overrun) is a projected consequence in relation to the hazard of a contaminated runway. By first defining the hazard clearly, one can then project the proper consequence or outcome. It may be noted that consequences can be multi-layered, including such things as an intermediate unsafe event before an ultimate consequence (accident). Refer to Appendix 2, Table 2-A2-3, for further information.

2.13.6 In the crosswind example above, an immediate outcome of the hazard could be loss of lateral control followed by a consequent runway excursion. The ultimate consequence could be an accident. The damaging potential of a hazard materializes through one or many consequences. It is therefore important for safety assessments to include a comprehensive account of all likely consequences, described accurately and in practical terms. The most extreme consequence, loss of human life, should be differentiated from those that involve the potential for lesser consequences such as increased flight crew workload, passenger discomfort or reduction in safety margins. The description of consequences according to their plausible outcomes will facilitate the development and implementation of effective mitigation strategies through proper prioritization and allocation of limited resources. Proper hazard identification leads to appropriate evaluation of their potential outcomes.

2.13.7 Hazards should be differentiated from error, a normal and unavoidable component of human performance, which must be managed.

Hazard identification and prioritization

2.13.8 Hazards exist at all levels in the organization and are detectable through use of reporting systems, inspections or audits. Mishaps may occur when hazards interact with certain triggering factors. As a result, hazards should be identified before they lead to accidents, incidents or other safety-related occurrences. An important mechanism for proactive hazard identification is a voluntary hazard/incident reporting system. Additional guidance on voluntary reporting systems can be found in Chapter 4, Appendix 2, and Chapter 5, Appendix 5. Information collected through such reporting systems may be supplemented by observations or findings recorded during routine site inspections or organization audits.

2.13.9 Hazards can also be identified from the review or study of investigation reports, especially those hazards which are deemed to be indirect contributing factors and which may not have been adequately addressed by corrective actions resulting from the investigation process. Thus, a systematic procedure to review accident/incident investigation reports for outstanding hazards is a good mechanism to enhance an organization's hazard identification system. This is particularly relevant where an organization's safety culture is not sufficiently mature to support an effective voluntary hazard reporting system.

2.13.10 Hazards may be categorized according to their source or location. Objective prioritization of hazards may require categorizations according to the severity/likelihood of their projected consequences. This will facilitate the prioritization of risk mitigation strategies so as to use limited resources in the most effective manner. Refer to Appendix 3 to this chapter for an example of a hazard prioritization procedure.

Hazard identification methodologies

2.13.11 The three methodologies for identifying hazards are:

- a) *Reactive*. This methodology involves analysis of past outcomes or events. Hazards are identified through investigation of safety occurrences. Incidents and accidents are clear indicators of system deficiencies and therefore can be used to determine the hazards that either contributed to the event or are latent.
- b) *Proactive*. This methodology involves analysis of existing or real-time situations, which is the primary job of the safety assurance function with its audits, evaluations, employee reporting, and associated analysis and assessment processes. This involves actively seeking hazards in the existing processes.
- c) *Predictive*. This methodology involves data gathering in order to identify possible negative future outcomes or events, analysing system processes and the environment to identify potential future hazards and initiating mitigating actions.

Distinguishing between aviation hazards and occupational safety, health and environment (OSHE) hazards

2.13.12 Understanding whether a hazard is pertinent to aviation safety or OSHE depends on its potential or foreseeable consequence or risk. Any hazard that can have an impact (whether directly or indirectly) on the operational safety of aircraft or aviation safety-related equipment, products and services should be deemed pertinent to an aviation SMS. A hazard having purely OSHE consequences (i.e. without any impact on aviation safety) should be addressed separately by the organization's OSHE system/procedures in accordance with its relevant national or organizational OSHE requirements as appropriate. OSHE hazards and consequences with no impact on aviation safety are not pertinent to an aviation SMS.

2.13.13 Safety risks associated with compound hazards that simultaneously impact aviation safety as well as OSHE may be managed through separate (parallel) risk mitigation processes to address the separate aviation and OSHE consequences respectively. Alternatively, an integrated aviation and OSHE risk mitigation system may be used to address such compound hazards. An example of a compound hazard is a lightning strike on an aircraft at an airport transit gate. This hazard may be deemed by an OSHE inspector to be a "workplace hazard" (ground personnel/ workplace safety). To an aviation safety inspector it is also an aviation hazard with risk of damage to the aircraft and a risk to passenger safety. Since OSHE and aviation safety consequences of such compound hazards are not the same, due consideration should be taken to manage them separately. The purpose and focus of preventive controls for OSHE and aviation safety consequences would be different.

2.14 SAFETY RISK

2.14.1 Safety risk management is another key component of a safety management system. The term safety risk management is meant to differentiate this function from the management of financial risk, legal risk, economic risk and so forth. This section presents the fundamentals of safety risk and includes the following topics:

- a) a definition of safety risk;
- b) safety risk probability;

- c) safety risk severity;
- d) safety risk tolerability; and
- e) safety risk management.

Definition of safety risk

2.14.2 Safety risk is the projected likelihood and severity of the consequence or outcome from an existing hazard or situation. While the outcome may be an accident, an “intermediate unsafe event/consequence” may be identified as “the most credible outcome”. Provision for identification of such layered consequences is usually associated with more sophisticated risk mitigation software. The safety risk mitigation worksheet illustrated in Appendix 2 to this chapter also has this provision.

Safety risk probability

2.14.3 The process of controlling safety risks starts by assessing the probability that the consequences of hazards will materialize during aviation activities performed by the organization. Safety risk probability is defined as the likelihood or frequency that a safety consequence or outcome might occur. The determination of likelihood can be aided by questions such as:

- a) Is there a history of occurrences similar 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, managerial or regulatory implications that might reflect larger threats to public safety?

2.14.4 Any factors underlying these questions will help in assessing the likelihood that a hazard may exist, taking into consideration all potentially valid scenarios. The determination of likelihood can then be used to assist in determining safety risk probability.

2.14.5 Figure 2-11 presents a typical safety risk probability table, in this case, a five-point table. The table includes five categories to denote the probability related to an unsafe event or condition, the description of each category, and an assignment of a value to each category.

2.14.6 It must be stressed that this is an example only and that the level of detail and complexity of tables and matrices should be adapted to be commensurate with the particular needs and complexities of different organizations. Also, it should be noted that organizations may include both qualitative and quantitative criteria that may include up to fifteen values.

<i>Likelihood</i>	<i>Meaning</i>	<i>Value</i>
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 2-11. Safety risk probability table

Safety risk severity

2.14.7 Once the probability assessment has been completed, the next step is to assess the safety risk severity, taking into account the potential consequences related to the hazard. Safety risk severity is defined as the extent of harm that might reasonably occur as a consequence or outcome of the identified hazard. The severity assessment can be based upon:

- a) *Fatalities/injury*. How many lives may be lost (employees, passengers, bystanders and the general public)?
- b) *Damage*. What is the likely extent of aircraft, property or equipment damage?

2.14.8 The severity assessment should consider all possible consequences related to an unsafe condition or object, taking into account the worst foreseeable situation. Figure 2-12 presents a typical safety risk severity table. It includes five categories to denote the level of severity, the description of each category, and the assignment of a value to each category. As with the safety risk probability table, this table is an example only.

Safety risk tolerability

2.14.9 The safety risk probability and severity assessment process can be used to derive a safety risk index. The index created through the methodology described above consists of an alphanumeric designator, indicating the combined results of the probability and severity assessments. The respective severity/probability combinations are presented in the safety risk assessment matrix in Figure 2-13.

2.14.10 The third step in the process is to determine safety risk tolerability. First, it is necessary to obtain the indices in the safety risk assessment matrix. For example, consider a situation where a safety risk probability has been assessed as occasional (4), and safety risk severity has been assessed as hazardous (B). The composite of probability and severity (4B) is the safety risk index of the consequence.

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

Figure 2-12. Safety risk severity table

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 2-13. Safety risk assessment matrix

2.14.11 The index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix (see Figure 2-14) that describes the tolerability criteria for the particular organization. Using the example above, the criterion for safety risk assessed as 4B falls in the “unacceptable under the existing circumstances” category. In this case, the safety risk index of the consequence is unacceptable. The organization must therefore:

- a) take measures to reduce the organization's exposure to the particular risk, i.e. reduce the likelihood component of the risk index;
- b) take measures to reduce the severity of consequences related to the hazard, i.e. reduce the severity component of the risk index; or
- c) cancel the operation if mitigation is not possible.

Note.— The inverted pyramid in Figure 2-14 reflects a constant effort to drive the risk index towards the bottom APEX of the pyramid. Figure 2-15 provides an example of an alternate safety risk tolerability matrix.

2.15 SAFETY RISK MANAGEMENT

2.15.1 Safety risk management encompasses the assessment and mitigation of safety risks. The objective of safety risk management is to assess the risks associated with identified hazards and develop and implement effective and appropriate mitigations. Safety risk management is therefore a key component of the safety management process at both the State and product/service provider level.

2.15.2 Safety risks are conceptually assessed as acceptable, tolerable or intolerable. 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 safety, that immediate mitigation action is required.

2.15.3 Safety risks assessed in the tolerable region are acceptable provided that appropriate mitigation strategies are implemented by the organization. A safety risk initially assessed as intolerable may be mitigated and subsequently moved into the tolerable region provided that such risks remain controlled by appropriate mitigation strategies. In both cases, a supplementary cost-benefit analysis may be performed if deemed appropriate. Refer to 2.15.7 for further details.

2.15.4 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.

Risk management documentation/worksheet

2.15.5 Each risk mitigation exercise will need to be documented as necessary. This may be done on a basic spreadsheet or table for risk mitigation involving non-complex operations, processes or systems. For hazard identification and risk mitigation involving complex processes, systems or operations, it may be necessary to utilize customized risk mitigation software to facilitate the documentation process. Completed risk mitigation documents should be approved by the appropriate level of management. For an example of a basic risk mitigation worksheet, refer to Appendix 2.

Tolerability description	Assessed 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, 1A	Acceptable based on risk mitigation. It may require management decision.
Acceptable region	3E, 2D, 2E, 1B, 1C, 1D, 1E	Acceptable

Figure 2-14. Safety risk tolerability matrix

Risk index range	Description	Recommended action
5A, 5B, 5C, 4A, 4B, 3A	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.
3E, 2D, 2E, 1B, 1C, 1D, 1E	Low risk	Acceptable as is. No further risk mitigation required.

Figure 2-15 An alternate safety risk tolerability matrix

Human factors and risk management

2.15.6 Given that mature SSPs and SMSs target both human and organizational factors, a specific analysis process is a component of any mature, effective risk management system. In the course of any hazard identification and risk mitigation exercise involving human elements, it is necessary to assure that existing or recommended defences have taken human factors (HF) into consideration. Where necessary, a supplementary HF analysis may be conducted to support that particular risk mitigation exercise/team. An HF analysis provides an understanding of the impact of human error on the

situation and ultimately contributes to the development of more comprehensive and effective mitigation/corrective actions. A human error model is the basis of the analysis process, and it defines the relationship between performance and errors and categorizes errors to permit the root hazards to be more readily identified and better understood. This understanding ensures the adequate completion of a root-cause analysis. Individual actions and decisions viewed out of context can appear to be virtually random events, escaping their due attention. Human behaviour is not necessarily random. It usually conforms to some pattern and can be analysed and properly understood. Ultimately, this important HF perspective results in a more comprehensive and in-depth mitigation process. An HF analysis ensures that during the organization's risk mitigation process, when identifying root, contributory or escalation factors, human factors and their associated circumstantial, supervisory and organizational impacts are duly taken into consideration.

Cost-benefit analysis (CBA)

2.15.7 Cost-benefit or cost-effectiveness analysis is normally an independent process from safety risk mitigation or assessment. It is commonly associated with a higher level management protocol, such as a regulatory impact assessment or business expansion project. However, there may be situations where a risk assessment may be at a sufficiently high level or have a significant financial impact. In such situations, a supplementary CBA or cost-effectiveness process to support the risk assessment may be warranted. This is to ensure that the cost-effectiveness analysis or justification of recommended mitigation actions or preventive controls has taken into consideration the associated financial implications.

2.16 PRESCRIPTIVE AND PERFORMANCE-BASED REQUIREMENTS

Understanding performance-based requirements

2.16.1 There is a growing belief within the aviation community that effective implementation of a State safety programme (SSP) and safety management system (SMS) requires that the existing prescriptive approach to safety be complemented with a performance-based approach. A performance-based approach, supported by the collection and analysis of relevant data, makes good business sense while simultaneously providing an equivalent level of safety.

2.16.2 One aim of an SMS is to introduce supplementary performance-based elements for more effective control of safety risks. In a conventional compliance-based regulatory environment, the approach to safety management is relatively rigid and prescriptive whereby safety regulations are used as administrative controls. A regulatory framework is supported by inspections and audits to assure regulatory compliance.

2.16.3 In a performance-based, enhanced safety environment, certain performance-based elements are introduced within a prescriptive framework. This will allow the "compliance" aspect of a regulation to have room for a more flexible, risk-based (and hence more dynamic) performance. As a result, some elements within the SMS and SSP frameworks may be managed on an increasingly performance-based rather than being purely prescriptive approach. These performance-based elements are under the safety assurance and safety risk management components of the respective frameworks.

2.16.4 The performance-based elements within an SMS/SSP framework include the process for safety performance monitoring and measurement at the individual product or service provider level as well as at the State level. This element allows the organization to select its own safety monitoring indicators and the setting of relevant alerts and targets that are pertinent to its own context, performance history and expectations. There are no fixed (mandatory) prescribed safety indicators or alert levels or prescribed values under this SMS/SSP expectation.

Prerequisites for performance-based requirements

2.16.5 The State and its product and service providers respectively should have an SSP and an SMS in place. An interface needs to be in place for regulatory organizations to agree with individual product and service providers on their SMS-related safety performance indicators and associated targets and alert settings. The regulator will also need to have a process for continuous monitoring of the individual product and service provider's safety performance. Additional new performance-based processes introduced and duly accepted/approved by the regulator should have appropriate performance indicators developed for monitoring such performance-based processes. Such process-specific indicators may be viewed as supplementary indicators to the higher level SMS safety performance indicators.

Baseline and equivalent level of safety

2.16.6 The safety performance outcome from the introduction of performance-based elements within or supplementary to an SMS framework should not be worse than that of an existing, purely prescriptive regulatory framework. To assess or monitor that such "equivalence" is indeed the case, there should be safety indicators to monitor the overall outcome of events (non-conformance occurrences) of the system/process concerned for which the performance-based element will be introduced. As an example, the overall flight planning and fuel management (FPFM) average incident rate after introduction of performance-based provisions should not be worse than the incident rate prior to the introduction of performance-based FPFM provisions. By such a comparison process, the pre-implementation "baseline" performance can be verified against post-implementation performance, to see if an "equivalent" level of performance has been maintained. If the post-implementation performance turns out to be better, then a "better" level of performance has in fact been manifested. Where there is a degradation of the system's performance, the service provider should work in conjunction with the regulator to verify the causal factors and take actions as appropriate, which may include modification of the performance-based requirement itself or, where necessary, restoration of basic prescriptive requirements. Details of how system performance can be measured through safety performance indicators are addressed in 2.16.7 as well as in Chapters 4 and 5 of this manual.

Performance-based monitoring and measurement

2.16.7 Monitoring and measurement of a performance-based process should be done through appropriate performance, quality or safety indicators that continuously track the performance of that process. Parameters for such performance tracking may be occurrence outcomes, deviations or any event types that reflect the safety, quality or risk level of the process. A data trending chart should be used to track such outcomes. Outcome occurrences should normally be tracked as occurrence rates rather than absolute numbers. In conjunction with such indicators, alert as well as desired improvement target levels should be set for each indicator, where applicable. These will serve as markers to define what is the abnormal/unacceptable occurrence rate as well as the desired target (improvement) rate for the indicator. The alert level setting will effectively serve as the demarcation line between the acceptable trending region and the unacceptable region for a safety indicator. So long as the occurrence rate for a process does not trend beyond or breach the set alert level criteria, the number of such occurrences is deemed to be acceptable (not abnormal) for that monitoring period. On the other hand, the aim of a targeted improvement level is to achieve the desired improvement level within a defined future milestone or monitoring period. With such defined alert and target settings, it becomes apparent that a qualitative/quantitative performance outcome can be derived at the end of any given monitoring period. This may be done by counting the number of alert breaches and/or the number of targets achieved for an individual indicator and/or a package of safety indicators. Examples of safety performance indicators and target/alert setting methodologies are further addressed in Chapters 4 and 5 respectively.

Oversight of performance-based requirements

2.16.8 Unlike auditing of prescriptive, stand-alone requirements, the assessment of a performance-based process would require the assessor to be aware of the context of that process/element within its overall regulatory framework as well as within the complexity of the audited organization. There may be no simple “go/no-go” or pass/fail criteria to apply. An example would be the acceptability of a hazard reporting system or the acceptability of proposed target/alert levels for a performance-based process, which may involve more interaction, monitoring, negotiation and objective judgement for the auditor. The level or degree of compliance or performance of such elements would also vary depending on the complexity of the process or operation audited. An example of element performance or compliance which is subject to organizational or process complexity is the risk mitigation process. A risk mitigation process may involve the use of a one-page worksheet for a workshop task of a simple one-man operation. On the other hand, risk mitigation of a complex, multi-disciplinary process (e.g. operations in airspace affected by volcanic eruptions) may require the use of risk mitigation software in order to perform a satisfactorily comprehensive safety assessment.
