NAMIBIA CIVIL AVIATION AUTHORITY

Technical Guidance Material – Volume 9

RISK MANAGEMENT MANUAL

Part 4

Document: TGM-09-4-RMM

Edition 1.0

Document Control

Edition Number	**1.0**	**Effective Date**	8 December 2023	
	Position	**Name**	**Signature**	**Date**
Prepared By	Senior Manager Safety Promotion and Quality	Mr Godfried G. Matroos		8/12/23
Recommended by:	General Manager Safety	Mr Ericsson M. Nengola		07/12/2023
NCAA Approval	Executive Director	Ms Toska Sem		8/12/2023

NAMIBIA CIVIL AVIATION AUTHORITY NCAA 2023 -12- 08

Change Summary

Edition Number	Brief Description of Change	Prepared by	Effective Date
1.0	First Edition	SPQ	8 Dec 2023

NOTE:

1. When amended, this document will be re-issued in full. Each page will indicate the edition number and the effective date. The edition number shall be the same on each page.
2. When printed this document is uncontrolled.

Contents

CHAPTER 1 INTRODUCTION

1.1 Purpose

1.1.1 The Risk Management Manual is designed to provide guidance for the for reviewing aviation safety assessments, hazard identification and risk mitigation processes, and the assessment and documentation of the management of change.

1.1.2 The document also provides a means for the to demonstrate that recognized risk assessment and risk management techniques have been used and the processes for safety management have been appropriately documented within their approved Safety Management Systems (SMS).

1.1.3 The reference throughout this manual of SMS shall be used, however the principles explained apply equally to the State Safety Programme Risk Management and Safety Assurance.

1.2 Context

1.2.1 Since November 2013, ICAO safety management Standards and Recommended Practices (SARPS) are contained in Annex 19, having been previously located in, several Annexes – Annex 1, 6, 8, 11, 13 and 14, which now cross reference to Annex 19.

1.2.2 Annex 19 describes the need to establish and implement a Safety Management System (SMS) across several aviation fields, namely, international commercial aviation operators, aviation training organisations (ATOs), aviation maintenance organisations (AMOs) offering services to aircraft involved in international general aviation, design manufacture organisations, international general aviation operators of large or turbojet aircraft, air navigation service providers, and aerodrome operators. Part 140 further requires that all air transport operators and AMOs have an SMS.

1.2.3 NAMCAR Part 11 specifies that the Executive Director, Namibia Civil Aviation Authority shall implement and maintain a State Safety Programme, the details of which are contained within TGM Volume 9 Part 1 SSP Manual.

1.2.4 This manual covers two of the key components of the required Safety Management System:

a. Safety Risk Management *(Component 2);* and
b. Safety Assurance *(Component 3).*

1.2.5 Safety Risk Management comprises two elements:

a. Hazard Identification *(Element 2.1);* and
b. Safety Risk Assessment and Mitigation *(Element 2.2).*

1.2.6 Safety Assurance comprises three elements:

a. Safety Performance Monitoring and Measurement (Element 3.1);
b. The Management of Change *(Element 3.2); and*
c. Continuous Improvement (Element 3.3)[1].

1.2.7 This document establishes a set of processes that will satisfy the part of the regulatory requirements for an SMS relating to risk management and management of change, including, but not limited to:

a. Risk Management
b. Hazard Identification
c. Change Evaluation (CE) and associated Change Evaluation Checklist (CEC);

d. Safety Statements (SS);
e. Safety Plans (SP);
f. Safety Assessments (SA); and
g. Safety Cases (SC).

1.2.8 This document is intended for safety and quality managers, safety and quality team members, safety specialists, operational managers, project managers, specialists in risk management, and those delegated with risk management responsibilities by their line manager.

Continuous improvement is dealt with in more detail in TGM Volume 10 – Quality Management System

CHAPTER 2 SAFETY RISK MANAGEMENT PROCEDURES

2.1 Purpose

2.1.1 This chapter describes a range of procedures that will enhance the level of safety risk management within an aviation organisation or authority and which safety division inspectors shall look for when conducting compliance and safety oversight activities. It contains a number of high-level principles and recommendations (*based on ICAO[1] and ISO[2] principles*) that shall be followed in managing safety risks across all parts of an organization.

2.1.2 To help ensure that people understand why they are being told to do various things, these procedures and principles are supported by examples and scenarios.

2.1.3 In a number of cases references to other (*NCAA and external*) documents are also provided to assist users with application of risk management. These supplementary documents introduce some of the many risk assessment techniques and change management tools that can be used to manage safety risks effectively and efficiently.

2.1.4 This chapter provides information on safety risk management based on the following core elements of good risk management practice:

a. effective communication and consultation with all stakeholders;
b. transparency in recording and reporting of safety risks;
c. the ability to anticipate changes in risk exposure through continual monitoring and periodic review; and
d. focus on meeting and exceeding regulatory and legal requirements and international best practices.

2.2 Objectives and Risk Management Principles

2.2.1 Civil Aviation Regulations - Safety Management System

2.2.1.1 NAM-CAR Part 140 deals explicitly with Safety Management Systems (SMS) and outlines the minimum requirements for all aviation sectors in Namibia. It requires that service providers establish safety management systems that will, as a minimum:

a. identify safety hazards;
b. ensure implementation of remedial action necessary to maintain agreed safety performance;
c. provide for continuous monitoring and assessment of the safety level achieved; and
d. aim at continuous improvement to overall performance of the SMS.

2.2.1.2 The technical standards supporting NAM-CAR Part 140 (NAM-CATS-SMS-140) specifically require the establishment of a formal safety risk management process that ensures analysis, assessment, and control of the safety risks of the consequences of hazards during the provision of service. It further requires that:

[1] International Civil Aviation Organization
[2] International Standards Organization

a. the safety risks of the consequences of each hazard identified through the hazard identification processes be analyzed in terms of probability (likelihood) and severity (consequence) of an occurrence, and assessed for their tolerability;
b. management levels with authority to make risk tolerability decisions are defined; and
c. safety controls for each safety risk assessed as tolerable are defined.

2.2.1.3 Safety Risk management is a fundamental part of the State Safety Programme as detailed in TGM-09-1 SSP Manual Section 2.

2.2.2 Safety Risk Management Principles

2.2.2.1 To support these requirements, the following 10 principles, adapted from ISO 31000[3], shall govern and inform the approach to safety risk management and form the basis against which all safety justifications are assessed.

1.	**Risk management creates and protects value** Risk management contributes to the demonstrable achievement of objectives and improvement of performance.
2.	**Risk management is an integral part of all organizational processes** Risk management is an integral part of the responsibilities of management - it is not a stand-alone activity that is separate from the main activities of the organization.
3.	**Risk management is part of decision making** Risk management helps decision makers make informed choices, prioritize actions, and distinguish among alternative courses of action.
4.	**Risk management is systematic, structured, and timely** The management of safety risk is a systematic process that identifies hazards, assesses risk, and decides what control measures are needed to ensure that those risks are reduced to a level that is As Low As Reasonably Practicable (ALARP).
5.	**Risk management is based on the best available information** The process of managing risk is based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts, and expert judgment.
6.	**Risk management takes human and cultural factors into account** Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of safety objectives.
7.	**Risk management is transparent and inclusive** Appropriate and timely involvement of stakeholders and decision makers at all levels of the organization ensures that risk management remains relevant.
8.	**Risk management is dynamic, iterative, and responsive to change**

[3] ISO 31000 – 2009 Risk Management – Principles and Guidelines

	Through monitoring and review, and awareness of changes in the operating environment, risk management continually senses and responds to change.
9.	**Safety risk assessment and management are common place processes** They shall ideally be carried out by the person accepting the safety risk. Where that person does not feel comfortable with the safety risk assessment, advice shall be sought from people with appropriate knowledge and experience.
10.	**Safety risk management shall be expressed concisely and in plain language** It shall provide, in simple terms, sufficient information for people within the industry to understand and manage the safety issues.

Table 1: ISO 31000 Risk Management Principles

2.2.3 Risk Limitation and ALARP

2.2.3.1 In some areas of aviation, specific safety limits, target levels of safety (TLS), or safety performance targets (SPTs) have been set, and changes to the system require that risks are managed within those target parameters. In most areas, however, the safety of aviation is not an absolute, and risks shall be managed so as to achieve an "…appropriate balance between production and protection[4]…".

2.2.3.2 One of the ways of achieving this is by applying the 'As Low As Reasonably Practicable (ALARP)' principle to the management of aviation safety risks.

2.2.3.3 The ALARP principle is applicable across all risk analysis techniques - quantified risk analysis, semi-quantified risk analysis, or qualitative risk analysis.

2.2.3.4 By correctly applying the ALARP[5] principle – and ensuring that risks are accurately mapped against the tolerability diagram shown in Figure 2.1 (*adapted from ICAO Doc 9859*) – unacceptable risks will not be tolerated and shall be further reduced through mitigation.

2.2.3.5 Where a specific TLS has been set – e.g., as an upper limit on the amount of risk set for entry to, or for implementation of, a new ICAO standard – it can be interpreted as the boundary between the 'A' and 'B' classifications of risk on the tolerability diagram and is equivalent to a 'Basic Safety Limit' (BSL)

EXAMPLE: For Reduced Vertical Separation Minima (RVSM), the target level of safety for collision risk set by ICAO is 5×10^{-9} Fatal Accidents per Flight Hour.

NOTE: In the diagram below, ALARP means that in reducing the level of risk from X to Y with X being initial risk (the risk level before any new controls are put in place) and Y being residual risk (the risk level after the application of risk treatment and controls) the ALARP shall be when the benefits gained from the reduction in risk shall be greater than the costs, time, and effort taken to reduce the risk. For higher levels of risk greater expenditure is justified.

[4] ICAO Safety Management Manual (*ICAO Doc 9859*) p.11

[5] Further guidance on ALARP is provided in Chapter 5 – *ALARP Guidance*

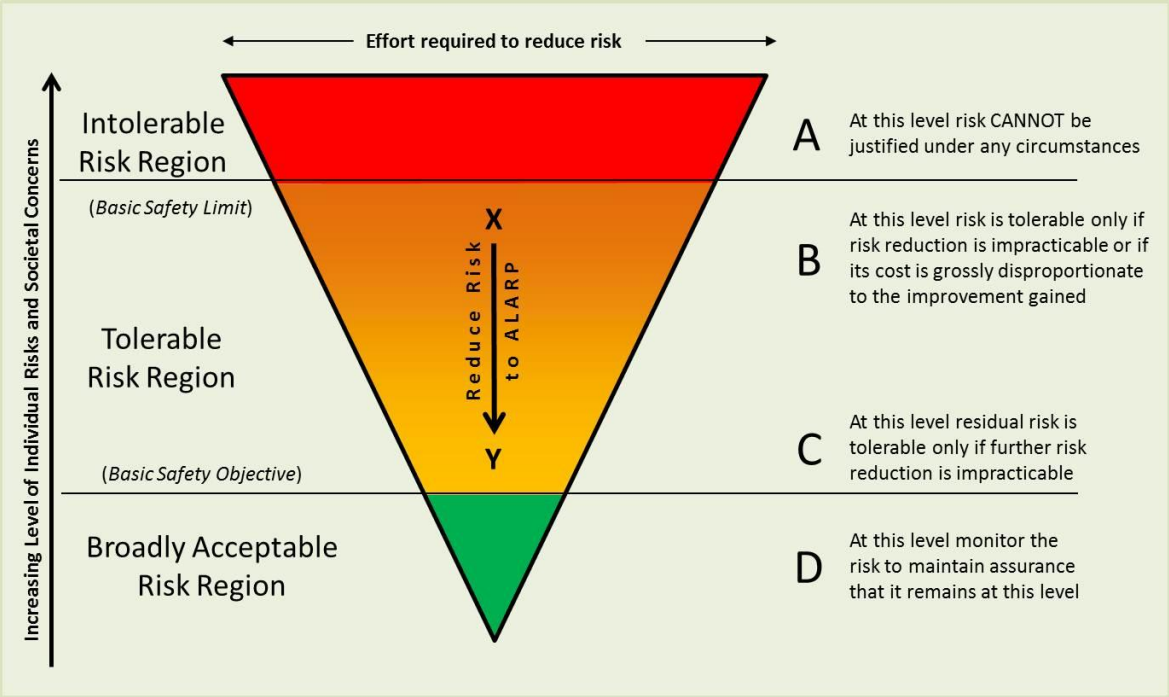

Fig 2.1: ALARP and Risk Tolerability

2.2.3.6 It is important that managers understand that there are risk limitations, and these are encapsulated within the safety risk management process.

2.2.4 Risk Criteria and ALARP

2.2.4.1 The principles of managing risk to a level that is ALARP are as follows:

- **There is an upper level of risk that is deemed to be intolerable.**
  If a risk is found to be intolerable, risk reduction measures are essential, regardless of cost – or the activities shall be stopped.

- **There is a lower level of risk that is deemed to be broadly acceptable.**
  At this risk level, current risk controls shall be maintained, and the risk shall be monitored and reviewed. Further risk reduction may be made, but only if the cost is insignificant.

- **The tolerable region lies between the intolerable and broadly acceptable levels of risk.**
  If a risk falls into this region, it shall be reduced. Risk reduction measures shall be identified and evaluated in terms of cost and benefit:
  - **ALARP Tolerability**, in this region the risk must be mitigated unless the cost of reducing the risk further is grossly disproportionate to the benefit gained i.e. the cost of reducing the risk is many times the value of the benefits gained. At this point it is defined as ALARP.

2.2.4.2 If the risk is assessed as falling into the tolerable region, this does not mean that the risk can simply be declared as ALARP. The risk can only be said to be tolerable when it can be demonstrated that all justifiable risk reduction measures have been adopted and the remaining options cannot be justified.

2.2.5 Safety Risk Management Process

2.2.5.1 The process for managing safety risks shall broadly follow ISO 31000 as shown in Figure 2.2 below. Each of the steps in this process is explained in the following chapters.

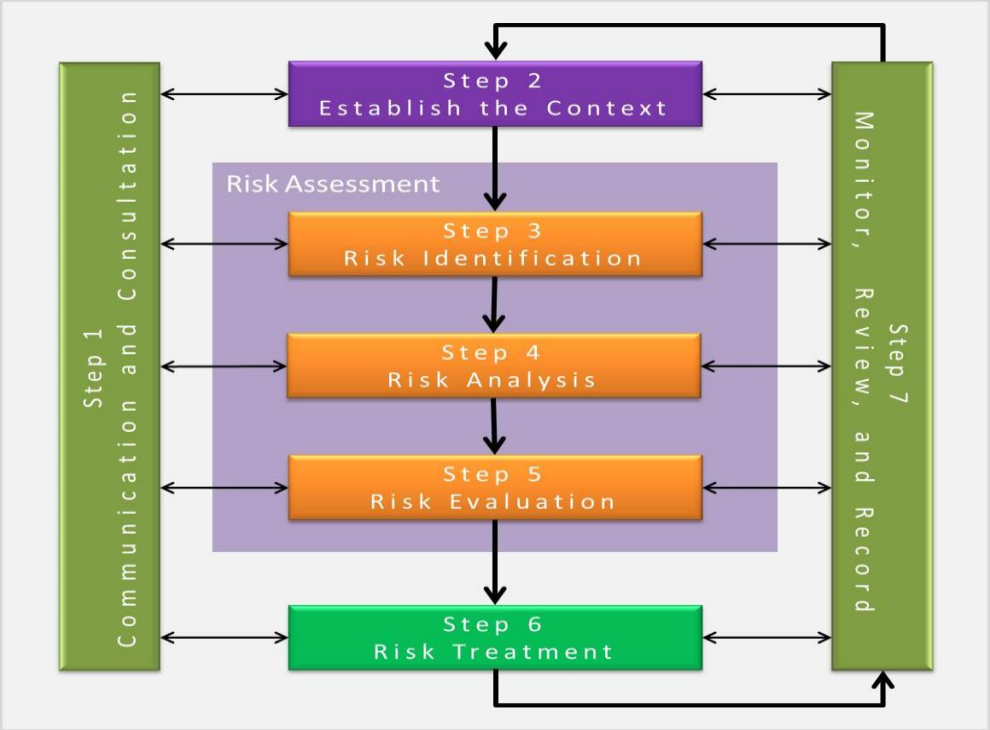

Fig 2.2: The Risk Management Process (*Source: ISO 31000-2009)*

2.3 Step 1: Communication and Consultation

2.3.1 Desired Outcome

1. An identified set of stakeholders; and
2. A plan for ensuring that those stakeholders are communicated with and consulted regarding risks and the risk management process.

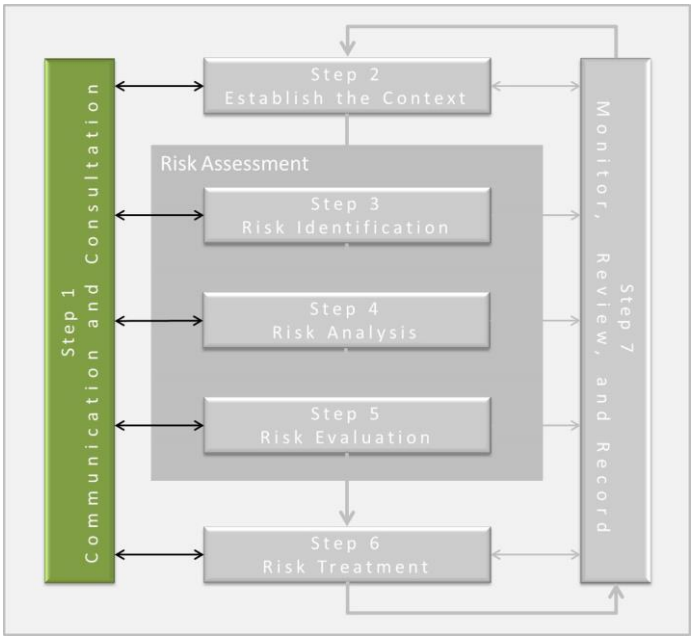

Figure 2.3- Step 1

2.3.2 Why is this Needed?

2.3.2.1 Communication and consultation are essential considerations at all steps of the safety risk management process. If these processes are carried out effectively it ensures that:

a. all stakeholders remain engaged and trust is enhanced;
b. risk mitigation adds value to the risk process as information and perspectives are shared; and
c. everyone is aware of the changes implemented, and why, for the risks being managed.

2.3.2.2 In this context, stakeholders are those who are potentially impacted by a particular threat, hazard, or change and those who have a role in controlling the related hazards and risks. Consultation with such individuals is particularly important where stakeholders shall:

a. Impact on the effectiveness of proposed risk treatments;
b. Be affected in incidents;
c. Add value to the assessment of risk;
d. Incur additional cost; or
e. Be constrained by future risk controls.

2.3.2.3 Although Communicate and Consult is listed as Step 1 of this procedure it is ***an ongoing process that shall be applied across all steps***.

2.3.3 What You Need To Do

Internal Stakeholders

2.3.3.1 Identify, communicate, and consult with internal stakeholders, including:

a. designers of the equipment, procedures, software, or systems under consideration;
b. managers and staff with current knowledge and experience;
c. subject matter experts;

d. workplace safety specialists;
e. standardization specialists;
f. safety and or risk specialists; and
g. human factors specialists.

2.3.3.2 Communication and consultation can be achieved verbally, by email, or at formal meetings e.g. progress meetings, hazard identification meetings, etc. meeting minutes and attendance must be kept for risk management records.

2.3.3.3 At later stages in the risk process you shall:
a. Gain input from stakeholders to ensure the assessment of hazards and risks that are associated with the proposed change is an accurate reflection of the situation.
b. Ensure staff are aware of:
i. the potential risks to which they are exposed or they shall encounter;
ii. their role in protecting themselves and others from the risks; and
iii. the operation of risk controls.

External Stakeholders

2.3.3.4 You shall determine if your risk management activity has external implications. If so, identify, communicate, and consult with external stakeholders. These could include:
a. airspace users;
b. other government departments or agencies;
c. equipment suppliers or manufacturers;
d. maintenance contractors; or
e. other third-party service providers (AMO, ATO, AOC, MET, AIS, ANS, etc.)

2.3.3.5 establish processes for identification of and communication with stakeholders (e.g. date and formats of meetings, timing of progress reports) if not already documented.

2.3.3.6 Examining previous similar risk management activities shall provide a good guide to these external stakeholders. Consider contacting previous project or line managers to seek their input on who you shall involve.

4.3.3.7 At later stages in the risk process you shall:
a. Ensure the assessment of hazards and risks associated with the proposed change is an accurate reflection of the current practice and situation.
b. Ensure personnel and external stakeholders are aware of the potential risks to which they shall be exposed and their role in controlling those risks.

2.3.4 The Communication and Consultation Plan

2.3.4.1 Depending on the size of the risk management activity you shall benefit from documenting your communication and consultation plan. Document the objectives, a list of stakeholders, the perspectives which the participants need to address, the communication methods and the evaluation process to be used.

2.4 Step 2: Establish the Context

2.4.1 Desired Outcome

1. An understanding of the scope of the activity under review – **WHY**, **WHERE,** and **HOW** is this being done, **WHO** is affected, and **WHAT** are the likely outcomes.

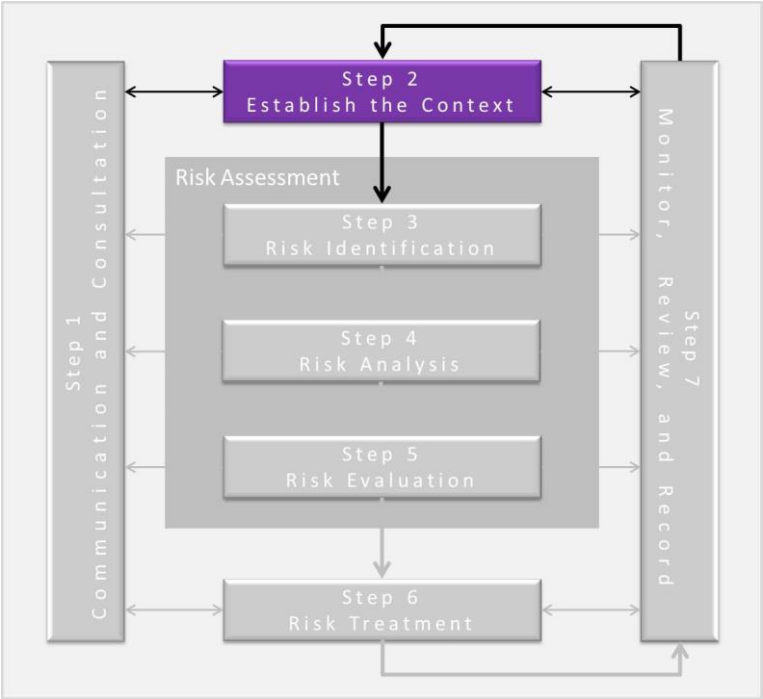

Figure 2.4 – Step 2

2.4.2 Why is this Needed?

2.4.2.1 Establishing the context is a vital part of the safety risk management process as it:

a. defines the basic parameters within which risks shall be managed;
b. sets the scope and scale for the rest of the risk management process;
c. ensures that internal and external stakeholders are considered when developing risk management criteria; and
d. minimizes the risk of not achieving organizational objectives.

2.4.3 What You Need To Do

Internal Context

2.4.3.1 You shall identify and understand:

a. internal stakeholders;
b. structure;
c. capabilities i.e. people, systems, processes;
d. organizational goals and objectives; and
e. physical constraints at the location of the proposed change e.g. remote location or confined space etc.

NOTE: *In most cases, such knowledge is intuitive as you work in the organisation but it is appropriate to consider how each shall impact on your activity e.g., subtle changes to organisational structure shall modify your stakeholders.*

External Context

2.4.3.2 You shall:

a. consider the external environment in which the risk operates;
b. consider the relationship between the risk and the external environment. This shall include:
   i. business, social, regulatory, cultural and competitive;
   ii. organizations strengths, weaknesses, opportunities and threats;
   iii. external stakeholders; and
   iv. key business drivers e.g., business plan, project plans etc.

Risk Management Context

2.4.3.3 You shall:

a. define the risk management activity, and the scale, by establishing goals and objectives;
b. specify the nature of the decision that needs to be made;

Example*: e.g. validate what is currently being done, discontinue work until particular controls are in place, and apply temporary protective measures until permanent solutions are in place;*

c. describe the relationship between the safety risk management activity and other activities within organisation that shall have an impact;
d. decide if it is a new risk management activity or a validation of existing risk management activity;
e. identify resources required;

Example: *is a qualified hazard facilitator required, what level of safety management assistance shall be required*

f. discuss roles and responsibilities of participants involved within the safety risk management process.

Example: *who has management responsibility, who has the authority to make decisions, who is controlling the hazard identification process, etc.*

2.5 Step 3: Identify Hazards and Risks

2.5.1 Desired Outcome

1. A documented and comprehensive list of hazards and causes covering all the credible threats that could present a safety risk.

2.5.2 Why is this Needed?

2.5.2.1 The identification of a comprehensive list of hazards and threats is fundamental to the whole risk management process - you can't analyze and control what you don't know.

2.5.2.2 To identify hazards and threats you shall determine appropriate identification techniques to help look for events that are a source of potential harm. This is a simple matter of deciding **WHAT** can happen, **WHEN** it can happen, **WHERE** it can happen, **HOW** it can happen, and **WHY** something can happen. During this step you shall continue to consult and communicate with stakeholders and record findings.

2.5.2.3 The identification of hazards and threats is an ongoing activity, all identified safety issues shall be brought to the attention of the relevant manager as soon as these are identified.

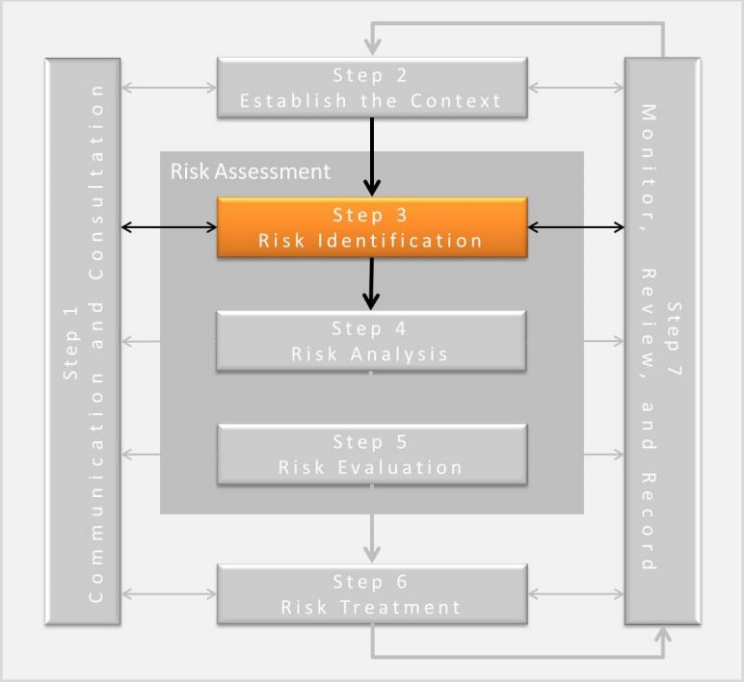

Figure 2.5 – Step 3

2.5.3 What you Need to do

What, Where, When

2.5.3.1 You shall generate a comprehensive list of sources of safety risks and events (*e.g. threats and initiating events)* that might have an impact on your overall achievement of the objectives identified in the context.

Note: *For projects, a typical technique for risk assessment at the concept stage is Preliminary Hazard Analysis (PHA – See Section 4.9 and Appendix E3). The PHA examines the broad functionality of the new system or service and considers the effects of losses of that functionality on the operating system or service. This enables the setting of high-level safety objectives or safety performance requirements.*

How, Why

2.5.3.2 You shall consider all possible causes and scenarios that are relevant to the context of the risk assessment.

2.5.3.3 Once these questions have been addressed you shall:

a. Determine appropriate techniques to help identify threats, hazards, and risks; and
b. Consult and communicate with stakeholders.

Note: *Hazard identification for individual tasks or projects of low to medium complexity can be completed using basic 'brainstorming' techniques, either formally or informally. For more complex individual tasks - or projects of medium to high complexity you shall use a very structured approach such as Hazard and Operability studies (HAZOP- see Appendix E5).*

2.5.3.4 Data collected in the safety data collection and processing system (SDCPS) shall be used as part of the input for this step where it is available.

2.6 Step 4: Analyze Risk

2.6.1 Desired Outcome

1. An expanded *and recorded* list from step 3 including existing controls, consequences, and likelihood of occurrence.

2.6.2 Why is this Needed?

2.6.2.1 Risk analysis involves developing an understanding of the (*untreated or current*) risk associated with the system (*if re-evaluating*) or the proposed change. Risk analysis provides an input to risk evaluation – and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies, and methods. Risk analysis can also provide an input into making decisions where choices need to be made about controls and residual levels of risk.

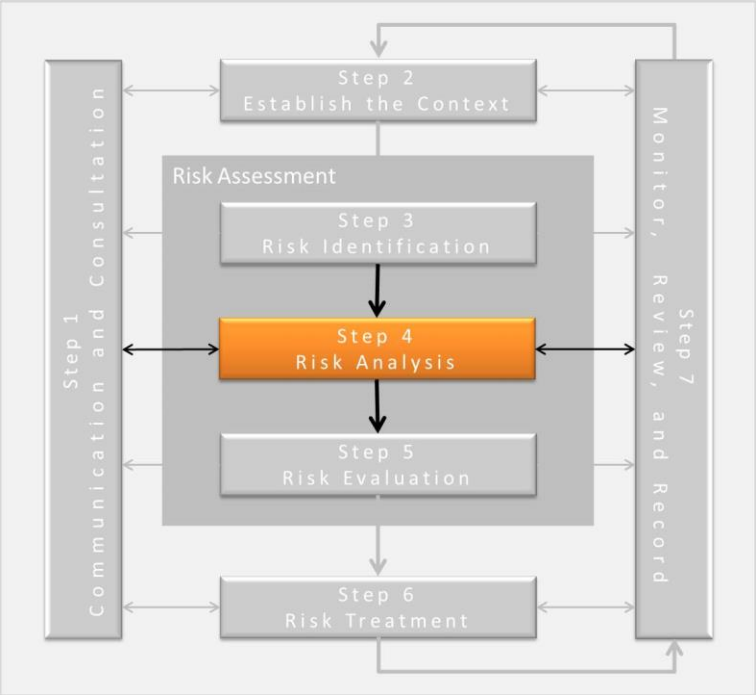

Figure 2.6: Step 4

2.6.2.2 Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood shall be identified.

2.6.2.3 Risk is analyzed by determining consequences and their likelihood of each hazard, and other attributes of the risk. An event can have multiple hazards and so multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency shall also be considered.

2.6.2.4 The way in which severity and likelihood are expressed - and the way in which they are combined to determine a level of risk – shall reflect the type of risk, information available, and purpose for which the risk assessment output is to be used. These shall all be consistent with the risk criteria. Consider also the interdependence of different risks and their sources.

2.6.2.5 Risk analysis can be undertaken with varying degrees of detail - qualitative, semi-quantitative, or quantitative - or a combination - depending on the circumstances.

2.6.3 What you Need to do

Evaluate Existing Risk Controls

2.6.3.1 You shall:

a. Identify existing controls or barriers where established and recorded, and confirm that they are operating as intended;
b. Identify additional existing control information which shall not yet have been recorded or entered into a Hazard Log system.

Determine the Severity and Likelihood

2.6.3.2 You shall:

a. Look at relevant information sources, such as previous records, before determining the severity and likelihood.

b. Communicate and consult to determine the relevant sources of information.

***Note**: To avoid subjective bias when determining consequence and likelihood levels, objective sources of data shall include incident records, statistical surveys, trials, safety reports, etc.*

2.6.3.3 Determine the severity and likelihood, using tables 2.2 and 2.3 below - use this information to determine the risk level (A, B, C or D) from table 2.4 (see also paragraph 2.6.3.6). Record the risk level.

2.6.3.4 Ensure that stakeholders are kept informed and that there is general agreement on the evaluated risk level. If agreement cannot be reached, discuss with your safety unit or safety manager for expert opinion then reconsult.

Consider Inter-related Risks and Cumulative Effects

2.6.3.5 You shall:

a. Identify any groups of related risks whose interactions and aggregate effect shall be considered when evaluating, treating, and accepting risk. Consider whether the cumulative effect of multiple aggregated risks shall result in an elevated overall level of risk and necessitate a higher level of sign-off. This determination shall be performed quantitatively, if sufficient data is available, and/or as a qualitative assessment.

b. Ensure these related risks, their possible interactions and cumulative effects are illustrated in your risk analysis.

***Note:** The effect of one minor risk event occurring frequently can be as debilitating on a system as a major risk event occurring rarely.*

LIKELIHOOD OR PROBABILITY CRITERIA			
Category	**Description**	**Examples of what to look out for**	**Examples of frequency**
1	Extremely improbable (Rare)	Almost inconceivable that the event will occur.	e.g., 1 in > 5 years
2	Improbable (Seldom)	Very unlikely that the event will occur. It is not known that it has ever occurred recently.	e.g., 1 in 3-5 years
3	Remote (Unlikely)	Unlikely but could possibly occur. Has occurred rarely.	e.g., 1 in 1-3 years
4	Occasional	Likely to occur sometimes. Has occurred infrequently.	e.g., 1 in 2 months to 1 year
5	Frequent	Likely to occur many times/regularly. Has occurred frequently/regularly.	e.g., daily, weekly, monthly

Table 2.2: Likelihood Criteria

SEVERITY CRITERIA					
Risk Severity definition		***Consequence (i.e., can lead to….)***	***Examples of what to look out for…***	***Examples of Effect on Aircrew or Passengers***	***Examples of Effect on ANS***
Category	***Code***				
Catastrophic	**5**	One or multiple deaths & complete loss / destruction of equipment	• A major accident.	• Multiple fatalities due to collision with other aircraft, obstacles or terrain	• Sustained inability to provide any service
Hazardous	**4**	Serious injuries/Major Damage to equipment	• Large reduction in safety margins, physical distress or workload such that the operators cannot be relied upon to perform their tasks accurately or completely.	• Large reduction in safety margin • Serious or fatal injury to small number • Serious physical distress to air crew	• Inability to provide any degree of service (including contingency measures) within one or more airspace sectors for a significant time
Major	**3**	Minor injuries/ Minor equipment damage	• A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of increase in workload, or as a result of conditions impairing their efficiency.	• Significant reduction in safety margin • Major illness or injury • Physical distress to occupants	• The ability to provide a service is severely compromised within one or more airspace sectors without warning for a significant time
Minor	**2**	Incidents	• Operating limitations are breached. • Procedures are not used correctly.	• Slight reduction in safety margin • Minor illness • Some physical discomfort to occupants	• The ability to provide a service is impaired within one or more airspace sectors without warning for a significant time
Negligible	**1**	Negligible outcome or Inconvenience	• Few consequences. • No safety consequences. • Nuisance.	• Potential for some inconvenience.	• No effect on the ability to provide a service in the short term, but the situation needs to be monitored and reviewed for the need to apply some form of contingency measures if the condition prevails

Table 2.3: Severity Criteria

2.6.3.6 The Likelihood versus Severity Risk Matrix shown in Table 2.4 below has been modified slightly from the matrix shown in ICAO Doc 9859. The adaptation allows a differentiation between risk that falls at the upper range of ALARP, and the lower range of ALARP, allowing a differentiation of risk treatment and management, and allowing the possibility to spread responsibility for risk management through an organisation. It shall be used in conjunction with the ALARP diagram (figure 2.1).

			Extremely Improbable (1)	Improbable (2)	Remote (3)	Occasional(4)	Frequent(5)
L	no mitigation needed	Cantastrophic (5)	6	7	8	9	10
M1	mitigation required should be treated as important - eg time frame 90 days	Hazardous (4)	5	6	7	8	9
M2	mitigation required should be treated as urgent - eg time frame 30 to 90 days	Major (3)	4	5	6	7	8
M3	mitigation required should be treated as critical - eg time frame less than 30 days	Minor (2)	3	4	5	6	7
H	activity must be stopped or immediate action required	Negligible (1)	2	3	4	5	6

Table 2.4: Likelihood versus Severity Risk Matrix

Risk Level	Risk Assessment Index (from Table 4)	Suggested Criteria
A	8-10	At this level risk CANNOT be justified under any circumstances.
B	6-7	At this level risk is tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained.
C	5	At this level residual risk is tolerable only if further risk reduction is impracticable.
D	2-4	At this level monitor the risk to maintain assurance that it remains at this level.

Table 2.5 – Risk Level

2.7 Step 5: Evaluate Risks

2.7.1 Desired Outcome

1. A list - expanded from the Step 4 list - identifying acceptable risks and those risks requiring additional risk treatment.

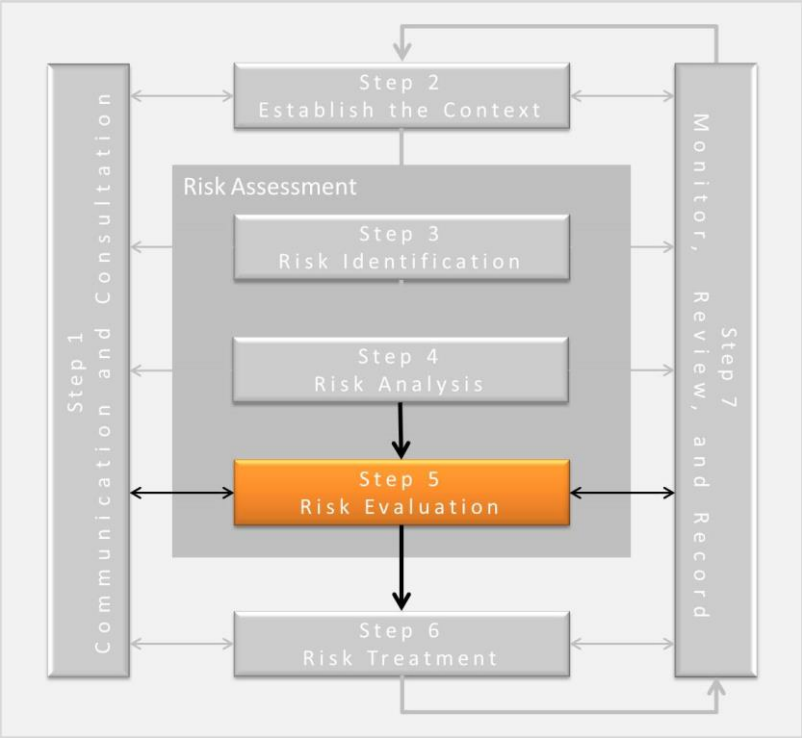

Figure 4.7: Step 5

4.7.2 Why is this Needed?

2.7.2.1 Risk evaluation is needed to enable you to make decisions based on the outcomes of the risk analysis, about which risks need further treatment, and treatment priority, taking into account the ALARP principle.

2.7.2.2 The evaluating process means you shall decide on whether risks shall be accepted, or whether they require further analysis or treatment and how much. This is done using the ALARP principle.

2.7.2.3 Decisions shall take account of the wider context of the risk and include consideration of the tolerance of the risks borne by internal and external parties. Decisions shall be made in accordance with any legal, regulatory, or other requirements.

2.7.2.4 In some circumstances, the risk evaluation can lead to a decision to undertake further analysis (return to step 4). The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls.

2.7.2.5 As previously, during each step, you shall consult, record, review and monitor.

2.7.3 What you Need to do

Compare Against Criteria

2.7.3.1 You shall compare the determined risk level from Step 5 against the tolerability diagram (*figure 2.1*) and risk level (Table 2.5). This will show the tolerability of the determined risk (*before risk treatment*).

Note: *As indicated earlier ALARP, with respect to categories B and C risks, means that in reducing the level of risk from X to Y with X being initial risk (the risk level before any new controls are put in place) and Y being residual risk (the risk level after the application of risk treatment and controls) the benefits gained from the reduction in risk shall be greater than the costs, time and trouble taken to reduce the risk. For higher levels of risk greater expenditure is justified.*

Note: *All safety risks shall be managed to either the tolerable or broadly acceptable regions in the tolerability diagram, irrespective of target levels of safety or which particular methodology has been used for assessment and evaluation.*

Note: *To ensure the highest levels of scrutiny, 'B' class risks should only be signed off by General Managers, Accountable Executives, Deputy Directors, or higher, see table 2.7).*

Set Priorities

2.7.3.2 You shall now set risk treatment priorities using the following considerations:

a. For new risk management activity: Are there any controls required to reduce the risk to ALARP? Consider cost and business implications.
b. For existing risk management activity: Are there any additional controls which can be implemented to reduce risk level? Consider cost implications.

Note: *A formal Cost Benefit Analysis shall be appropriate for high severity risks or for lower severity risks where the cost of risk treatment is considered excessive.*

Factors to be Considered

2.7.3.3 When prioritizing risks for treatment, and assessing potential controls, the overall judgment that risk is tolerable shall be based on broad considerations that include:

a. Does the design and operation comply with standards or industry codes of practice?
b. Is the project or risk new or has it been assessed previously?
c. What is the current status of safety management system controls?
d. Is this type of risk something we have historically managed well or otherwise?
e. Is the evaluation of the cost/benefit balance qualitative or quantitative or (preferably) both?
f. Has the safety risk assessment process been conducted correctly?
g. Are we using industry best practice?

The Effect of Uncertainty

2.7.3.4 In the absence of firm evidence it is more difficult to make absolute judgments about likelihood or severity. If estimates, assumptions, or data containing general uncertainty have been used in risk analysis you shall conduct a sensitivity analysis. This allows you to look at how the risk profile would vary if one or more parameters changed. This can provide you with assurance that your risk assessment is sustainable and help in assessing treatment strategies.

2.7.3.5 If high levels of uncertainty about the evaluation exist, additional control measures SHALL be considered.

Note: *A sensitivity analysis involves the study of how the evaluated severity level of risk varies dependent on changes in the assessed frequency of occurrence and consequences of the likely outcomes i.e. the inputs to the calculation, qualitatively or quantitatively, are varied to ascertain the effect on the evaluated risk level.*

2.8 Step 6: Treat Risks

2.8.1 Desired Outcome

1. A list – expanded from the Step 5 list – identifying all risks controls required to ensure the risk levels are ALARP.

2.8.2 Why is this Needed?

2.8.2.1 All identified risks from Step 5 shall be treated to reduce the level of risk to a level that is ALARP. Treating risks involves selecting the most appropriate option to overall balance the costs of implementing each option against the benefits derived from it, this becomes known as the risk treatment plan.

2.8.2.2 All feasible options for treating risks shall be considered, and complex treatments shall require significant planning effort and the use of Cost/Benefit Analysis.

2.8.2.3 As risk management shall be continued during the entire life cycle of the system it is possible that controls which have been rejected at present based on cost could be implemented at a later date. All identified potential controls or barriers shall be recorded and tracked in a hazard log system so future project/line managers do not have to redo work.

2.8.2.4 A risk impact assessment and change management process shall be completed prior to implementation of any proposed actions.

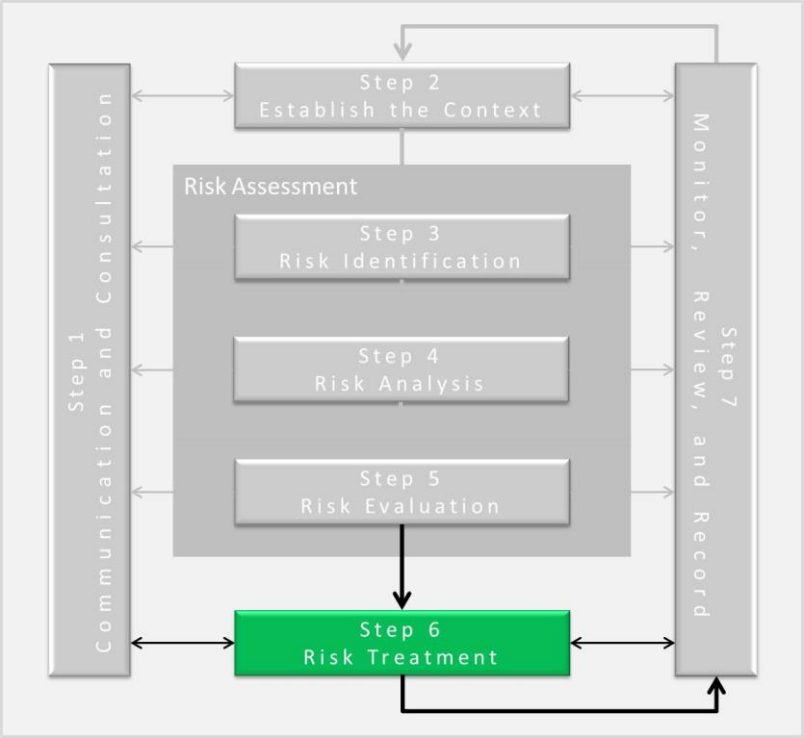

Figure 2.9 – Step 6

2.8.3 What you Need to do

Selecting Appropriate Risk Treatment

2.8.3.1 Risk treatment can involve a number of options, including:

a. avoiding the risk by deciding not to start or continue with the project;
b. taking or increasing controlled risk in order to pursue an opportunity, with mitigation;
c. removing the risk source;
d. changing the likelihood;
e. changing the consequences;
f. transferring or sharing the risk with another party or parties; or
g. retaining the risk by informed decision.

2.8.3.2 If the decision is taken to treat the risks, there are four hierarchical strategies that shall be pursued:

a. **Risk Elimination or Avoidance**: Removal of the specific threat or exposure to the specific threat that shall lead to a consequence, this is a permanent solution and, when conditions permit is the most preferred since the risk will no longer be present.

b. **Risk Prevention:** Prevention of the threat from causing a consequence, this shall involve replacing or substituting the hazard or creating a new response to the hazard.

c. **Risk Reduction and Mitigation**: Reduction and mitigation of the immediate impact of the risk or hazard, preferably by use of engineering controls (*these involve physical barriers or structural*

changes to the environment or process). If engineering controls cannot be implemented then administrative controls shall be applied (*e.g., documented procedures and instructions*).

d. **Risk Recovery:** Recovery from the consequences of the risk shall be considered in the form of contingency or emergency plans.

2.8.3.3 Risk treatments for each hazard and threat shall be considered both individually - and as a group.

2.8.3.4 A good risk treatment strategy is biased towards risk elimination (*the most effective strategy is to eliminate the hazard, if at all possible, by designing out the hazardous activity*), but will cover all aspects, providing 'defense in depth'. If this is not possible, then the hazard shall be prevented from occurring, or have the likelihood reduced by providing more effective means of controlling some of the causes.

2.8.3.5 If the risk can't be eliminated or prevented there shall be a reduction in the effects of the hazard (*e.g., by improving detection systems, providing additional redundancy, awareness, procedures, and controls, etc.*). Finally, further measures shall be taken to recover from the occurrence and hence reduce the overall risk, for example by shortening repair times.

2.8.3.6 An effective control strategy also includes a range of different physical and administrative types of controls. Some shall be practical things such as engineering back-up systems or specific software functionality. Others shall be procedures and processes designed to prevent or detect errors.

2.8.3.7 Engineering controls are generally more expensive than procedural controls, but they are more reliable. On the other hand, while easier to implement, procedural controls are subject to the strengths and weaknesses of human behavior. Training and awareness is essential when implementing new controls of either kind.

2.8.3.8 If the action required to manage the hazard is broad ranging and not always well defined then the best control strategy shall be to make use of human adaptability and judgment.

2.8.3.9 Once the strategies are determined they shall be used to create a risk treatment plan inclusive of a risk impact assessment and change management evaluation (see chapter 3 and 4).

2.9 Step 7: Monitor and Review

"Risk has a dynamic context resulting from the constantly changing external and internal environments. Organisations must monitor not only risks but also the effectiveness and adequacy of existing controls, risk treatment plans and the process for managing their implementation." AS ISO 31000: 2009

2.9.1 Desired Outcome

1. A mechanism to identify, evaluate, and continuously monitor new risks that may arise from actions taken to mitigate other safety risks, including residual risks.
2. A documented record of the risk management process for each system change.

2.9.2 Why is this Needed?

2.9.2.1 Ongoing monitoring and review are essential to the success of the safety risk management process. Factors that affect the likelihood and consequences of an outcome shall change, as shall the factors that affect the suitability or cost of the risk treatments used. It is therefore necessary to keep the safety risk management system under continual review.

2.9.2.2 Operational and technical managers, project managers, and staff, shall be vigilant in monitoring residual risk levels and if necessary, changing the risk treatments at all times, not just during an annual review or at a particular milestone in a project.

2.9.2.3 The monitoring and review process shall be pro-active, identifying and rectifying deficiencies as they occur in real time. It also allows for lessons to be learned, not only from the risk management process but also from events, incidents, and accidents that occur despite our best endeavors to control them.

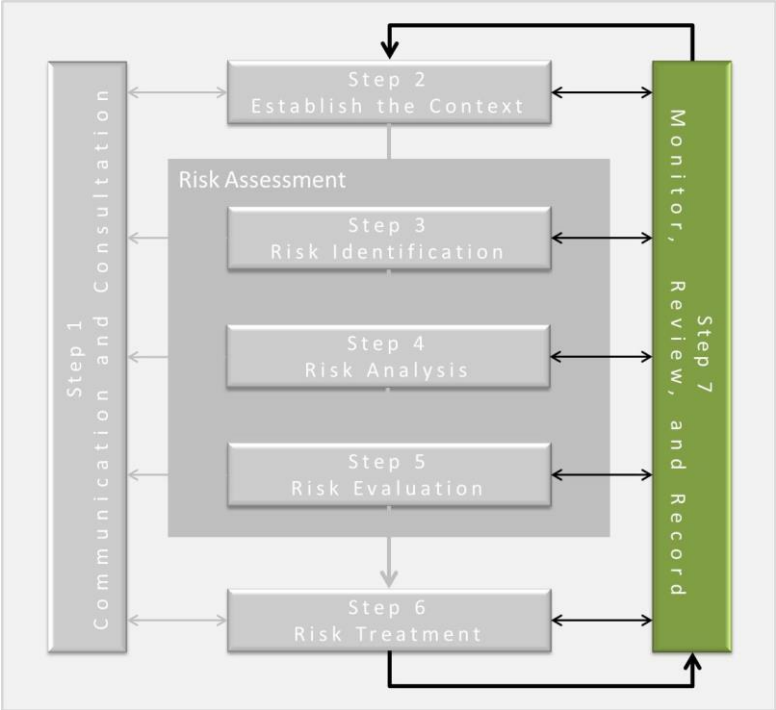

Figure 2.10 – Step 7

2.9.2.5 Monitoring and review of safety risks is a continuous process and is carried out at various levels of management to ensure that nothing 'slips through the safety net'.

2.9.3 What you Need to do

Monitor and Review

2.9.3.1 All new risk mitigation strategies must be monitored for potential effects of the change. There must be a feedback loop and review process. Monitoring and review must be a planned part of the risk management process, results of which should be recorded and reported.

2.9.3.2 Monitoring and review should be most frequent after the changes are implemented once changes are ingrained normal monitoring is sufficient.

2.9.3.3 Responsibilities for monitoring and review should be clearly defined. The monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

a. Ensuring that controls are effective and efficient in both design and operation
b. Obtaining further information to improve risk assessment
c. Analysing and learning lessons from risk events, including near-misses, changes, trends, successes, and failures
d. Detecting changes in the external and internal context, including changes to risk criteria and to the risks, which may require revision of risk treatments and priorities
e. Identifying emerging risks

2.9.3.4 Risk monitoring and measurement can include ad-hoc audits, planned audits, user surveys, management surveys, customer surveys, safety data collection and processing system output analysis, or output review. The means required will be determined by the size of the change mitigation implemented.

Record and Document

2.9.3.5 You shall record each step of the Safety Risk Management Process. All safety risk assessments shall be properly approved and endorsed by the appropriate manager or authority. A safety risk recording system (*e.g., Hazard Log*) is essential to ensure that the hazards and risks identified in the risk assessments are documented and their controls implemented. The following steps indicate an outline of what type of recording you shall consider at each step.

Safety Risk Management Steps		What to Record and Document
Step 1	**Communicate & Consult**	Record your findings, assumptions, contributions, and recommendations.
Step 2	**Establish the Context**	Describe the system or process that is under assessment.
Step 3	**Identify the Hazards and Risks**	Select and document an appropriate and relevant technique to use for Safety Risk Management activity. Further consultation and communication shall be recorded. Record findings into the Hazard Log.
Step 4	**Analyse Risks**	Document results as a record of risk assessments.
Step 5	**Evaluate Risks**	Review controls that shall be required to reduce the risk to ALARP and document it. When considering controls, review existing information in Hazard Logs.
Step 6	**Treat Risks**	Prepare a treatment plan and document it. **R**ecord the proposed risk treatment (*controls and barriers*) in a Hazard Log.
Step 7	**Review, Monitor, and Record**	Record findings in a Hazard Log for ongoing monitoring and review.

Table 2.6: The Recording Process

2.10 Sign-Off Authority for Risk

2.10.1 After having determined the risks associated with a project and having treated those risks to reduce then to ALARP, an appropriate entity needs to accept accountability for that residual risk.

2.10.2 The level of risk that can be accepted by a particular person is fundamentally related to the consequences of the risk, level of authority of that person to apply the resources necessary to control the risk, and level of management accountability of the person. Low or insignificant risks can be accepted at a lower level in the management structure than high levels of risk.

2.10.3 Table 2.7 below indicates the accountability and sign off authority for risks. The risk classification (*A-D*) relates to both the unmitigated or untreated risk, the responsible mitigation, and then the treated risk categorization that has been determined from the tables (*Tables 2.2, 2.3, and 2.5*) in Step 4.

Risk Classification	Actions Required	Sign-Off Authority
A	**Risk intolerable and cannot be justified or accepted under any circumstances**	
B	Risk shall be reduced unless the cost of reducing the risk is grossly disproportional to the benefits gained.	Only accepted in exceptional circumstances with the approval of the **General Manager or Deputy Director or higher** accountable executive for the affected people or service. The responsible manager will require a risk re-evaluation after project implementation to try to reduce the risk to C or lower.
C	Risk shall be reduced unless the cost of reducing the risk is disproportional to the benefits gained.	Shall be accepted by a **3rd level manager** (e.g., Section Chief, Senior Manager, Manager of Safety) with accountability for the affected people or service. *Note: Where a Class C risks affects more than one manager's accountability, it shall be necessary to elevate the risk to the relevant General Manager for sign-off.*
D	Maintain current systems, monitor and review. Further reduction only if cost is insignificant.	Acceptable by the **manager/supervisor** with accountability for the affected people or service. Shall also be acceptable at an operational level (e.g., ATC, pilot, engineer, etc.)

Table 2.7: Safety Risk Management Actions and Sign – Off

2.10.4 Most often a project or a change proposal will result in several risks – and after treatment each will have residual risk at varying risk classifications – some at "D", some at "C", and ideally only one or two at "B". Each completed risk assessment package shall be accepted and signed-off individually by the appropriate management level.

2.10.5 The project can only proceed after all risks have been accepted and signed-off.

2.10.6 In the case of Category "B" risks, most often the General Manager will specify a requirement that the risk is accepted only on the basis that it will be re-evaluated after the change has been implemented to see if the risk can be reduced to "C" or less.

Guidance: *Often, in the absence of evidence, the severity or likelihood of a risk shall be classified conservatively in the design phase – but after a post implementation review it shall become apparent that the risk assessment may be changed. Whilst this is often a re-assessment to a lower risk classification, caution shall be exercised, as the 'apparent' change in risk could be the result of increased focus on safety during the change itself which may relax with time.*

CHAPTER 3 THE CHANGE ASSESSMENT PROCESS

3.1 Introduction

3.1.1 Any change to the way in which a service is provided, equipment utilized, procedures and processes, and any risk mitigation implemented shall first be assessed to identify if there is any change in safety risk or impact on risk assessment due to the change. If so, what is the magnitude of that change in safety risk, and what level of mitigation is required to continue to provide an acceptable level of safety performance (ALoSP). This is a fundamental tenet of the management of change under a Safety Management System.

3.1.2 Many changes will be relatively small and some have no impact on operational safety – however some are of a nature that affects large parts of the organisation, significantly affects operations, and/or significantly affects users.

3.1.3 It is necessary to tailor both the safety risk assessment process – and the means of recording the assessment and decision making processes (the safety argument) – to the size or level of the change. **This ensures that safety management resources are appropriately focused according to risk**.

3.1.4 There are three primary steps to the change management process:

- **Step 1:** Change Evaluation Process and/or Safety Statement;
- **Step 2:** Safety Plan;
- **Step 3:** Safety Assessment or Safety Case.

3.1.5 Completion of the first step will determine if steps two and three are required.

3.1.6 Figure 3.1 shows an overview of the 3-Step process. Each step is discussed in more detail in the following sections.

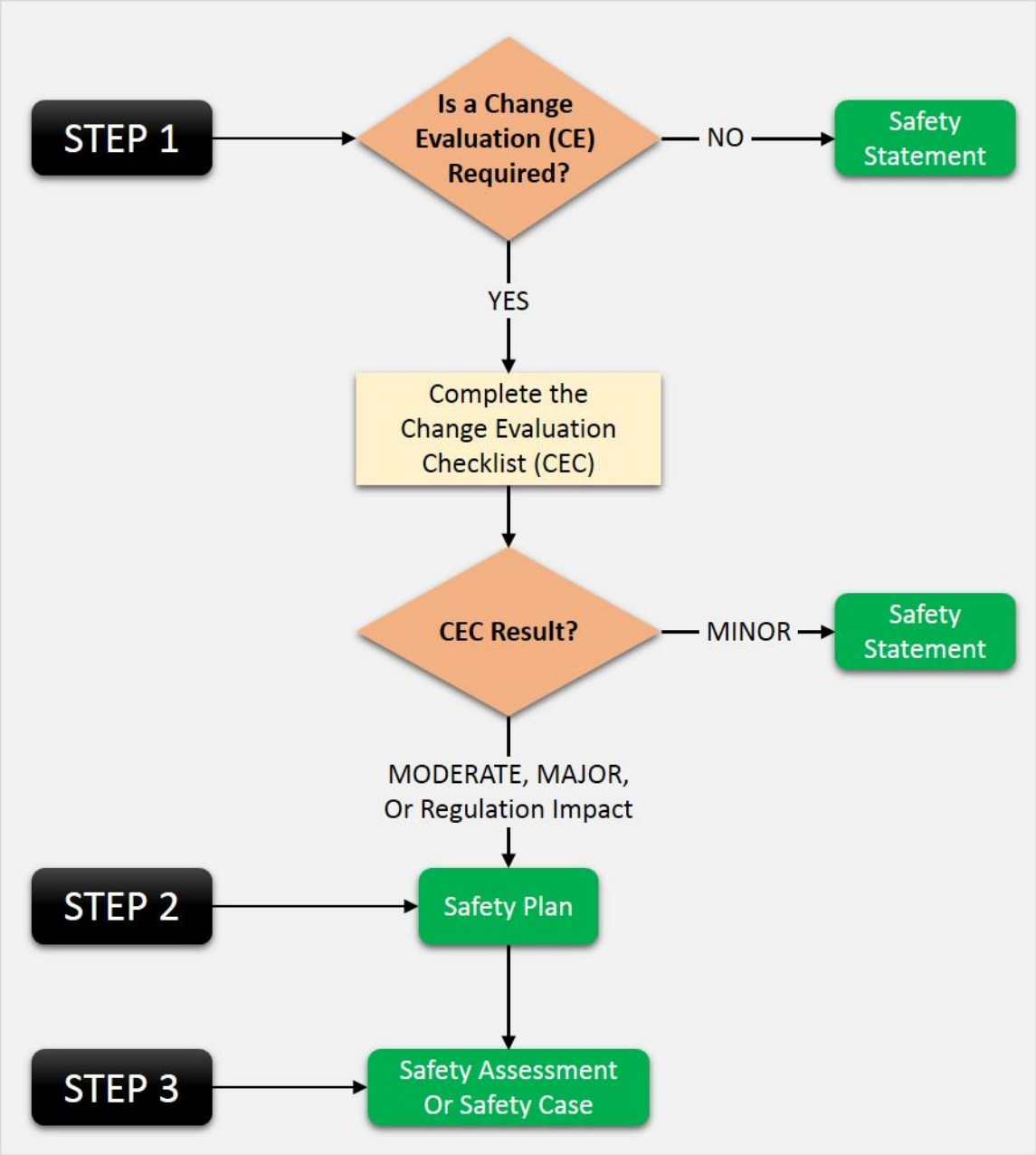

Figure 3.1: The 3-Step Safety Assessment Process

3.2 Step 1 – Change Evaluation (CE) and Safety Statement (SS)

3.2.1 Is a Change Evaluation (CE) Required?

3.2.1.1 A Change Evaluation (CE) shall be conducted for:

- changes to service levels, procedures, or equipment, which will affect the performance, functional or technical specification of a system or service; and
- organizational changes affecting safety accountabilities.

3.2.1.2 Where the proposed change will not result in any of the above items, or the change is of a routine maintenance or administrative nature, the applicable change process shall be used instead of the CE and associated CE Checklist (CEC).

3.2.1.3 Where a change process is used instead of the CE/CEC, a Safety Statement (SS) shall be prepared.

3.2.1.4 The Safety Statement shall provide sufficient information to demonstrate that safety has been considered and the change presents minimal or no safety issues.

3.1.1.5 A Safety Statement shall also be used if the CEC results in an assessment of "Minor".

3.2.2 Complete the Change Evaluation Checklist (CEC)

3.2.2.1 The CEC is designed to assist users to evaluate the change proposal, so that they can determine what type (or scale) of safety assessment and safety reporting is required.

3.2.2.2 The CEC shall be completed at the start of a change process, to ensure that the safety reporting requirements and impact of the change are identified and managed for all affected areas.

3.2.2.3 The CEC template form (Appendix A) is designed to help in assessing the proposed change in relation to its technical and operational considerations.

3.2.2.4 Because of this, adequate representation from all appropriate areas affected by the change shall participate in the completion of the CEC.

3.2.2.5 The CE Checklist is discussed in detail in Chapter 4. Templates for the CEC are in Appendix A.

3.2.3 CEC Outcome

3.2.3.1 Where the outcome of the CEC indicates a Minor change, a simple Safety Statement is the only requirement, and this shall be included in, or attached to, the CEC.

> ***Guidance**: The CEC process itself forms the main evidence that a safety process has been done for the proposed change – so the Safety Statement shall be as simple as "…on the basis of the CEC, it has been determined that no further safety assessment is required for this change…". This statement can be written into the CEC document or attached separately to the CEC.*

3.2.3.2 The Safety Statement or justification included in the CEC shall provide management with sufficient information to demonstrate that safety has been considered, and the change presents minimal or no safety issues.

3.2.3.3 Where he/she considers it appropriate, the change/project sponsor or responsible Manager shall direct a Safety Assessment to be developed even where the outcome of the CEC indicates a Minor change would take place.

3.2.3.4 Where this occurs, Steps 2 and 3 of the 3-Step process apply.

3.2.3.5 Where the outcome from the CEC indicates that a Safety Assessment or Safety Case is required, i.e., a Moderate or Major assessment, Steps 2 and 3 of the 3-Step process apply.

> ***Guidance**: A Safety Assessment is made when a situation may be approved by the senior manager or internal entity; when it is determined that changes to regulations or standards would be required, a Safety Case is required, which requires prior approval from the regulator.*

3.3 Step 2 – Safety Plan

3.3.1 Where the outcome of the CEC indicates that a Safety Assessment or Safety Case is required, a Safety Plan shall first be prepared.

3.3.2 Safety Plan preparation shall commence early in the project/change life cycle and shall be updated as appropriate during the project/change implementation.

> ***Guidance**: A Safety Plan need not be a complicated document. In basic terms, it is a 'story' or 'narrative' telling the reader how the project personnel will consider safety throughout the project. This shall include statements about conducting a CEC, taking certain safety actions, employing certain safety personnel, carrying out risk assessments and so on. For simple projects the Safety Plan may simply be a chapter in the Project Plan.*

3.3.3 A Safety Plan may be a stand-alone document or incorporated into a Project Plan.

3.3.4 Whichever option is utilized, the review and approval requirements detailed in this document apply.

3.3.5 The Safety Plan (or Project Plan if Safety Plan is incorporated) shall detail the:

a. scope of the change in operational and organizational context;
b. assumptions, constraints, and dependencies influencing the safety outcome of the project/change;
c. responsibilities, titles, and names of the people managing the project/change;
d. consultation and communication arrangements for the project/change;
e. safety management activities to provide the safety assurance of the project/change (hazard identification and risk management activities);
f. timelines and milestones;
g. resources and facilities;
h. training and education requirements;
i. review process; and
j. approval authorities and requirements for the resultant safety documentation.

3.3.6 Much of the content of the Safety Plan can then be exported directly to the Safety Assessment or Safety Case.

3.3.7 A template for a Safety Plan can be found in Appendix B.

3.4 Step 3 – Safety Assessment or Safety Case?

3.4.1 Staff preparing Safety Assessments and Safety Cases shall have appropriate safety management training.

3.4.2 A Safety Assessment is used primarily for internal purposes.

3.4.3 Safety Assessments are prepared for Major/Moderate changes where a Safety Case is not required. Safety Assessments shall provide operations management with sufficient assurance about the safety of the change.

3.4.4 A Safety Case is the type of safety report sent to or performed by the regulator, where prior regulatory approval of the proposed change is required – e.g., if a change to regulations or technical standards is required.

3.4.5 Safety Cases shall provide all parties with sufficient assurance about the safety of the change to proceed with the planned change or select an alternative solution.

3.4.6 Safety Assessments and Safety Cases shall be updated during the course of the project/proposal implementation.

3.4.7 Safety Assessments and Safety Cases shall detail the:

a. scope of the change in operational and organizational context;
b. validation of any assumptions, constraints, and dependencies affecting the safe outcome of the project/change;
c. responsibilities, titles and names of the people managing the project/change;
d. consultation and communication arrangements for the project/change;
e. the outcomes of the safety management activities detailed in the Safety Plan including the:
    i. hazard identification and risk management activities, tools, procedures, and standards used to provide safety assurance, for normal and abnormal modes of operation;
    ii. risk report detailing the identified hazards and risk controls/safety requirements, including their status;
    iii. acceptance by the appropriate level of management of the various levels of risk associated with each hazard;
f. arrangements for any training and education requirements;
g. timelines and milestones for the ongoing safety management of the change pre- and post-implementation;
h. argument that, when implemented with the identified controls, the proposed change will be adequately safe; and
i. arrangements and timing for the Post Implementation Review (PIR) of the change following implementation.

3.4.8 A template for a Safety Assessment / Safety Case can be found in Appendix C.

3.5 Review of Safety Documents

3.5.1 All Safety Plans, Safety Assessments, and Safety Cases shall be reviewed on a regular basis – i.e., they are ‘living documents’.

3.5.2 Safety Plans prepared to support Safety Assessments shall be reviewed by the relevant operational and/or technical units.

3.5.3 Safety Assessments shall be reviewed by the relevant operational and/or technical units.

2.5.4 Safety Plans prepared to support Safety Cases shall first be reviewed by the relevant operational and/or technical units, then the Safety and Quality Assurance department for review and endorsement.

2.5.5 Safety Cases shall first be reviewed by the relevant operational and/or technical units, then sent to the Safety and Quality Assurance department for review and endorsement.

2.5.6 Where recommendations from the review(s) are not included into the final documentation, justification for this shall be provided to the reviewer.

2.5.7 Where the Safety Plan forms part of the Project Plan, the review shall demonstrate that the requirements for a Safety Plan have been met.

2.5.8 Once a Safety Case has been finalized and endorsed, it shall be circulated for approval by the regulator prior to the change taking place.

3.6 POST IMPLEMENTATION REVIEW

3.6.1 A Post Implementation Review (PIR) of the safety aspects of a change detailed in a Safety Assessment or Safety Case shall be completed and documented.

3.6.2 The PIR shall be conducted in accordance with the timeline specified in the Safety Assessment or Safety Case and no later than twelve months after the change becomes operational.

3.6.3 The PIR shall include:

a. a review of the risks identified relating to the change;
b. the arrangements for the ongoing management of hazards/controls;
c. details of any new safety issues identified resulting from the change; and
d. details of any safety lessons learned.

3.7 DOCUMENT MANAGEMENT

3.7.1 Safety Plans, Safety Assessments, Safety Cases and Change Evaluations shall be managed in accordance with approved record management procedures.

3.7.2 To ensure coordination of changes across the system, draft and approved Safety Plans, Safety Assessments, and/or Safety Cases shall be indexed in a document database to indicate their existence, set review dates, and provide a contact point for further information.

CHAPTER 4 CHANGE EVALUATION CHECKLIST (CEC)

4.0 Introduction

4.0.1 This chapter discusses a recommended Change Evaluation Checklist process aimed at determining the size and scale of a change, from a safety perspective, and the subsequent safety reporting process required.

4.0.2 The CEC contains 8 sections with guided questions designed to support the 3-Step process discussed in Chapter 3, and to determine if a simple Safety Statement is required, or a more complex Safety Plan, followed by a Safety Assessment or Safety Case.

4.0.3 Refer to Appendix A Change Evaluation Checklist.

4.1 Section 1 – Details of the Proposed Change

4.1.1 In this section the proponent shall provide a more substantial description of the proposed change or project. Where there is other project documentation available to describe the change, this shall be referenced here, and attached to the Safety Risk Assessment (electronically if it is a large file).

4.2 Section 2 – Will Civil Aviation Regulations be Affected?

4.2.1 This step contains questions to determine if the regulator needs to be directly involved in the safety approval process. This will generally only be the case if the proposal involves a change that would alter the regulatory certification of the organization.

4.2.2 For example, if the change was about upgrading air traffic controller workstations, this might affect conditions in NAMCARs Part 172 or associated Technical Standards – and would therefore require prior approval from ANSSO.

4.2.3 If the change was an upgrade of an existing fleet for an AOC holder it will require a change to the certificate and associated manuals and requires regulatory approval.

4.2.4 If the change was simply to replace ATC workstations with identical equipment because of routine maintenance, this would not materially change the conditions in regulations – and would not, therefore, require ANSSO approval.

4.2.5 It is possible that the answer to Question 2.1a of Step 2 will be YES – in which case it is determined already that a Safety Case will be required. Even so, the proponent shall continue the Safety Risk Assessment process and complete the form, as the analysis done by completing the form could be of significant use in completing the subsequent Safety Case.

4.3 Section 3 – Size of Change

4.3.1 Assessing the size of the change is important as it allows the proponent to determine the stakeholders involved or affected by the change and identify the likely level of coordination involved.

4.3.2 The indicative size of the change is determined through the quantitative rating of six elements is made based on qualitative data. To complete the step, the person(s) completing the assessment shall select a rating or number for each element based on judgment and experience. When these ratings are added together the change can be assessed as:

- Small (score of 6-18),
- Medium (score of 19-30) or
- Large (score of 31-42).

4.3.3 It shall be noted that a rating of 1 would indicate a small change, localized to a single location, with little or no noticeable effect on the system – whilst a rating of 7 would have maximum impact on system performance. The person(s) completing the assessment shall be realistic about their rating and shall avoid simply picking a middle number.

4.3.4 Having selected a rating or number, the person(s) completing the assessment shall provide a basic justification for their selection. This need not be detailed – but shall be defensible.

4.4 Section 4 – Operational Safety Impact

4.4.1 The estimated Operational Safety Impact is determined through a **Preliminary Hazard Analysis** (PHA). It involves identifying the obvious hazards and assigning a severity to those hazards. Based on the number of hazards and their severity, the safety impact rating is identified as either Minimal, Reasonable or Substantial.

4.4.2 As with the Size of Change, it is important to record the names and qualifications of the persons conducting the operational safety impact assessment, to provide appropriate assurance to the people ultimately authorizing the Safety Risk Assessment.

4.4.3 More information on the Preliminary Hazard Analysis can be found at paragraph 4.9.

4.5 Section 5 – Overall Operational Safety Magnitude

4.5.1 This is a simple matrix process where the size of change is matched to the operational safety impact to determine whether the safety magnitude of the proposed change will be Major, Moderate, or Minor.

4.5.2 It shall be remembered that these classifications are only for the purpose of determining what safety reporting process will ultimately be required – and to provide some assurance that the process was sound.

4.6 Section 6 – Operational Safety Reporting Requirement

4.6.1 This is the step which identifies the required Safety Reporting for the change or project. It is simply a matter of checking the responses from Section 2 and Section 5 against the table. This will determine if a Safety Statement, a Safety Assessment, or a Safety Case is required – and identify the basic required actions.

4.6.2 It shall be noted that if Section 2 identifies a requirement for a Safety Case, it will over-ride any smaller

requirement from Section 5, for example a classification of "Minor".

4.6.3 It shall also be noted that if the answer to question 2.1b was YES, the regulator must be contacted to discuss exactly what they will or will not require. The regulator may, for example, look at the change and advise that they do not need a safety case – but may want to see the safety documentation from time to time, including continual review of safety risks.

4.7 Section 7 – Additional Information

4.7.1 In this section, any additional information relevant to the change proposal shall be referenced or included.

4.8 Section 8 – Forwarding the Assessment

4.8.1 Once the Change Evaluation Checklist has been completed, it shall be distributed to the appropriate persons for authorisation. Once authorized, a copy shall be kept with the project documents, and a copy sent to the records management area for filing.

4.9 Preliminary Hazard Analysis (PHA)

Context

4.9.1 Section 4 (see 4.4) of the Safety Reporting Assessment Template involves the determination of the operational safety impact of a change or project. It proposes Preliminary Hazard Analysis (PHA) as an appropriate methodology. A hazard is a source of potential harm or a situation with a potential to cause loss. Hazard identification and analysis is simply the process of determining what can happen, why, and how, and determining the level of risk.

4.9.2 Preliminary Hazard Analysis (PHA) is a hazard identification and frequency analysis technique. It can be useful when analyzing existing systems or prioritizing hazards where circumstances prevent a more extensive technique from being used.

4.9.3 One of the first tasks in PHA is the creation of a Primary Hazard Listing (PHL). This is done to identify the main generic hazards and accident scenarios that shall be associated with the proposed change to the system. PHA shall be applied to all systems, subsystems, components, procedures, and interfaces.

Purpose

4.9.4 The purpose of a PHA is to identify the hazards, hazardous situations and events that can cause harm for a given activity, facility, or system. PHA identifies possibilities for accidents, qualitatively evaluates the extent of injury or damage from these, and identifies possible remedial measures.

Advantages

4.9.5 The PHA identifies areas of the system that will influence safety by evaluating the major hazards associated with the system. These hazards shall be controlled by engineering, administration, or eliminated by design if possible – i.e., by seeking to 'adjust' the change proposal or project specification.

Disadvantages

4.9.6 The PHA is based on data available at the early design stages, therefore only basic or incomplete information shall be available at the time.

Procedure

4.9.7 PHA shall be carried out by means of a Hazard Identification (HAZid) (See Appendix E2) or Hazard Operability Study (HAZOP) (see Appendix E5) or other similar techniques that have been agreed by the project manager. The following are the steps taken in PHA:

- Identify the service or system(s) that are the subject of the change proposal;
- Identify potential failure/s of those services or systems;
- Review existing and proposed risk management controls;
- Examine the effects on the overall system and the human factors effect on staff; and the effect on external stakeholders including aircraft, flight crew, airports etc.

4.10 Using the Completed Change Evaluation Checklist

4.10.1 The information contained in the completed change evaluation checklist is part of the ongoing safety management process for the change or project. In many cases, the information can provide everything needed to complete a Safety Statement if that is the result of the CEC.

4.10.2 In many cases, the information in the CEC can also provide substantial input to the Safety Assessment or Safety Case.

4.10.3 The important thing to note here is that the process of completing the CEC is not a wasted effort – but is a significant contributor to the safety management of any change or project.

CHAPTER 5 ALARP GUIDANCE MATERIAL

5.1 Introduction

5.1.1 Under a Safety Management System, the responsible entity shall establish and maintain processes to identify and manage hazards and risks in their operations and define safety controls for tolerable risks.

5.1.2 Responsible entities shall also develop and maintain safety assurance processes to ensure those safety controls achieve their intended objectives.

5.1.3 There are practicable limits to which a service provider should go to manage risk – these include the availability of cost-effective solutions, and the practicality of implementing those solutions.

5.1.4 In practical terms, risk management activities shall be directed towards realizing potential opportunities whilst managing adverse effects.

5.1.5 International practice accepts that not all risk can be eliminated – and that rather than trying to eliminate all risk, organizations shall strive to balance productivity versus safety by reducing those risks that cannot be accepted to a level that is A**s Low As Reasonably Practicable** – or ALARP.

5.1.6 Deciding that a risk is ALARP can be challenging because it requires accountable managers to exercise their judgment. However, its correct application will assist to demonstrate that it has:

- discharged its duty of care under the law; and
- applied a degree of rigor and consistency in the management of its safety risks.

5.2 What is 'Reasonably Practicable'?

5.2.1 In order to apply the ALARP principle, accountable managers and safety staff need to understand the term 'reasonably practicable', which, in simple terms, describes the "…**effort required to reduce risk…"**.

5.2.2 A definition which is often used to assist people to understand 'reasonably practicable' was set out by the United Kingdom Court of Appeal by Lord Justice Asquith in 1949:

"…Reasonably practicable is a narrower term than 'physically possible' and it seems to me to imply that a computation shall be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time, or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – this risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them. Moreover, this computation falls to be made by the owner at a point of time anterior to the accident…".

5.2.3 When weighing the risk against the 'sacrifice' or effort incurred in reducing it, the decision needs to be weighted, not surprisingly, towards the safety and wellbeing of people using aviation services, and to staff.

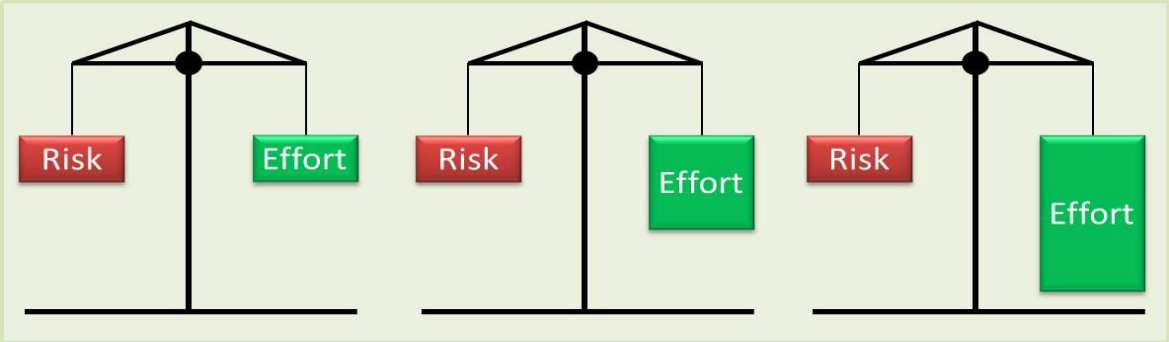

Figure 5.1. Balancing Risk Against Sacrifice or Effort

5.2.4 The presumption is that an organization shall implement risk reduction measures - unless the sacrifice (effort/cost) incurred is too great.

5.2.5 The 'reasonably practicable' assessment has the potential to change over time. New technology can provide opportunities for new controls, costs associated with controls shall decrease and as such something which is rejected today shall be viable in a year, five years, or even in a decade.

5.2.6 For this reason, identified risks and risk controls across the system shall be reviewed on a regular basis to see if there are opportunities to improve risk management.

5.3 Effort Required in Making ALARP Judgments

5.3.1 As mentioned previously determining whether a risk level is ALARP can be challenging because it requires accountable managers to exercise their judgment.

5.3.2 In the majority of cases managers can decide by referring to existing 'good practice' that has been established either by experience, and/or by a process of discussion with stakeholders to reach consensus on what is ALARP.

5.3.3 In high hazard, complex, or new situations, managers shall build on good practice, using more formal decision making techniques, including cost-benefit analysis, to inform judgment.

5.3.4 The more systematic the approach, the more rigorous and more transparent it is. The amount of rigor shall, however, reflect the initial level of risk.

5.3.5 The greater the risk the greater the degree of rigor required to argue or show that those risk levels have been reduced to ALARP.

5.3.6 Paragraphs 5.4 and 5.5 provide an overview of how to determine how complex or detailed your assessment shall be.

5.4 Assessing Benefits and Disadvantages

5.4.1 ALARP judgments are based on the balance which is achieved between the benefits (*the 'upside'*) of any changes and the risks and disadvantages (*the 'downside'*).

5.4.2 The level of resources applied to this process shall be proportionate to the magnitude of the consequence.

5.4.3 At the outset of the decision process, the 'balancing act' between the known benefits and risks and disadvantages can be easily understood if presented in a table like the one below.

	Benefits (on completion)		**Risks and Disadvantages** (during implementation)	**Risks and Disadvantages** (on completion)
Safety		 *Balancing*		
Operational and Other Factors				

Table 5.1: Example Benefit and Risk Table

5.4.4 Qualitative information and data can be used to fill out the table and can assist in determining just how complex your assessment needs to be.

5.4.5 Thinking about a range of operational performance areas will help identify specific items, for example societal, operational, performance based

5.4.6 Examples of benefits include:

a. Reduces workload e.g., controller, pilot, firefighting, maintenance, etc.;
b. Improves resistance to hazards;
c. Improves single failure tolerance;
d. Improves system reliability (= *less maintenance/equipment downtime*);
e. Improves resistance to common cause failures; and
f. Improves system functionality and performance.

5.4.7 Example risks and disadvantages include:

a. Interference with safety systems;
b. Increase in safety risks;
c. Extended timescale to implement;
d. Loss of familiarity for operators;
e. High initial cost;
f. Complexity of engineering solution;
g. Novelty of solution leading to uncertainty;
h. Poor reliability (= *additional maintenance burden and operating costs*);
i. High cost of resources; and
j. Loss of revenue, reputation, and/or function during implementation.

5.4.8 Once an assessment has been made, you shall decide how much weight or importance to give to each benefit/risk and disadvantage.

5.5 Components of the ALARP Process

5.5.0 This section discusses the components and considerations that shall be taken into account when applying the ALARP principle.

5.5.1 Risks

5.5.1.1 When determining which risks to evaluate it shall be remembered that risks shall not only be constrained to operations and facilities, but shall also extend beyond to stakeholders (ANS, airports, airlines, etc.) who might also be affected by a change proposal.

5.5.1.2 In addition, some risks arise from external events or circumstances over which there is no control, but the consequences of which we can mitigate. Such risks shall be included in the ALARP assessment along with the risks over which there is direct control.

5.5.1.3 There is a need to consider all identifiable hazards when carrying out risk assessments, effort shall be concentrated on those hazards that are a reasonably foreseeable source of danger or direct cause of harm. Avoid expending undue effort on the extremely unlikely and 'theoretical' – but do not ignore such risks in your assessment.

5.5.1.4 Risks shall be assessed in an integrated manner. It is important to consider the 'full picture' when assessing risk and not a partial view. Location by location consideration of risks shall however be carried out to determine whether the application of a control measure system-wide would be ruled out on the grounds of excessive costs.

5.5.1.5 Keep in mind that the application of a control measure shall be reasonably practicable in certain locations, such as those that present a particularly high risk and/or low cost.

5.5.2 Sacrifice

5.5.2.1 The sacrifice under consideration here is the cost as a consequence of taking measures to avert or reduce the risks identified. This 'cost' is not necessarily a financial matter – it can be time, money, or effort. We shall also consider the impact on our service provision and societal outcomes, such as the environment.

5.5.2.2 The costs which shall be considered are only those which are necessary and sufficient to implement the measures to reduce risk.

5.5.2.3 For any particular measure, these might include the cost of installation, operation, maintenance, and the costs due to any consequent productivity losses resulting directly, for example from shutdowns, or indirectly from the introduction of the measure (*for example, a new procedure shall cause the system to operate less efficiently initially*).

5.5.2.5 Benefits gained as a result of instituting a safety measure shall be offset against the costs incurred.

5.5.3 Comparison

5.5.3.1 In any assessment as to whether risk levels have been reduced to ALARP, measures to reduce risk can only be ruled out if the sacrifice involved in taking those measures would be 'grossly disproportionate' to the benefits of the risk reduction.

5.5.3.2 This also means that the greater the risk, the more that shall be spent or sacrificed in reducing it.

5.5.3.3 This is of importance when considering a level of risk which is at the upper range of 'Tolerable' as illustrated in Figure 2.1, below. The price of that level of risk in particular circumstances can be identified. Reducing that level of risk will incur costs.

5.5.3.4 In measuring the risk to be reduced and the sacrifice involved to achieve that reduction, the starting point shall be the present assessment of the risk. If there are several options, therefore, they shall each be considered against the present situation.

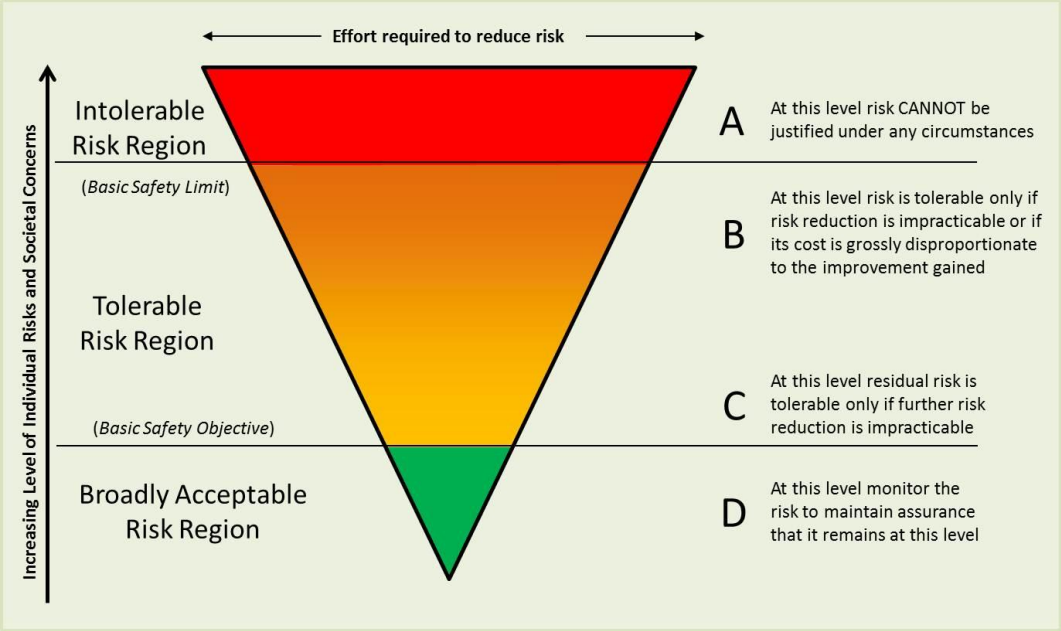

Figure 2.1 Risk Tolerability Diagram

5.5.3.5 In some situations, it will not be possible to assess options in this way. For example, where an installation is being built, it will not be possible to separate the costs of risk reduction measures from the costs of building.

> ***Note:*** *This is important when considering the cost benefit of starting a service, versus the cost-benefit of stopping a service. For example, to put in place a control tower at an airport to manage collision risk, you need to consider the establishment cost (i.e., the cost of building and equipping the tower) – not just the staff costs. To take the service away, the disestablishment costs only factor the savings in terms of staff and maintenance, hence it can be difficult to shut down a service – even if the risks are small.*

5.5.3.6 In such situations, the starting point shall be an option which is known to be reasonably practicable (*such as one which represents existing good practice in determining an assessment of risk*).

5.5.3.7 Any other option(s) shall be considered against that starting point, to determine whether further risk reduction measures are reasonably practicable.

5.5.3.8 Conversely, if risks are viewed as being in the broadly accepted region of risk tolerability, then only those measures which involve minimal sacrifice need to be implemented.

5.5.4 Societal Concerns

5.5.4.1 Societal concerns can arise when the realization of a risk (*i.e., an accident or a serious incident – or the threat of it*) impacts on society as a whole (large numbers of people). The impact shall produce an adverse societal or political response.

5.5.4.2 The harm which results from this is a loss of confidence by society in the provisions and arrangements in place for protecting people and, consequently, a loss of trust in the organization that was managing the risk.

5.5.4.3 These concerns might arise, for example, where:

a. there is an accident in which large numbers of people are killed at one time (*which we call "societal risk"*);
b. potential victims are particularly vulnerable (*such as children*); or
c. the nature of the risks inspire dread and fear (*such as long-term or irreversible effects – Chernobyl is a good example*).

5.5.4.4 The judgment as to whether measures are 'grossly disproportionate' shall reflect or consider societal risk – that is to say, large numbers of people (*employees or the public*) being killed at one time. This is because society has a much greater aversion to an accident killing 10 people than to 10 accidents killing one person each.

5.5.5 Transfer of Risks

5.5.5.1 Introduction of an operational measure to control a hazard shall transfer risk to other parts of the organization. When conducting a risk assessment care shall be given to assessing how the controls might affect other units or how they might interact with controls being implemented for other projects.

5.5.6 Changed Circumstances

5.5.6.1 If there is a need to alter the conditions in which equipment is operated or otherwise alter some or all control measures in response to changed circumstances. This is permissible provided that the altered control measures continue to ensure that risk levels are reduced to ALARP and that the current level of risk is not increased. To do this a new risk assessment is needed.

5.5.7 Good Practice

5.5.7.1 The determination of control measures forms part of the required risk management. Such activities involve:

a. identifying the hazards and determining who might be harmed and how;

b. evaluating the risk from the hazards; and
c. deciding whether the existing control measures are sufficient or whether more shall be done.

5.5.7.2 In reality, there are often only a limited number of options for dealing with a particular safety issue and the best option is in many cases likely to have been already established as relevant good practice and accepted as reducing risk levels to ALARP.

5.5.7.3 Often there will be a need to rely on authoritative documented sources of good practice, such as ICAO regulations and guidance, international best practice, or experience from other organizations in Namibia.

5.5.7.4 A note of caution, however, a universal practice in the industry may not necessarily be good practice or reduce risk levels to ALARP, and it shall not be assumed that it is.

5.5.7.5 Once the assessment is complete, there is a need to continually review and monitor what is good practice, both within Namibia and internationally, as with the passage of time new technology and knowledge shall make higher standards reasonably practicable.

5.5.7.6 Relevant good practice provides companies with generic advice for controlling the risk from a hazard. Whilst relevant good practice or even international best practice can be adopted (*e.g., ICAO guidelines for operational risks*), it shall also take account of individual risk, costs, technical feasibility, and the acceptability of residual risk, even though these will also have been considered (*in general terms*) when the good practice was established.

5.5.8 Choosing Between Options

5.5.8.1 A selection amongst risk reduction options may be needed at any stage of a particular project. At the design stage, there may be a choice between different design concepts for the whole project; as the project is developed, there may be a choice between more detailed options, for example avionics suites, or display parameters.

5.5.8.2 In considering these options safety risk assessment shall be undertaken through the whole project life cycle.

5.5.8.3 Where changes impact Approval Certificates issued under the NAM-CARs, the regulator must be consulted. This shall also have an impact on the operational risk options prior to approval of these changes.

5.5.8.4 In practice, there will be a number of options to reduce risk where an assessment would show that the costs of doing so are not grossly disproportionate to the benefits to be obtained.

5.5.8.5 The option or combination of options which achieves the lowest level of residual risk shall be implemented.

5.5.9 New Versus Existing Equipment

5.5.9.1 Reducing the risk associated with the continued operation of existing equipment to a level that is ALARP shall in some cases result in a level of residual risk which is higher than that which would be achieved by introducing similar new equipment.

5.5.9.2 Factors that could lead to this difference include:

a. the practicability of retrofitting a measure on an existing equipment item;
b. the extra cost of retrofitting measures compared with incorporating them in the new equipment;
c. the risks involved in installation of the retrofitted measure (which shall be weighed against the benefits it provides after installation); and
d. the projected lifetime of the existing equipment.

5.6 Frequently Asked Questions

5.6.1 Does ensuring that risk levels are reduced to ALARP mean that we have to raise standards continually?

The aim of SMS shall be to seek continual improvements in safety achievements. However, given the dynamic nature of aviation operations the level of risk is continually changing over time with activity levels. Any decision about what is ALARP will also be affected by changes in knowledge about the size or nature of the risk presented by a hazard e.g. larger aircraft or increased traffic.

If there is sound evidence to show that a hazard presents significantly greater risks than previously thought, then of course we shall press for stronger controls to tackle the new situation. However, if the evidence shows the hazard presents significantly lesser risks than previously thought, then we shall consider accepting a relaxation in control provided the new arrangements ensure the risks remain ALARP.

5.6.2 Does ensuring that risk levels are reduced to ALARP mean that we shall insist on all possible risk controls?

No. ALARP does not mean that every measure that could possibly be taken to reduce risk shall be taken. Sometimes, there is more than one way of controlling a risk. These controls can be thought of as barriers that prevent the risk being realized and there is a temptation to require more and more of these protective barriers, to reduce the risk to as low as possible. This is not required, as the standard to be met is as low as is reasonably practicable so barriers are only added until a point that the cost no longer justifies the benefit.

5.6.3 Does ensuring that risks are reduced to ALARP mean that there will be no accidents?

No. ALARP does not represent zero risk. We have to expect the risk arising from a hazard to be realized sometimes, and so for harm to occur, even though the risk is ALARP. This is an uncomfortable thought for many people, but it is inescapable. Where there is an operation there is risk.

Of course, we shall strive to make sure that we reduce and maintain risk levels to ALARP, and we shall never be complacent, but, nevertheless, we have to accept that risk from an activity can never be

entirely eliminated unless the activity is stopped. A ship is safe in a harbour, but that is not what ships are meant to do. Measures need to be in place to minimize the level of consequence. Mitigators seek to reduce the probability of a consequence or its severity so that the residual risk is ALARP.

Intentionally left blank

APPENDIX A

CHANGE EVALUATION CHECKLIST TEMPLATE

This is a sample template for the completion of a Change Evaluation. The template includes explanatory notes and examples. There is also guidance material provided for completion of this document in the main text, Chapter 4, of this document.

The template shall be adapted or modified as required depending on the project or the safety management processes implemented

NAMIBIA CIVIL AVIATION AUTHORITY
No 4 Rudolph Hertzog Street, (9pt)
P/Bag 12003, Ausspannplatz,
Windhoek, Namibia
Web: www.ncaa.com.na, email: info@ncaa.na
Phone: +264 83 235 2100

CHANGE EVALUATION CHECKLIST (CEC) – TEMPLATE

Reference Number | |

TITLE OF PROPOSED PROJECT / CHANGE

SUMMARY OF PROPOSED CHANGE

RESULT OF CHANGE EVAUATION

This Change Evaluation has determined a requirement for a (*tick the requirement*):

Safety Case ☐ **Safety Assessment** ☐ **Safety Report** ☐

AUTHORISATION

By signing this Change Evaluation Checklist you acknowledge that:

- You are satisfied that the Change Evaluation process has been completed correctly;
- Appropriately experienced and/or qualified staff participated in the process; and
- Sufficient information has been included to justify the outcome.

Name and Position	Signature	Date
Prepared by: *Name/Position of the person who conducted this assessment.*		
Proposed by: *Name/Position of the person responsible for the safe implementation of the change*		
Agreed by: *Name(s)/Position(s) of applicable system and/or service authority(ies). Where multiple systems or services are affected, agreement from each is required*		
Approved by: *Name(s)/Position(s) of Manager(s) with safety accountability for the change.*		

SECTION 1: DETAILS OF THE PROPOSED CHANGE

1.1 Description of the Proposed Change:

(Write a description of the change and how it will affect the overall ATM system)

SECTION 2: WILL CIVIL AVIATION REGULATIONS BE AFFECTED?

If you are not sure about any of these questions, contact your Safety and Quality Assurance unit, or contact ANSSO.

2.1 Does the proposed change involve changes to service levels, procedures, or equipment, which will affect the performance, functional, or technical specification of an system or service – or involve organisational changes affecting safety accountabilities?

YES		If **YES** continue with the Change Evaluation Checklist. • Continue to Question 2.2
NO		If **NO** a CEC is **not required** – use normal change management processes.

2.2 Does the proposed change require an amendment to an approval issued under the NAM-CARs (*including any restrictions or requirements of a certificate*)?

NOTE: This includes changes to procedures or services (e.g., a new ICAO defined service or a new type of airways system, or the removal of an ICAO defined service or a type of airways system.)

YES		If **YES** a Safety Case **will be** required. • Notify ANSSO. • Continue to Section 3.
NO		If **NO** continue to Question 2.3

Note: Even if the answer is YES, continue to answer all questions as it shall assist with the Safety Case later.

2.3 If 2.2 doesn't apply, will the change still need approval?

For Example, amendment of a manual, incorporation of new equipment, requiring regulator approval

YES		If **YES** a Safety Case **shall** be required. • Contact the regulator to discuss safety reporting requirements • Continue to Question 2.4
NO		If **NO** continue to Question 2.4

Note: Even if the answer is YES, continue to answer all questions as it shall assist with the Safety Case later.

2.4 Does the proposed change require notification to the regulator prior to commissioning or notification to industry?

For Example: where a facility noticeable to the user (DME, VOR, ILS, etc.,) is being decommissioned, or where there shall be a significant reduction to the level of service for a period of time

YES		If **YES** a Safety Assessment is required. • Notify ANSSO • Continue to Section 3
NO		If **NO** continue to Section 3

SECTION 3: SIZE OF CHANGE

Complete the following questions to determine the size of the change. For each question, choose a rating from 1 (Low) to 7 (High); and provide justification (*i.e., why did you choose this number*). *(The diagram on the next page shall help to answer the size of change questions.)*

1	**How significant is the change inside the operation?** *Consider all of the work areas that shall be affected. Consider the effects on facilities and engineering support, maintenance, various ATC areas (Tower, Approach, En-route, different locations), operational context, and rescue fire fighting if applicable.*	**Rating 1-7** *1=Low 7=High*
Justification:		

2	**How significant is the change outside the operation?** *Consider the number of service users and/or stakeholders affected, including the interfaces between these parties.*	**Rating 1-7** *1=Low 7=High*
Justification:		

3	**Has a level of functionality been introduced, altered, or removed by the proposed change?** *E.g., Does the change enhance existing functionality; provide different functionality; remove functionality; reduce the level of service; affect the operator's role?*	**Rating1-7** *1=Low 7=High*
Justification:		

4	**Does the proposed change have a technical impact on the operating system(s)?** *E.g., Does the change affect single or multiple systems; affect operational or non-operational systems; introduce new hardware or software affecting operational capability; affect system interfaces; affect redundancy, maintainability, integrity, etc; affect operational data and/or databases?*	**Rating 1-7** *1=Low 7=High*
Justification:		

5	**How big is the training component associated with the change?** *Consider type of training required, classroom or simulation, time lines, resources, recency requirements, etc.*	**Rating 1-7** *1=Low 7=High*
Justification:		

6	**How complex is the transition from the existing system?** *Consider resources available, training, documentation, procedures, communication, time lines, approvals etc.*	**Rating 1-7** *1=Low 7=High*
Justification:		

Total Score =	
Resultant Size of This Change = Small = 6-18 Medium = 19-30 Large = 31-42	

1. Assess the Significance of the Change inside ANS Consider the work areas affected. Consider the effects on facilities and maintenance, ATC units and workstations, and other ANS infrastructure

1 → 7

Change is expected to affect only a single unit or location	**Change is expected to affect all operational groups incl. personnel, procedures, systems and services**

2. Assess the Significance of the Change outside ANS

Consider the number of users and stakeholders affected, including the interfaces between these parties

1 → 7

Change is expected to be completely transparent to all stakeholders	**Change is expected to affect the way in which all stakeholders interact with ANS services.**

3. Assess the Level of Functionality Introduced, Altered or Removed. Does the change enhance existing functionality; provide different functionality, remove functionality; reduce the level of service; affect the operator's role; etc

1 → 7

Change is expected to be completely transparent to system or service operators	**Change is expected to deliver significant changes to the way operators interact with the system and services provided.**

4. Assess the Technical Impact on Operating Systems Does the change affect single or multiple users, introduce new hardware or software, affect system interfaces, affect redundancy, maintainability, affect operational data/databases etc

1 → 7

Change is not expected to have a technical impact on any operating systems	**Change is expected to affect a significant number of operational and non-operational systems**

5. How Substantial is the Training?

Consider the type of training required, classroom or simulation, timelines, resources, recency requirements etc

1 → 7

Change is not expected to require any new training or changes to existing training	**Change is expected to require major training across the country and upgrade to a large amount of existing training material**

6. How Complex is the Transition?

Consider resources available, training, documentation, procedures, communication, timelines, approval, etc

1 → 7

Change is not expected to affect service delivery and will not require resources or training, Can be done as part of 'normal business'	**Change will significantly affect service delivery over a large part of the network, Substantial planning and high level approval will be required**

Size of Change Guidance Example ANS

SECTION 4: OPERATIONAL SAFETY IMPACT

To assess the operational safety impact of the change, conduct a preliminary hazard analysis to determine the likely operational safety hazards that shall result from the change and complete the table below. After considering the number and severity of the likely hazards, estimate the Operational Safety Impact as **Minimal**, **Reasonable** or **Substantial** and enter this below.

Note: This analysis shall only be used for the determination of the Operational Safety Impact. All Hazards identified through this analysis that require control and ongoing management, or further assessment through a hazard identification process, shall be recorded in the change's risk database (e.g. HAZLOG) and processed according to the risk management techniques detailed in Chapter 2.

Service or System	Potential Failures	Risk Controls		Effect on	
		Existing	Proposed	Air Traffic Services	Aircraft/Aircrew

Based on the above, what is the estimated Operational Safety Impact of the proposed change? (Minimal, Reasonable or Substantial)	

List the persons that completed this analysis for both Sections 3 and 4:

Name	Position	Date

SECTION 5: OVERALL OPERATIONAL SAFETY MAGNITUDE

The Overall Operational Safety Magnitude is determined by combining the **Size of the Change** and the **Operational Safety Impact** of the change. The results obtained from Sections 3 and 4 are applied to the matrix below to determine the **Overall Operational Safety Magnitude**.

Size of the Change	Operational Safety Impact		
	Substantial	**Reasonable**	**Minimal**
Large	**MAJOR**	**MAJOR**	**MODERATE**
Medium	**MAJOR**	**MODERATE**	**MINOR**
Small	**MODERATE**	**MINOR**	**MINOR**

SECTION 6: OPERATIONAL SAFETY REPORTING REQUIREMENT

Take the results from Section 2 or Section 5 and use the matrix below to determine the Operational Safety Reporting Requirements.

Note that a Section 2 requirement for a Safety Case or Safety Assessment overrides any lesser outcome from Section 5. (e.g., if Section 5 says Safety Statement but Section 2 says Safety Case, a Safety Case is required)

Question	If outcome is:	To be reported as a:	Required Actions
2.1	YES	**SAFETY CASE**	1. Prepare a Safety Plan 2. Conduct Safety Assessment activities 3. Prepare a Safety Case 4. Forward to ANSSO and also your SQA unit
2.2	YES	• Contact ANSSO for reporting requirements	
2.3	YES	**SAFETY ASSESSMENT**	1. Prepare a Safety Plan 2. Conduct Safety Assessment activities 3. Prepare a Safety Assessment 4. Forward to ANSSO and also your SQA unit
5	MAJOR	**SAFETY ASSESSMENT**	1. Prepare a Safety Plan 2. Conduct Safety Assessment activities 3. Prepare a Safety Assessment 4. Forward to your safety section
	MODERATE		
	MINOR	**SAFETY STATEMENT**	1. Prepare a Safety Statement. *Note: the safety information in sections 3 and 4 of this document shall be used to satisfy the requirement for a Safety Statement*

Note that the ANSSO shall require or impose a higher safety reporting requirement.

SECTION 7: ADDITIONAL INFORMATION

If necessary, list any related documents or additional relevant information.

SECTION 8: FORWARD THIS CHANGE EVALUATION DOCUMENT

A copy of the signed and approved Change Evaluation Checklist (CEC) shall be sent to the responsible department of the operator/service provider and regulator.

APPENDIX B

SAFETY PLAN TEMPLATE

This is a sample template for the completion of a Safety Plan. The template includes explanatory notes. The template is consistent with the guidance provided in the main text of this document.

The template shall be adapted or modified as required depending on the project, or the safety management processes implemented .

<Insert Logo>

<insert project name>
<Insert Section>

Safety Plan

Name and Position	Signature	Date
Prepared by: *<name>* **Position:** *<insert position title>*		
Proposed by: <name> **Position:** *<insert position title>*		
Agreed by: <name> **Position:** *<insert position title>*		
Agreed by: <name> **Position:** *<insert position title>*		
Agreed by: <name> **Position:** *<insert position title>*		
Agreed by: <name> **Position:** *<insert position title>*		
Approved by: <name> **Position:** *<insert position title>*		

i. Document Control Information

Document Owner	*<insert project management area>*
File Reference	*<insert year>/<insert number>*
Electronic Master Storage	*<insert reference>*
Hard Copy Master Storage	*<insert reference>*
Document Register Number	*<insert number>*

ii. Amendment Record

Issue Number	Section(s) Amended	Amended by	Date
0.1	Initial Draft		<insert date>

iii. Table of Contents

1. Background

In this section provide basic background material – what the project is, why the project has been created, what the project links to, etc. Most of this material will be available from associated strategy documents or regional plans, etc.

1.1

2. Purpose

In this section outline the purpose of this document. Identify the key purpose of the Safety Plan – i.e., why have you created the Safety Plan. The following is an example that shall satisfy the requirement:

2.1 NAM-CAR Part 140 (Safety Management Systems) and the associated Document NAM-CATS-SMS-140 requires a service provider to develop and maintain a formal process for the management of change that will:

a. identify changes within the service provider's organization and organizational environment, which shall affect established processes and services;

b. describe the arrangements to ensure safety performance before implementing changes; and

c. eliminate or modify safety risk controls that are no longer needed due to changes in the operational environment.

2.2 The identification of changes as per 2.1(a) above, and the description of the arrangements to ensure safety performance before implementing changes as per 2.1(b) above is generally accomplished through the development of a **Safety Plan**.

2.3 This document constitutes the **Safety Plan** for design and implementation of changes associated with the *<insert name of project>.*

2.4 The identification and treatment of risk and management of risk controls as per 2.1(c) above will be accomplished through the development of a **Safety Assessment**, or a **Safety Case** if considered necessary after the Safety Assessment.

2.5 <*add text relevant to this project*>

3. Scope of the Change

In this section clearly identify the main changes that are proposed under your project and how they will impact the rest of the system or operation. Where a particular change has not been finalised, or will be finalised based on the development of the project, be sure to indicate this in the Safety Plan.

4. Assumptions, Constraints and Dependencies

4.1 Assumptions

In this section identify the main assumptions that will affect your project – specifically those assumptions that are critical to the success or timing of your project.

4.2 Constraints

In this section identify key constraints – those circumstances that will affect your project significantly if they are not addressed.

4.3 Dependencies

In this section identify the key dependencies. These shall appear to be similar to constraints or assumptions – but often are factors outside the scope of this particular project. As an example, your project shall be dependent on another project delivering a capability by a certain date. If it is not delivered by that date it shall become a constraint.

5. Responsibilities

In this section you shall clearly identify who has a responsibility in relation to your project – either to do a task, or to approve a task or action or project outcome. It shall not be possible to identify all responsibility areas in the initial version – it shall be updated as the project progresses. This section shall be presented as a table or matrix.

6. Consultation and Communication

In this section you shall identify how you intend to communicate throughout the project (e.g., meetings, workshops, phone, e-mail etc.) and who will be involved in those meetings – i.e., who are the stakeholders and how will you engage with them.

7. Safety Management Activities

This is a critical section. Here you shall identify as many of the safety management activities that you can in relation to your project. You need to make statements about how you intend to identify safety issues, and how you intend to manage those safety issues. Identify hazards and apply risks management and mitigation strategies. Identify the safety challenges associated with your project. If you already have an idea about how you intend to address a particular safety challenge, you can include some commentary on that, as it shall reassure readers that you have been considering solutions as well as the problem – or that you have a particular direction in mind.

8. Timelines and Milestones

Here you shall include a project plan or timeline showing the key activities and inter-dependencies. If you are using the Safety Plan as your Project Plan, the timelines will need to be more detailed. You shall identify the key safety dependencies and when they are to be completed.

<*insert project timeline diagram*>

9. Resources

In this section you shall identify the resources that will be assigned to safety assurance activities associated with your project. These will generally be the same as those assigned to your project activities – but in some cases you shall engage specialist safety personnel on certain activities. It shall be clear, however, that you have not split safety away from the core project activity – the two are interlinked.

10. Training and Education

Here you shall identify the training and education activities that will be undertaken in the project and which will be used to address safety concerns. Where a Training Needs Analysis is required, you shall identify who will do this, and when (unless it has already been completed). Where the project will affect external stakeholders (airlines, airports, etc.) you shall also include a description of how you will create training and education material for them – or how they will train and educate their personnel.

11. Review

In this section you shall state how you intend to review safety activities – and who will be responsible for signing-off those review processes. You shall also identify how you intend to review the Safety Plan. Also include a statement about post-implementation review (PIR) of your project, and actions you shall take to address any PIR issues.

12. Approvals

This section relates to regulatory or other approval processes that will need to be addressed in your project. You shall also consider regulatory or other approvals for all stakeholders (e.g., airworthiness approvals for aircraft, Operations Manual approval for airline operators, etc.).

13. Related Documents

In this section identify as many of the documents as possible that you will refer to during the project. This shall include various ICAO SARPS or procedures documents and manuals, ISO standards, technical manuals, etc.

APPENDIX C

SAFETY ASSESSMENT / SAFETY CASE TEMPLATE

This is a sample template for the completion of a Safety Assessment (or Safety Case where required). The template includes explanatory notes. The template is consistent with the guidance provided in the main text of this document.

The template shall be adapted or modified as required depending on the project, or the safety management processes implemented.

SAFETY ASSESSMENT / SAFEY CASE - TEMPLATE

(Delete the non-applicable term)

Reference Number

TITLE OF PROPOSED PROJECT / CHANGE

SUMMARY OF PROPOSED CHANGE

AUTHORISATION

NOTE:- By signing this Safety Assessment or Safety Case document you acknowledge that:

- You are satisfied that the document has been completed correctly;
- Appropriately experienced and/or qualified staff participated in the process; and
- Sufficient information has been included to justify the outcome.

Name and Position	Signature	Date
Prepared by: *Name/Position of the person who conducted this assessment.*		
Proposed by: *Name/Position of the person responsible for the safe implementation of the change/project*		
Agreed by: *Name(s)/Position(s) of applicable system and/or service authority(ies). Where multiple systems or services are affected, agreement from each is required*		
Approved by: *Name(s)/Position(s) of Manager(s) with safety accountability (see note below).*		
Endorsed by: *(Accountable Executive/ S&Q Manager only if a Safety Case has been prepared)*		

***Note**: Where changes have national implications and affect operations under the NAM-CAR Part 172, the manager(s) with the safety accountability for the service delivery is the approval authority. For other changes, the manager(s) who has the safety accountability for the change is the approval authority.*

STEP 1. BACKGROUND

In this Step discuss why has the change come about? Describe the reasons for undertaking this project. Include reference to the relevant change request and/or Safety Reporting Assessment document where applicable.

STEP 2. PURPOSE OF THIS DOCUMENT

In the Step describe the purpose of this document and what it is expected to achieve.

STEP 3. SCOPE OF THE PROPOSED CHANGE

In this step describe what the project is going to change? Describe the present system and the change(s) proposed for that system. Consider the effect on: service provision(s) under the NAM-CARS Operating Certificates and/or non-regulated Service Delivery Units, and supporting Systems, Facilities and Equipment (including data and networks) – and consider design, operations and maintenance; and people and associated procedures.

STEP 4. ASSUMPTIONS, CONSTRAINTS AND DEPENDENCIES

In this Step write down what you thought or stated 'up front' that influenced the safety outcome of the change? Detail any additional assumptions, constraints and dependencies not included in the Safety Plan. Validate all the assumptions, constraints and dependencies affecting the safe outcome of the change.

4.1 ASSUMPTIONS

In this sub-step describe any assumptions made which affected the project scope, strategies or outcomes.

4.2 CONSTRAINTS

In this sub-step describe any constraints which restricted the ability of the project to achieve a safe outcome.

4.3 DEPENDENCIES

In this sub-step describe any dependencies on other projects or activities which impacted the outcome of this project or where other projects or activities are dependent on the outcome of this project.

STEP 5. RESPONSIBILITIES

In this Step write down the names and responsibilities of the 'key players' in this change. Describe the people who have been committed to the project and their primary roles and responsibilities – i.e., what will they do?

STEP 6. CONSULTATION AND COMMUNICATION

In this Step describe who you consulted and communicated with. Describe the consultation and communication arrangements that were undertaken by the project team throughout the project phases. This includes both internal and external stakeholders.

STEP 7. DESIGN PROCESS

7.1 DESIGN INTEGRITY

In this Step ask "how did I develop a good design"? Describe the process used to develop the design solution. This section shall provide information on the standards and design methods employed for error avoidance, detection and elimination during the development of the design and present arguments as to why these are appropriate. Assurance of the design shall come from, for example, design maturity - proven reliability and integrity; experience of similar systems; proven system architectures; or design calculations - reliability and integrity. In some cases, design development shall not be completed until the system has been operated and evaluated in its intended environment. Any work affecting safety assurance of the design that still needs to be done shall be highlighted.

7.2 FUNCTIONAL AND PERFORMANCE REQUIREMENTS

In this Step specify the "underived" or "given" functional and performance requirement – i.e., the requirements pre-specified for the change or project. Include targets for accuracy/resolution, audibility, definition, response times, ergonomics, availability, procedures, alerts and ANS procedures and training requirements where these affect the safety of the System. Describe how these will be confirmed before implementing the change.

7.3 DESIGN CONFIRMATION

In this Step ask "how have I confirmed that I have developed a good design"? Provide evidence (such as test results) that the design meets the intended requirement and fulfills the safety objectives and that the functional and performance requirements have been achieved.

7.4 DESIGN PROCEDURES AND STANDARDS

In this Step ask "what procedures/standards were applied or met"? Describe any specific procedures or standards that were used in achieving a safe outcome. Where other parts of ANS, or other organization, are required to develop or amend standards, confirm the development or amendment of the standards.

7.5 DESIGN LIMITATIONS AND SHORTCOMINGS

In this Step we need to find out if the system will do everything it was intended to do. If not, does its use need to be limited in some way? State any limitations on the use or maintenance of the system or shortcomings identified in the design. Reliance on other systems and procedures shall be explained. Any unresolved system shortcomings which could result in a hazard shall be declared. Temporary design fixes and short term procedures or workarounds shall be declared.

7.6 DESIGN AUTHORITIES

In this Step we say who is responsible for the design integrity. Identify the design authorities for the airspace, procedures and systems as appropriate. All Design Authorities associated with the safety case shall be identified.

7.7 DESIGN SAFETY MANAGEMENT ACTIVITIES

In this Step we ask "how did I go about achieving a safe outcome"? What did I do to manage safety, identify hazards and controls, assess the risks and gather safety related information? Describe the safety management activities for the design phase of the project – e.g., hazard and risk identification processes; structured brainstorming workshops; etc. Provide information on:

- *how the hazards were identified for the design phase of the project;*
- *who was involved in the hazard identification and what was their relevant experience; including relevant Subject Matter Experts (SME) from the operational and technical areas and representatives of all relevant stakeholder groups (e.g. Defense, Airlines, pilots, external providers);*
- *what process were used to identify the hazard(s);*
- *why this process was selected;*
- *what risk assessment criteria were used;*
- *who did the risk estimations;*
- *who determined the risk controls; and*
- *timelines and milestones.*

Describe the process used for capturing hazards that were identified outside the formal means above, i.e. those hazards that were identified on an ad-hoc basis. Who were they sent to? How were they captured and processed?

7.8 DESIGN HAZARDS, CONTROLS, AND SAFETY REQUIREMENTS

In this Step we ask "what are the outcomes of the design hazard identification activities"? Detail the Hazards, Controls and Safety Requirements determined from the hazard identification activities, including their status. Controls and Safety Requirements shall be expressed so that their achievement can be measured. The proponent of change shall choose to use the HAZARD IDENTIFICATION Template and associated Hazard Log.

Important: Attach the Hazard Identification Documents

7.9 DESIGN RISK MANAGEMENT

In this Step we describe the process for managing the identified hazards. Include those that could not be managed locally or which required sign-off by senior management. Describe the process for reviewing the hazards, who was responsible for this activity and when this occurred. Where Controls or Safety Requirements are "not met" or "yet to be met":

- *provide a provisional argument regarding the safety of moving to operation;*
- *specify the monitoring arrangements; and*
- *validate residual risk estimations.*

State any other tools that were used for safety assurance purposes and how they were used.

STEP 8. CONCLUSION

A Safety Assessment or a Safety Case shall contain both the evidence and ARGUMENT that a concept/design change is adequately safe "in principle" Use the evidence gathered during the safety assessment process to make the ARGUMENT that this concept/design change is adequately safe "in principle".

STEP 9. DOCUMENT REVIEW

9.1 Service Delivery Line/Business Branch or Unit/Safety Services

Is this document compliant with ANSSO Procedures? Has the process been followed? Is the content valid? Provide a summary statement that there was a local/peer review and the review comments have been considered and acted on where appropriate in the safety document. Review feedback shall be available on an ANS file; the reference shall be provided.

9.2 Service Integrity

***Required for Safety Cases Only**: Is the document compliant with ANSSO Procedures? Does the argument address the identified risks? Is it compliant with relevant standards and regulations? If a Service Integrity review has taken place, provide a summary statement that the review comments have been considered and acted on where appropriate in the Safety Case. Review feedback shall be available on an ANS file; reference shall be provided.*

STEP 10. APPENDICES

Include any appendices referred to in the text.

STEP 11. RELATED DOCUMENTS

List any related documents (e.g. Safety Plan) and provide internal links where appropriate.

APPENDIX D

HAZARD IDENTIFICATION AND SUMMARY TEMPLATE

HAZARD IDENTIFICATION (HazID) TEMPLATE - <project title>

HAZARD REFERENCE	Hazard No. :	
HAZARD		
DESCRIPTION		
AREA(S) AFFECTED		
RISK CLASSIFICATION – PRE-MITIGATION	**Likelihood**	
	Severity	
	Risk Assessment	This risk is classified as:

MITIGATION	The strategies employed to mitigate against this risk are:	
Strategy	**Effect of Mitigation**	**Effect on Risk**

RISK CLASSIFICATION – POST-MITIGATION	**Likelihood**	
	Severity	
	Risk Assessment	This risk is classified as:

Guidance Material – Assessment of Risk

LIKELIHOOD OR PROBABILITY CRITERIA			
Category	**Description**	**Examples of what to look out for**	**Examples of frequency**
1	**Extremely improbable (Rare)**	Almost inconceivable that the event will occur.	e.g., 1 in > 50 years
2	**Improbable (Seldom)**	Very unlikely that the event will occur. It is not known that it has ever occurred before.	e.g., 1 in 20 – 50 years
3	**Remote (Unlikely)**	Unlikely but could possibly occur. Has occurred rarely.	e.g., 1 in 5-20 years
4	**Occasional**	Likely to occur sometimes. Has occurred infrequently.	e.g., 1 in 1-5 years
5	**Frequent**	Likely to occur many times/regularly. Has occurred frequently/regularly.	e.g., daily, weekly

			Extremely Improbable (1)	Improbable (2)	Remote (3)	Occasional(4)	Frequent(5)
L	no mitigation needed	Cantastrophic (5)	6	7	8	9	10
M1	mitigation required should be treated as important - eg time frame 90 days	Hazardous (4)	5	6	7	8	9
M2	mitigation required should be treated as urgent - eg time frame 30 to 90 days	Major (3)	4	5	6	7	8
M3	mitigation required should be treated as critical - eg time frame less than 30 days	Minor (2)	3	4	5	6	7
H	activity must be stopped or immediate action required	Negligible (1)	2	3	4	5	6

Table 2.4: Likelihood versus Severity Risk Matrix

Risk Level	Risk Assessment Index (from Table 4)	Suggested Criteria
A	8-10	At this level risk CANNOT be justified under any circumstances.
B	6-7	At this level risk is tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained.
C	5	At this level residual risk is tolerable only if further risk reduction is impracticable.
D	2-4	At this level monitor the risk to maintain assurance that it remains at this level.

SEVERITY CRITERIA

(See next page for further guidance on severity classification)

Risk Severity definition		***Consequence (i.e., can lead to….)***	***Examples of what to look out for…***	***Examples of Effect on Aircrew or Passengers***	***Examples of Effect on ANS***
Category	***Code***				
Catastrophic	**5**	One or multiple deaths & complete loss / destruction of equipment	• A major accident.	• Multiple fatalities due to collision with other aircraft, obstacles or terrain	• Sustained inability to provide any service
Hazardous	**4**	Serious injuries/Major Damage to equipment	• Large reduction in safety margins, physical distress or workload such that the operators cannot be relied upon to perform their tasks accurately or completely.	• Large reduction in safety margin • Serious or fatal injury to small number • Serious physical distress to air crew	• Inability to provide any degree of service (including contingency measures) within one or more airspace sectors for a significant time
Major	**3**	Minor injuries/ Minor equipment damage	• A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of increase in workload, or as a result of conditions impairing their efficiency.	• Significant reduction in safety margin • Major illness or injury • Physical distress to occupants	• The ability to provide a service is severely compromised within one or more airspace sectors without warning for a significant time
Minor	**2**	Incidents	• Operating limitations are breached. • Procedures are not used correctly.	• Slight reduction in safety margin • Minor illness • Some physical discomfort to occupants	• The ability to provide a service is impaired within one or more airspace sectors without warning for a significant time
Negligible	**1**	Negligible outcome or Inconvenience	• Few consequences. • No safety consequences. • Nuisance.	• Potential for some inconvenience.	• No effect on the ability to provide a service in the short term, but the situation needs to be monitored and reviewed for the need to apply some form of contingency measures if the condition prevails

HAZARD LOG SUMMARY - *<project name>*

Enter the hazards from the previous Hazard Identification templates and attach this summary sheet to the Safety Plan and Safety Assessment/Safety Case.
This hazards and mitigations in this Hazard Log shall also be transferred to the ANS Master Hazard Log (when established).

HZD No.	Hazard	Effect	Risk	SR No.	Safety Requirement (SR)	Control Responsibility	Residual Risk
1							
2							
3							
4							
5							

APPENDIX E

RISK MANAGEMENT TOOLS AND TECHNIQUES

RISK MANAGEMENT TOOLS AND TECHNIQUES

E.0 Introduction

0.1 Risk management decisions can only reflect the quality of the risk identification and assessment process. Consequently the selection of a technique for risk identification shall be based on:

- its appropriateness to the topic;
- the system or change proposal focus – procedures, human element, hardware and equipment, software, organization, and the operating environment;
- the system lifecycle stage – e.g., planned new system, implement new system, change to existing, etc.; and
- the resources required in terms of data (*input*) and expertise.

0.2 The purpose of this document is to provide basic guidance and assistance to safety management staff about the different techniques that can be used in support of risk management procedures.

0.3 This appendix cannot and does not provide all the information for each technique; however it does present background information, the advantages and disadvantages of the technique and advice about where to find further information.

0.4 It has been developed to assist managers and other staff - including project managers, project participants, specialists in risk management, and those delegated with risk management responsibilities by their line managers.

0.5 The table below provides an overview of the safety analysis techniques covered in this document. The following chapters then provide expanded but general information about the techniques.

0.6 More detailed information about the application of the various techniques can be found in the joint FAA and Eurocontrol document: *ATM Safety Techniques and Toolbox (Safety Action Plan 15) Issue 2.0 October 3rd, 2007*.

SUMMARY OF RISK ASSESSMENT TOOLS AND TECHNIQUES							
	Tool or Technique	**Short Description**	**Function**	**Lifecycle Stage**	**System Focus**	**Input Requirements**	**Expertise Requirements**
1	**Bow Tie presentation**	Illustrates the relationship between hazardous events, their causes and consequences and the way that the event is controlled	Combine hazards into a risk framework which guides risk mitigation and control	Late concept / design stage onwards	All aspects represented in the Bow Tie diagram	Identified hazard, causes and outcomes	Safety or risk assessment expertise
2	**HAZid**	The purpose of the HAZid technique is to identify hazards based on the interaction of various jobs, tasks and activities in a real field setting	Hazard identification	Concept / design stage	All system aspects	Group of experts, system description and operational concept	Safety or risk assessment expertise
3	**Preliminary Hazard Analysis (PHA)**	A hazard identification technique that identifies hazards, hazardous situations of an activity, facility or system	Hazard identification	Concept stage	Hardware	Hardware knowledge	Safety analysis expertise, domain knowledge
4	**Failure Mode Effects Analysis (FMEA/ FMECA)**	A fundamental hazard identification and frequency analysis technique which analyses all the likely failures associated with the change and the likely impact on safety as a result of one of these failures occurring anywhere in a system	Hazard identification (using Preliminary Hazard Listing)	Late concept / design stage onwards	Hardware	Requires complete and accurate modeling of the system under consideration, along with detailed knowledge of the operation of the system and any associated systems	Safety and risk analysis expertise, domain knowledge.
5	**Hazard and Operability (HAZOP)**	A systematic qualitative technique for identifying hazards and operability problems throughout a facility	Hazard identification, risk evaluation and risk mitigation/ control	Concept stage onwards	Usually all except software (unless specialized for this purpose)	Group of experts, system description and operational concept	Risk analysis (HAZOP) expertise and domain knowledge

		or system through brainstorming					
6	**Goal Structuring Notation (GSN)**	A graphical notation that is used to plan and describe the structure and relationships of a Safety Argument	To provide the structured breakdown of the logical argument from the top Goal, through Strategies and further decomposed Goals down to Evidence items and the activities necessary to provide this evidence. In addition provides linkages to the necessary Assumptions / Justifications and Context	Concept stage onwards	All system aspects	- Domain knowledge - Operational concept	- Domain knowledge - Safety and risk analysis expertise
7	**Hierarchical Task Analyses (HTA)**	A goal orientated technique which can be utilized to perform human error identification and/or human reliability quantification	Learning about human tasks at the beginning of a safety analysis	Late concept / design stage and onwards	Human (individual and team)	Domain knowledge, operational concept, simulations, access to experts on how the system will be operated	Human factors expertise
8	**Human Error Assessment and Reduction Technique (HEART)**	HEART is a human reliability assessment tool that is commonly used to quantitatively assess human reliability through an estimation of the human error probability	Risk evaluation	Late concept / design stage and onwards	Human (individual or team)	Task analysis and appreciation of possible error forcing conditions	Human reliability assessment expertise
9	**Human Reliability Analysis (HRA)**	A frequency analysis technique which deals with the impact of people on system performance and evaluated the influence of human errors on reliability	Risk evaluation	Late concept / design stage and onwards	Human (individual and team)	Human error data collected from actual events or simulations; or formal expert judgment sessions	Reliability assessment expertise; domain knowledge
10	**Structured What If Technique (SWIFT)**	Systematic technique used to identify hazards (including time-critical applications)	Hazard identification	Concept / design s stage and onwards	Hardware	Hardware knowledge	Safety and risk analysis expertise, domain knowledge

11	**Event Tree Analysis (ETA)**	Determination of possible outcomes leading from an event or hazard	Hazard identification, risk evaluation	Late concept / design stage	All system aspects	Scenarios and system knowledge, event analysis	Safety/risk analysis expertise, domain knowledge
12	**Fault Tree Analysis (FTA)**	Determining the possible causes of a hazard, whether single or multiple, related or unrelated	Hazard identification, risk evaluation	Late concept / design stage	All system aspects	Detailed system knowledge, event analysis	Safety/risk analysis expertise, domain knowledge
13	**Root Cause Analysis (RCA)**	Determines the underlying contributing reasons for observed deficiencies documented in the findings of an investigation	Hazard identification	Concept / design stage and onwards	All system aspects	Operational concept, design information, system definition, inter-relationships (can use case scenarios)	Safety /risk analysis expertise
14	**Sensitive Analysis (SA)**	Determines the relationship between the uncertainty in the independent variables used in an analysis and the uncertainty in the resultant dependent variable	Risk evaluation	Late concept / design stage and onwards	All system aspects	Detailed system knowledge	Mathematical and statistical expert

Table D1: Summary of Risk Assessment Techniques

E1. BOW TIE TECHNIQUE

1.1 Context

1.1.1 Bow Tie technique has both proactive and reactive elements that systematically work through a hazard and its management.

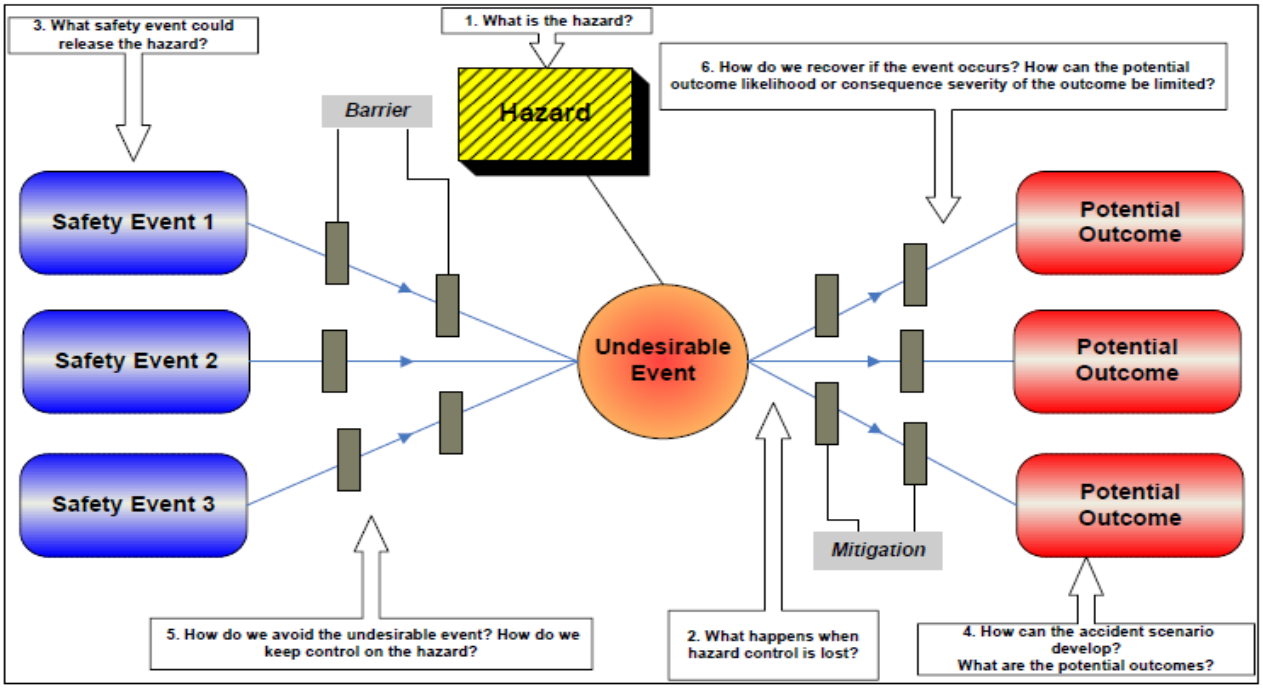

Fig 1: Bow Tie Format (Source: CANSO)

1.1.2 In representation, the knot in the Bow Tie represents a hazard and a top event as a pair. The hazard describes the potential source of harm and the top event describes how that source of harm is released. The left-hand side includes contributors leading to threats that can cause the hazard and barriers incorporated to control a hazard. The right hand side includes consequences of the hazard and the recovery measures to mitigate the consequence of the hazard.

Note: *A top event is a point in time which describes the loss of control of the hazard i.e. the loss of control point.*

1.2 Purpose

1.2.1 The aim of Bow Tie technique is to illustrate the relationship between hazardous events, their causes and consequences and the way that the top event is controlled.

1.2.2 The Bow Tie diagram gives the safety specialist a chance to use operational experts to develop ideas to improve safety.

1.3 Advantages

1.3.1 A Bow Tie diagram provides good awareness, education, and communication.

1.4 Disadvantages

1.4.1 It may be difficult to identify common causes of failures or links between barriers.

1.5 Further reading

- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E2. HAZARD IDENTIFICATION (HAZid)

2.1 Context

2.1.1 HAZid is a workshop-based technique that is followed in two stages; the first step is freeform brainstorming of hazards asking questions such as "What can go wrong?" and "What if...?" Once a list of hazards has been generated the second step is to cross check (*using a checklist*) to make sure that all relevant issues have been considered. The checklist shall not be used directly to generate the list of hazards.

2.2 Purpose

2.2.1 The purpose of HAZid technique is to generate hazards based on the interaction of various jobs, tasks, and activities in a real field setting.

2.3 Advantages

2.3.1 The HAZid technique is used to identify the following:

- the hazards;
- the hazardous scenarios;
- the initiating events;
- controls (*existing and potential*); and
- recovery factors.

2.4 Disadvantages

2.4.1 HAZid can be time consuming and relies on skills and knowledge of participants.

2.5 Further Reading

- Reason, J. (*1997*). Managing the risks of organizational accidents. Aldershot: Ashgate Publishing Company.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E3. PRELIMINARY HAZARD ANALYSIS (PHA)

3.1 Context

3.1.1 Preliminary Hazard Analysis (*PHA*) is a hazard identification and frequency analysis technique. It can also be useful when analyzing existing systems or prioritizing hazards where circumstances prevent a more extensive technique from being used. A Primary Hazard Listing (*PHL*) is created as part of PHA as it is performed to identify the main generic hazards and accident scenarios that shall be associated with the system. PHA shall be applied to all systems, subsystems, components, procedures, and interfaces.

3.2 Purpose

3.2.1 The purpose of a PHA is to identify the hazards, hazardous situations and events that can cause harm for a given activity, facility or system. PHA identifies possibilities for accidents, qualitatively evaluates the extent of injury or damage from these, and identifies possible remedial measures.

3.3 Advantages

3.3.1 The PHA identifies areas of the system that will have an effect on safety by evaluating the major hazards associated with the system. These hazards shall be controlled by engineering or administration or eliminated by design if possible.

3.4 Disadvantages

3.4.1 The PHA is based on data available at the early design stages, therefore only basic or incomplete information may be available and a hazard identification process will need to be repeated later.

3.5 Further reading

- Stephens, R. A., & Talso, W. W. (*1997*). System safety analysis handbook (*2nd edition*). New Mexico: System Safety Society.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E4. FAILURE MODE EFFECTS (CRITICALITY) ANALYSIS (FMEA/FMECA)

4.1 Context

4.1.1 Failure Mode and Effects Analysis (*FMEA*) examines potential failures in products or processes. It is a fundamental hazard identification and frequency analysis technique that systematically identifies all the fault modes of individual components and their effects on other components and the system.

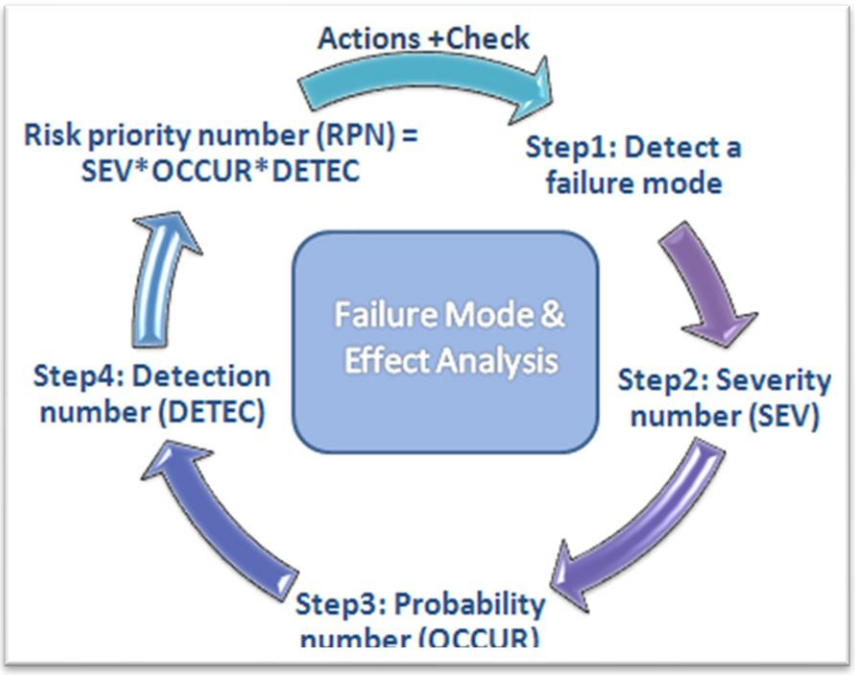

Figure 2: FMEA Process

4.1.2 By including the criticality of a failure mode FMEA becomes Failure Mode and Effects Criticality Analysis (*FMECA*) and is used as a ranking tool for each failure mode. FMECA identifies safety critical equipment, where a single failure shall be critical for the system.

4.2 Purpose

4.2.1 FMEA/FMECA is mainly used for component- based or procedural based systems. FMEA and FMECA are techniques for working bottom-up from a fault or undesired action, to estimate their top level effect on a system and/or procedure.

Note: *FMEA is ideal in combination with Fault Tree Analysis.*

4.3 Advantages

4.3.1 FMEA considers consequences of component fault modes one at a time. In contrast to developing a fault or failure tree assuming a hazard or undesired event and working top down, FMEA/FMECA works bottom-up from an assumption of the occurrences. The techniques can be used to pinpoint the likely impact on safety as a result of failure anywhere in a system and also assist in quantifying the probability of occurrence of the undesirable event.

Note: *The results can be readily verified by another person familiar with the system.*

4.4 Disadvantages

4.4.1 The main disadvantages of FMEA are:

a. The technique focuses on single component failures, and many of the faults and consequences

analyzed shall not be safety-related. Therefore considerable effort shall be expended to sift out those not relevant to safety;

b. Human errors are not considered in these analyses, although this is just the practice - it is not inherent in the approach; and
c. Time consuming and may be expensive to carry out as it focuses on single component failures.

4.5 Further reading

- AS//NZS 3931:1998 Risk Analysis of Technological Systems
- Hammer, W., “Handbook of System and Product Safety,” Prentice-Hall, Englewood
- Department of Defense, MIL-HDBK-217A, “Reliability Prediction of Electronic Equipment,” 1982.
- Wallace, R.C., “A Step by Step Guide to FMECA”, Reliability Review, Vol. 5 No. 2, June 1985.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007.

E5. HAZARD AND OPERABILITY (HAZOP) STUDY

5.1 Context

5.1.1 Hazard and Operability (*HAZOP*) study is a systematic qualitative technique used for identifying hazards and operability problems throughout a facility or system through a structured brainstorming process.

5.1.2 Originally developed for the chemical industry, a HAZOP study is a form of FMEA, and is often integrated with probabilistic analysis of considered conditions.

5.1.3 A HAZOP session involves a panel of multi-disciplined experts including operational and human factors experts, a process overview, and a brainstorming session using key words to create a table of hazards and their mitigations.

Note: *The most common form of HAZOP study is carried out at the detailed design phase and is called a HAZOP II Study.*

5.2 Purpose

5.2.1 The purpose of HAZOP study is to:

a. produce a full description of the process/facility (*including the intended design conditions*);
b. review systematically every part of the process or facility to discover how deviations from the intention of the design can occur; and
c. decide whether these deviations can lead to hazards or operability problems.

5.3 Advantages

5.3.1 HAZOP studies can highlight deviations from the normal which demand mitigating measures, or where mitigation is impractical, initiating events which require further analysis. Other general strengths are:

- HAZOP is effective for both technical faults and human errors; it covers human operators;
- HAZOP recognizes existing safeguards (*controls*) of a hazard and develops recommendations for additional ones;
- Unlike FMEA, HAZOP does not require the systematic study of the failure modes of each part of the functionality and of their effects of criticality on their failure mode;
- HAZOP has the potential to find more complex types of hazardous events and causes;
- It provides a systematic and exhaustive coverage and can lead to the discovery of new hazards. It can provide a very comprehensive hardware review;
- It encourages creative thinking about all the possible ways in which hazards or operating problems shall arise; and
- Only limited training required.

5.4 Disadvantages

5.4.1 Some disadvantages associated with HAZOP technique are:

- It may be weak at identifying interactive combinations of equipment failures that lead to

accidents;
- It depends heavily on data completeness and accuracy of drawings and documentation;
- It is not good for examining common cause or dependent failures;
- Can be very time consuming and labor intensive;
- The same group of experts identify both hazards and mitigating measures, whereas the latter function shall be better served by other experts; and
- Documentation of a HAZOP is lengthy (*for complete recording*).

5.5 Further reading

- Stephens, R. A., & Talso, W. W. (1997). System safety analysis handbook (*2nd edition*). New Mexico: System Safety Society.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E6. GOAL STRUCTURING NOTATION (GSN)

6.1 Context

6.1.1 Safety arguments need to be produced as part of the safety assurance work associated with change implementation. The safety argument needs to be a consistent, coherent, and complete logical structure that supports the top level safety goal based upon the developed evidence.

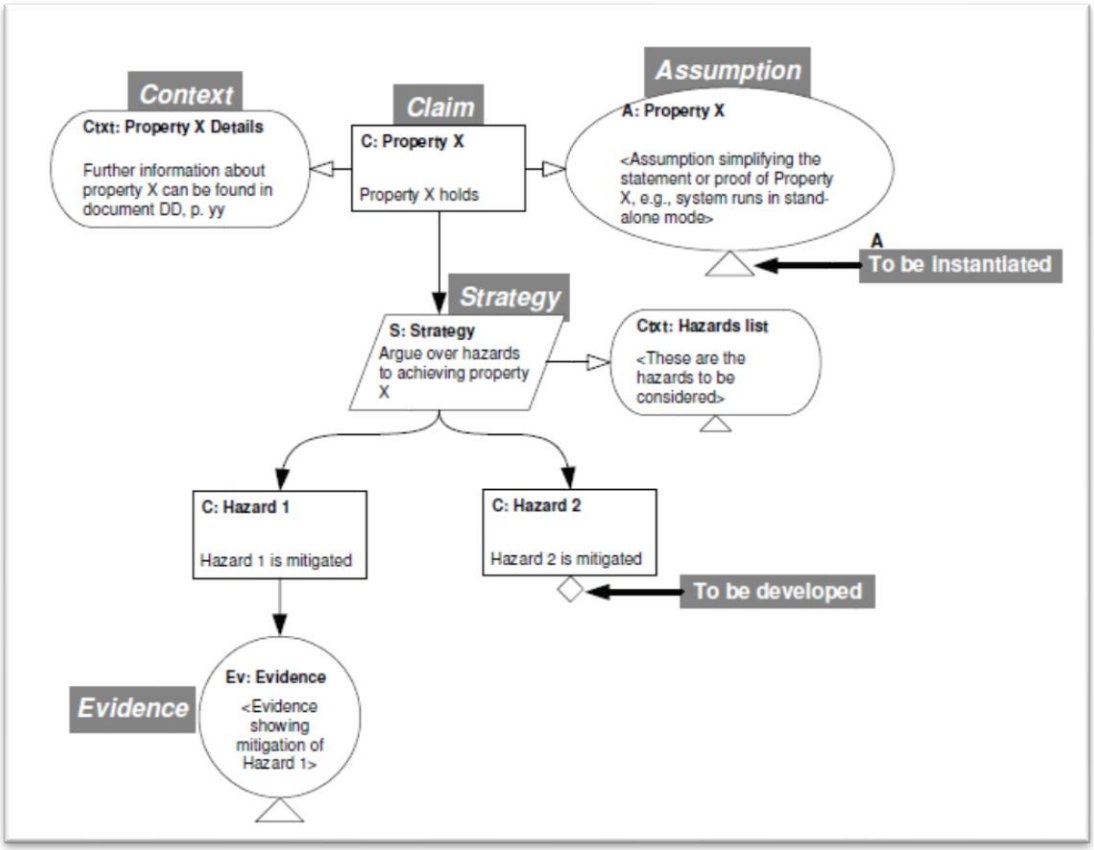

Fig 3: GSN Example

6.1.2 This logical structure can be difficult to ascertain, or evaluate, from purely textual information, especially for large safety assurance documents. GSN is a graphical argument notation that can be used to explicitly document the logical structure of the safety argument as a support to the textual presentation of the safety argument, i.e. it is a 'Roadmap' from Goals to evidence.

6.2 Purpose

6.2.1 GSN is intended to provide an explicit graphical representation of the logical structure associated with a safety argument. It provides a 'top down' decomposition of the argument structure from the top level Goal, via Strategies to further decomposed Goals until a Goal can be met directly by a piece of Evidence. In addition Context and Assumptions/Justification can be associated with Goals to further support and reinforce the Safety Argument.

6.2.2 The use of GSN to represent a safety argument does not replace the need to develop a 'good'

argument nor does it guarantee that a 'good' argument will be produced. The argument itself shall include assessment of the following argument qualities:

a. ***Completeness*** – all aspects necessary to support the argument are covered at each level of decomposition i.e. there is no additional considerations that could be added to the argument;
b. ***Correctness*** – each level of decomposition is supported by the 'right' elements below, down to the final evidence items;
c. ***Robustness*** – the argument is not sensitive to changes to Assumptions or Context/Justifications, and that the Evidence items have the requisite content and quality.

6.2.3 GSN is intended to support the full text safety argument - not replace it.

6.3 Advantages

6.3.1 The advantages of using GSN are that:

- it is flexible in its application;
- it can be applied at the start of a project to reach early agreement with stakeholders on the necessary argument structure and hence necessary evidence. Assists with project planning and safety stakeholder engagement;
- it assists in the planning of activities to produce items of necessary Evidence;
- its explicit graphical representation of the argument structure assists with :
    - Assessment of whether the argument is 'Complete'. This is done by assessing whether at each stage of decomposition that all the necessary elements to meet that Goal have been identified and included;
    - Assessment of whether the argument is 'Correct'. This is done by assessing the identified Strategies and Goals at each level, down to the set of evidence that is necessary to fully support the argument and hence the top level Goal;
    - Identification and therefore elimination of 'circular' arguments which would weaken or invalidate a Safety Argument;
    - Assessment of the impact of shortfalls in the Evidence or invalidated Assumptions and changes to Context / Justification and hence assess the 'Robustness' of the argument;
- it makes explicit the argument structure and allows complex argument to be sequentially broken down to individual goals for easier planning and understanding of system element relationships;
- arguments represented in a graphical format aid in the explanation and understanding of complex systems, hence this acts as a good communication tool so that project personnel can understand where they fit into the overall 'safety picture';
- it can be used as a simple diagrammatic overview of a safety argument as part of the safety assurance documentation (*i.e. as Appendices*) or can be used to provide the narrative framework through the entire safety assurance documentation. Provide a high level 'road map' that allows independent inspection and understanding of the Safety Argument structure;
- it assists in the tracking of safety activities progress as Evidence items can be marked as in-progress or completed.

6.4 Disadvantages

6.4.1 The disadvantages of using GSN are that:

- it requires some education and support for people being introduced to the notation for the first time; and

- the safety argument is subjective and will need input from multiple stakeholders to provide confidence that it is robust.

6.5 Further reading

- http://www-users.cs.york.ac.uk/~malihetb/Publication/GRR-Main.pdf
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007.

E7. HIERARCHICAL TASK ANALYSIS (HTA)

7.1 Context

7.1.1 A Hierarchical Task Analysis (*HTA*) is a "top-down" goal orientated technique, which arranges each task in hierarchical order, with the highest level (goal) being the most complex and the lower levels forming prerequisite skills for the higher levels (*tasks and subtasks*).

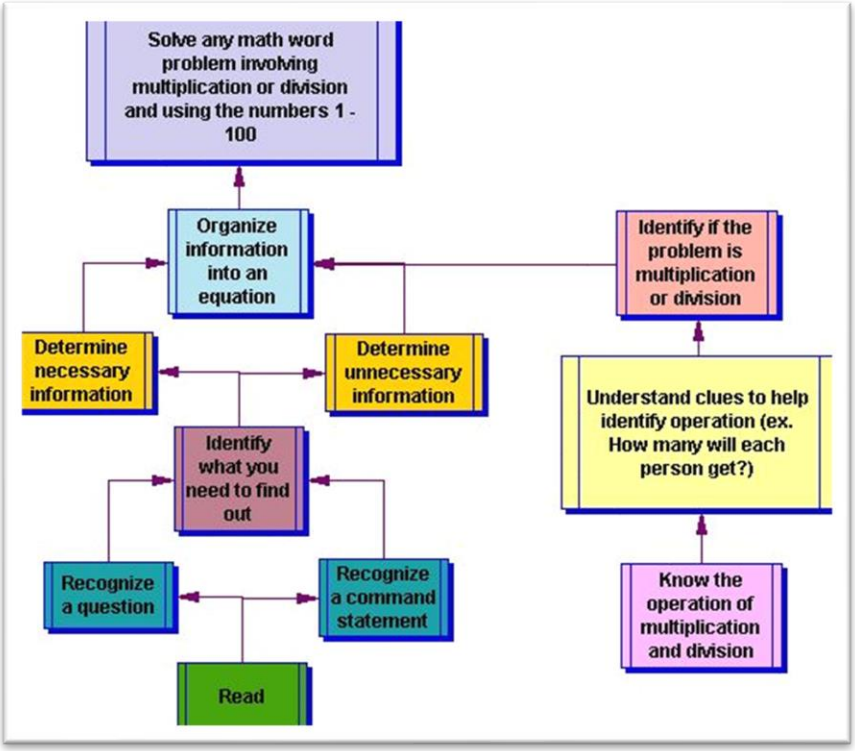

Fig 4: HTA Format Example

7.1.2 Each task shall be described and characterized with sufficient detail to allow for potential errors to be identified.

7.1.3 This technique produces a hierarchy of three levels of task analysis:

a. ***Goals*** - system state that the human wishes to achieve;
b. ***Tasks*** - structured set of activities in some sequence to achieve goals; and
c. ***Operations or actions*** - different things that a person shall do within a system simple tasks (*sub-tasks are needed if further breakdown is required*).

8.1.4 HTA is best suited for analyzing simple cognitive and physical tasks where a clear goal, task, and subtasks required to accomplish the goal can be determined. A HTA can be used to perform human error identification and/or human reliability quantification.

7.2 Purpose

7.2.1 The purpose of a HTA is to provide sufficient information to allow the potential errors during performance of a task/s to be identified and addressed.

7.3 Advantages

7.3.1 The HTA is a widely used structured analysis which results in a description of tasks in terms of sub-tasks. It allows for possible error identification opportunities and is easy to learn and use. The description of each task can be utilized to develop safeguards, training, and procedures.

7.4 Disadvantages

7.4.1 The disadvantages of HTA are that it:

- Can be time consuming;
- Does not account well for errors or unforeseen events; and
- Applies only to procedural activities and not to heavily parallel activities.

7.5 Further reading

- Merkelbach, E. J. H. M & Schraagen, J. M. C. A Framework for the Analysis of Cognitive Tasks. TNO Human Factors Research Institute, Report No TNO – TM 1994 B -13 (1994).
- Shepherd, A. Hierarchical Task Analysis. New York: Taylor & Francis, 2000. A Text Book on HTA
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E8. HUMAN ERROR ASSESSMENT AND REDUCTION TECHNIQUE (HEART)

8.1 Context

8.1.1 Human Error Assessment and Reduction Technique (*HEART*) is a human reliability assessment tool that is commonly used to quantitatively assess human reliability through an estimation of the human error probability (*HEP*). This is accomplished by categorizing the task and determining the factors e.g. environmental and ergonomic, which could reduce the chances of a successful conclusion.

Note: *The HEP is the probability of failure to complete the task and is implicitly inclusive of contributions from all possible failure modes (i.e. errors of omission and commission).*

8.1.2 HEART is based on the three foundations:

a. Basic human reliability is dependent on the generic nature of the task to be performed.
b. Level of reliability will tend to be achieved consistently with a given nominal likelihood within probabilistic limits.
c. Given that these perfect conditions do not exist in all situations, the human reliability predicted shall be expected to degrade as a function of the extent to which identified error-producing conditions (*EPCs*) might apply.

8.2 Purpose

8.2.1 The purpose of HEART is to present a method for assessing and reducing human error by providing defensive measures to overcome the effects of human error and to improve overall operational performance.

8.3 Advantages

8.3.1 HEART is known to be an effective tool for:

- predicting human reliability; and
- identifying ways of reducing human error.

8.4 Disadvantages

8.4.1 HEART is not a thorough technique and some aspects rely on judgments (*subjective view*).

8.5 Further reading

- Harvey, R.S & Sandom. C (2004). Human factors for engineers. Institution of Electrical Engineers
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E9. HUMAN RELIABILITY ANALYSIS (HRA)

9.1 Context

9.1.1 Human Reliability Analysis (*HRA*) assesses the reliability of human performance. Reliable human performance is necessary for the success of human-machine systems and is influenced by many factors, which are known as performance shaping factors (*PSFs*).

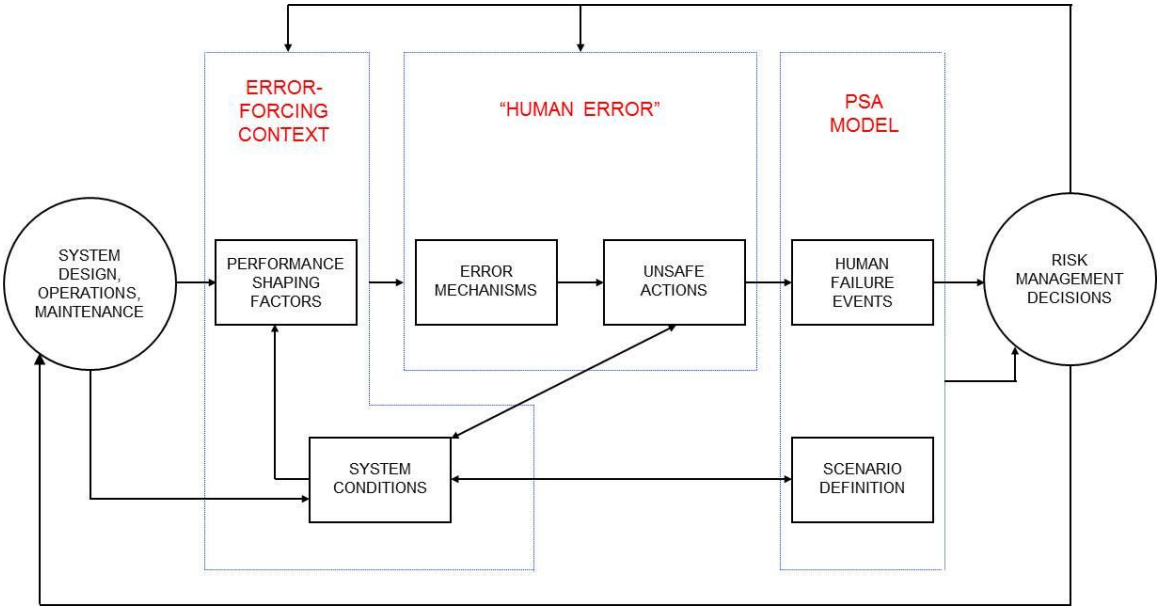

Fig 5: HRA Model

9.1.2 PSFs can either be internal attributes such as stress, emotional state, training, and experience, or external factors such as work hours, environment, actions by supervisors, procedures, and hardware interfaces.

9.1.3 The number of PSFs that affect human performance is vast. Although not all PSFs can be controlled, many can influence the success or failure of an operation or process.

9.1.4 HRA also looks at human error as part of PSF. Human error does not simply imply error committed by humans, but rather the course of an action being committed or omitted that has the potential to adversely influence safety.

9.2 Purpose

9.2.1 The purpose of a HRA is to assess factors that shall impact human reliability in the operation of a system by estimating the probabilities of human error that have the potential to make the defenses fail.

9.3 Advantages

9.3.1 HRA can be used to assess systems that are very small, well-defined, as well as large and complex.

9.4 Disadvantages

9.4.1 HRA technique has the capability of thoroughly analyzing the human-machine interactions for the system, but does not address other issues such as hazards caused by equipment failure.

9.4.2 For high complexity systems an extensive and in-depth analysis requires highly qualified individuals.

9.5 Further reading

- American Institute of Chemical Engineers - Knovel (*firm*). (*1992*). Guidelines for hazard evaluation procedures. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E10. STRUCTURED WHAT IF TECHNIQUE (SWIFT)

10.1 Context

10.1.1 The Structured What-If Technique (*SWIFT*) is an alternate systematic technique utilized to: identify hazards (including many time-critical applications); hazardous situations; or a specific event that could in turn lead to an undesirable consequence. It is best used following a Preliminary Hazard Analysis (PHA) to further investigate particular areas of concern and to identify the hazards.

10.1.2 SWIFT considers deviations from normal operations identified by brainstorming, with questions beginning "What if…?" or "How could…?". The brainstorming is supported by checklists to help avoid overlooking hazards. SWIFT shall be used simply to identify hazards for subsequent quantitative evaluation, or alternatively to provide a qualitative evaluation of the hazards and to recommend further safeguards where appropriate.

10.2 Purpose

10.2.1 The purpose of SWIFT is to identify hazards for a quantitative evaluation, or alternatively, for a qualitative evaluation on which could ultimately lead to an undesirable consequence. It is designed to add structure to the intuition and experience of operational personnel.

10.3 Advantages

10.3.1 SWIFT is effective in:

- capturing data regarding failure modes that can create hazards;
- its flexibility - it can be modified to suit each individual application; and
- recommending further safeguards where appropriate.

10.4 Disadvantages

10.4.1 The difficulty of application shall be increased as the processes or operations under study become more complex.

10.5 Further reading

- Department of Energy, DOE/EH-DRAFT (1993). "Preliminary Guide for Conformance with OSHA's Rule for Process Safety Management of Highly Hazardous Chemicals."
- Department of Energy, DOE/EH-Draft (1993). "Guide for Chemical Process Hazard Analysis."
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan - 15. Issue 2.0 October 3rd, 2007

E11. EVENT TREE ANALYSIS (ETA)

11.1 Context

11.1.1 An Event Tree Analysis (*ETA*) is a technique that can be either qualitative and/or quantitative. It is used to identify potential accidents and their outcomes by means of "forward thinking" from an initiating event, like equipment failure or human error and if required, their probabilities, given the occurrence of an initiating event.

Note: *An ETA is based on dual logic, in which an event either has or has not happened or a component has or has not failed.*

11.1.2 It is used to support hazard identification and risk assessment by providing further insight into hazardous events by examining the coincidental circumstances that need to be in place, and the barriers that need to be breached, for a hazard to manifest into an accident or incident. Event Trees (*ET*) can therefore be used on hazards to identify a more realistic likelihood of an accident or incident occurring.

11.1.3 ETA determines the likelihood and severity of a range of consequences given different sequences of events.

11.2 Purpose

11.2.1 An ETA identifies the potential outcomes or consequences of the occurrence of a specified initiating event. It is an analytical tool that can be used to organize, characterize, and quantify potential accidents in a methodical manner. An ETA models the sequence of events that results from a single initiating event.

11.2.2 An ETA asks the basic question "what happens if ...?" It clearly analyses and presents the relationship between the failure of various mitigating systems and ultimately the hazardous event which shall be a consequence of the occurrence of the single initiating event.

11.3 Advantages

11.3.1 It is very useful in identifying events which require further analysis i.e. Fault Tree Analysis (*FTA*) (see Appendix E12).

11.4 Disadvantages

11.4.1 In order to do a comprehensive risk assessment, all potential initiating events need to be identified however this can be time consuming;

11.4.2 There is a potential for missing important initiating events with this technique;

11.4.3 ET's only deal with success states and fault states of a system. It is difficult to deal with delayed success or recovery events; and

11.4.4 The probabilities in an ET are conditional probabilities. For example in a building explosion and fire, the probability of the sprinkler system working is not the probability obtained from tests under normal conditions, but the probability of its functioning under conditions of fire caused by explosion.

11.5 Further reading

- Stephens, R. A., & Talso, W. W. (1997). System safety analysis handbook (*2nd edition*). New Mexico: System Safety Society.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E12. FAULT TREE ANALYSIS (FTA)

12.1 Context

12.1.1 Fault Tree Analysis (*FTA*) identifies an undesirable event (*top event*) and the contributing elements (*faults/conditions*) that would precipitate it. The contributors are interconnected with the undesirable event, using network paths through Boolean logic gates.

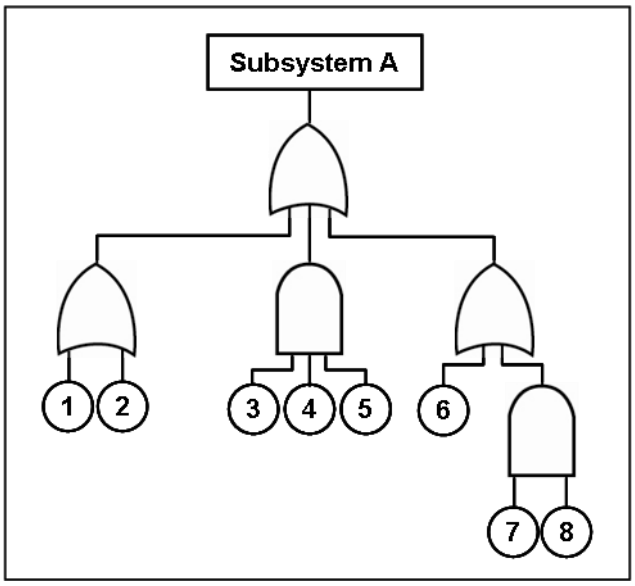

Fig 6: Fault Tree Example

Note 1: *Boolean logic considers two possible states: 0 and 1. These can then be translated into other, more useful meanings. For example, 0 could represent the state "false" and 1 could be "true".*
Note 2*: Boolean logic consists of a set of "logic gates", each of which is a different set of rules. The three main logic gates are AND, OR, and NOT.*

12.1.2 The specific undesired event is the "top event". Once this has been defined, deductive logic is employed working backwards from effect to cause. The basic events, which are implicated in bringing about the top event, show the logic of these combinations.

12.2 Purpose

12.2.1 The purpose of a FTA is to assess a system by identifying an undesirable end event and examining the range of potential events (*base event and intermediate events*) that could lead to that state or condition.

Note: *The top event is equal to the top event represented in the Bow Tie diagram. It is NOT the consequence. The base events are the threats.*

12.3 Advantages

12.3.1 FTA assists both expert and non-expert individuals to distinguish the cause and effect process of

undesired events (*top event*). It does so by displaying the precipitating events or combinations of events graphically, hence, facilitating a more complete identification of potential hazards and a more complete understanding of the nature of the hazard.

12.3.2 The top-down approach requires analysis completeness at each level before proceeding. The FTA addresses effects of multiple failures by identifying inter-relationships between components and identifying minimal failure combinations that cause the system to fail (*minimal cut sets*).

12.3.3 The method addresses the effects of design, operation, and maintenance. Many standardized computer analysis packages exist to make the process much faster and easier.

12.3.4 FTA provides both qualitative and quantitative (*probabilistic*) information; probabilities shall be assigned to each sub-event and aggregated to determine an overall probability for the top event.

12.3.5 As marked advantages, the method identifies minimum sets of contributing factors which, if they occur, will often precipitate the central undesirable event. Common causes and human operator paths to events are also disclosed by use of the method.

12.3.6 Contributory failures can be either hardware, software, human error or any other condition that shall influence the likelihood of the top event.

12.4 Disadvantages

12.4.1 The presumption is that contributing factors have been adequately identified and explored in sufficient depth;

12.4.2 It cannot guarantee identification of all failures but the systematic approach enhances the likelihood of completeness;

12.4.3 The technique can be expensive and time consuming;

12.4.4 It requires extensive work and detailed systems and/or operational knowledge. Therefore a FTA requires complete knowledge of the system or procedure being modeled, its interconnections/interfaces (*or sequential steps*), and the possible hardware or human failure modes;

12.4.5 The “top-down” approach focuses on those effects of failure which are directly related to the top event in the tree. This shall lead to missing effects which are important elsewhere; and

12.4.6 The pictorial trees generated are often large; this means the processing of fault trees shall require computer systems.

Note: *Although time-consuming, it is not difficult once the technique has been mastered. Computer aids are available and are increasingly used. Unlike ET analysis and FMEA, the technique explores only those faults and conditions leading to intolerable losses.*

12.5 Further reading

- Risk and Reliability Associates (n.d.). Risk & Reliability - An Introductory Text 5th Edition (available from http://www.r2a.com.au/)
- Stephens, R. A., & Talso, W. W. (1997). System safety analysis handbook (2nd ed.). New Mexico: System Safety Society.
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E13. ROOT CAUSE ANALYSIS (RCA)

13.1 Context

13.1.1 The Root Cause Analysis (*RCA*) determines the underlying contributing reasons (*root causes*) for the observed deficiencies documented in the findings of an investigation. By addressing a few root causes, management can correct a wide variety of deficiencies or faults in a system. RCA is used primarily for failure analyses and other investigations.

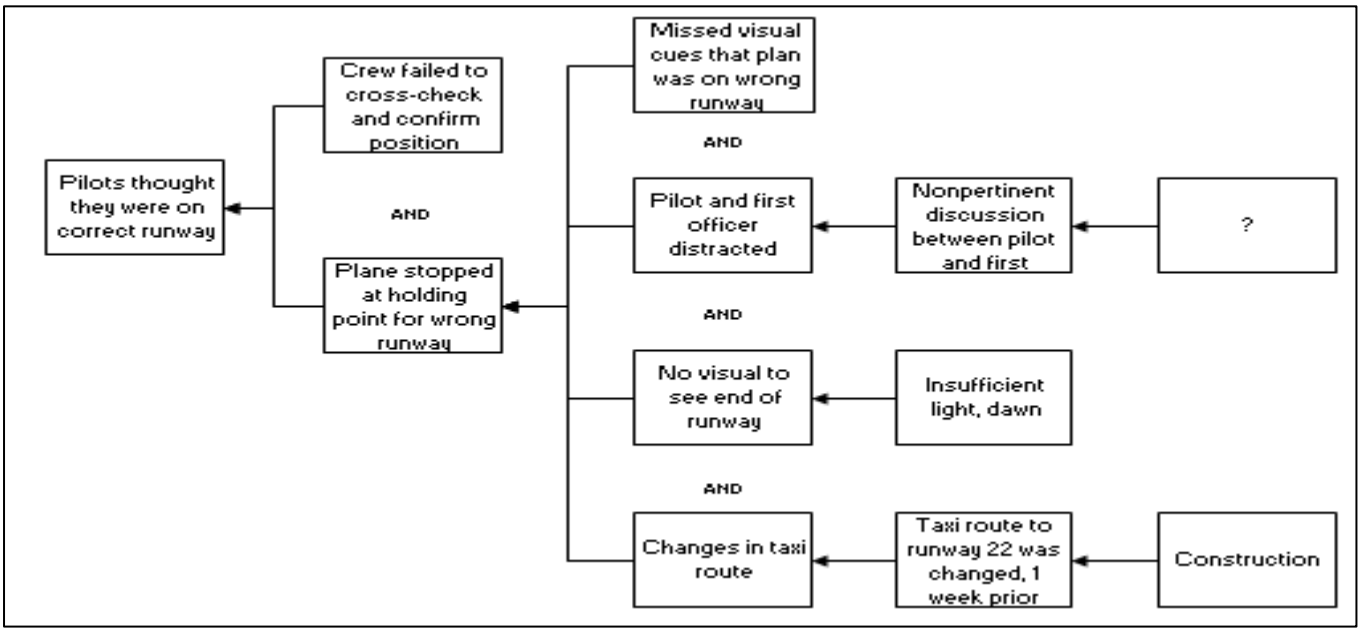

Fig 7: Simple RCA Example

13.2 Purpose

13.2.1 The purpose of the RCA is to identify causal factors relating to a mishap or a near-miss incident.

13.3 Advantages

13.3.1 RCA enables management to identify root causes and correct the deficiencies or faults associated within the system directly at the initiation point addressing wider issues.

13.4 Disadvantages

13.4.1 This technique can be time consuming and does not address intermediate deficiencies.

13.5 Further reading

- SAIC, EPRI-CS-1812 (1981). "Approach for Root Cause Analysis of Power Plant Equipment Problems."
- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007

E14. SENSITIVITY ANALYSIS (SA)

14.1 Context

14.1.1 Sensitivity analysis (*SA*) is the study of how the variation in the output of a model (*whether is it numerical or otherwise*) can be apportioned, qualitatively or quantitatively, to other sources of variation.

14.2 Purpose

14.2.1 The purpose of SA is to determine the relationships between the uncertainty in the independent variables used in an analysis and the uncertainty in the resultant dependent variables.

14.3 Advantages

14.3.1 SA increases the confidence in the model and its predictions, by providing an understanding of how the model response variables respond to changes in the inputs, be they data used to calibrate it, model structures, or factors, i.e. the model independent variables.

14.3.2 SA is closely linked to uncertainty analysis (*UA*), which aims to quantify the overall uncertainty associated with the response as a result of uncertainties in the model input.

15.4 Disadvantages

15.4.1 SA requires thorough training.

15.5 Further reading

- FAA/Eurocontrol. ATM Safety Techniques and Toolbox. Safety Action Plan -15. Issue 2.0 October 3rd, 2007