Advisory Circular

AC AN/ATM-SRM-01-14

GUIDELINES FOR PREPARING SAFETY ARGUMENTS

COVERING CAR-ANS PART 11(ATS)

Aerodrome & Air Navigation Safety Oversight Office (AANSOO)
Office of the Director General
Civil Aviation Authority of the Philippines
Old MIA Road, Pasay City, 1300
June 2, 2014

Advisory Circulars (AC) are intended to provide recommendations and guidance, illustrate a means-but not necessarily the only means of complying with regulatory requirements, or to explain certain regulatory requirements by providing interpretative and explanatory materials.

CAAP will generally accept that when the provisions of an Advisory Circular have been met, compliance with the relevant regulatory obligations has been satisfied.

Where an AC is referred to in a “Note” within regulatory documentation, the AC remains as guidance material.

ACs should always be read in conjunction with the referenced regulations.

CONTENTS

1. REFERENCES

1.1 This Advisory Circular (AC) should be read in conjunction with the Civil Aviation Regulations Part 1 – Air Navigation Safety Oversight and CAR-ANS Part 11 – Air Traffic Service Providers. These documents are available on the CAAP website at: www.caap.gov.ph. This document (AC) may also refer to portions of the following:

- CAR-Aerodromes
- Manual of Standards (MOS) for Aerodromes
- ICAO Annex 11, Air Traffic Service
- ICAO Annex 14, Aerodromes
- ICAO Annex 19, SMS and SSP
- ICAO Doc 4444, PANS-ATM
- ICAO Doc 9870, Manual on the Prevention of Runway Incursion
- ICAO Doc 9859, Safety Management Manual

2. PURPOSE

2.1 The Philippines, as signatory to the International Convention on Civil Aviation, adheres, to the extent practicable, to the ICAO Standards and Recommended Practices. The modern requirements for enhancing safety in civil aviation has brought into the fore the need for contracting States to develop, establish, and implement State Safety Programmes and for service providers to develop, establish, and implement Safety Management Systems.

The CAR-ANS Parts 1 and 11 regulatory standards covering air traffic service providers require the preparation of safety arguments, assessments and reviews to support a new service or a proposed change to an existing service (Ref: CAR-ANS Part 1, 1.5 and Part 11, 11.2.27, Annex 19, App 2, 2.2). This AC provides guidelines for ATS service providers to comply with the requirements.

3. STATUS OF THIS AC

3.1 ACs are numbered to reflect the regulatory basis, the serial number of the circular issued for that regulation and the revision status for that AC. In this case, the regulatory bases are CAR-ANS Part 1 – Regulations Governing Safety Oversight and CAR-ANS Part 11 – Regulations Governing Air Traffic Services. This is the first issue of AC AN/ATM-SRM-01. It remains current until re-issued, withdrawn or superseded.

4. DEFINITIONS

The following definitions are applicable to this AC. They are not necessarily definitions that apply to CAR-ANS Part 11.

Hazard: A hazard is defined as a condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.

Hazard identification: The process of recognizing that a hazard exists and defining its characteristics.

Operational requirement: The stated purpose of the service.

Risk assessment: The process of determining the risk involved in the occurrence of a hazardous event, and the tolerability of that risk.

Safety: The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level.

Safety risk: The predicted probability and severity of the consequences or outcomes from an existing hazard or situation.

Safety risk management: The systematic application of management policies, procedures and practices to the tasks of identifying hazards and assessing and controlling risks.

Safety risk probability: The likelihood or frequency that a safety consequence or outcome might occur.

Safety risk severity: The extent of harm that might reasonably occur as a consequence or outcome of the identified hazard

Safety argument: Safety arguments provide documented evidence and assessment that a service or facility, or a proposed change to the design of a service or facility, meet safety objectives or levels for the service or facility.

Safety management system (SMS): The policies, procedures and activities by means of which safety management is undertaken by a service provider.

Service: An air traffic service as defined in CAR-ANS Part 11.

5. SAFETY MANAGEMENT SYSTEM – SAFETY ARGUMENT

5.1 The primary purpose of a safety management system is to predict what accidents or incidents may occur, how they may happen, and how they may be prevented. The processes for safety assurance in various industries may differ in detail, however they all prescribe the systematic undertaking of safety risk assessment and the presentation of evidence and demonstration that the particular system is safe.

5.2 One way of presenting such evidence and demonstration is by preparing a safety argument. A safety argument provides documented evidence and demonstration that a service or facility, or a proposed change to the design of a service or facility, meets safety objectives or levels for the service or facility.

5.3 This document provides guidelines for the preparation and maintenance of safety arguments covering CAR-ANS Part 1 – Safety Oversight and Part 11-Air Traffic Services.

6. CAAP REQUIREMENTS FOR A SAFETY MANAGEMENT SYSTEM

6.1 CAR-ANS Part 1 and Part 11 require air traffic service providers to have a Safety Management System (SMS). One of the elements of the SMS is a requirement for a process for assessing the safety implications and safety hazards involved in their operations, and determining the action necessary to reduce the risk of those hazards to acceptable levels.

6.2 One appropriate methodology for addressing the above requirement is through the preparation and maintenance of a safety case or argument.

7. REQUIREMENTS FOR A SAFETY ASSESSMENT

7.1 CAR-ANS Part 1 (1.3, 1.4 and 1.5) and Part 11 (11.2.27) set the basic standards for a safety argument, or another equivalent safety assessment process, to be prepared by service providers, to support a new service or a proposed change to an existing service:

- the effect of which would be that the service would no longer be in accordance with the safety regulatory requirements or the certificate issued to the ATS provider; or
- that requires prior notification to CAAP because of a requirement to do so in the ATS provider's safety management system.

8. SAFETY PLANNING

8.1 It is expected that safety will be built into any new CAR-ANS Part 11 (Air Traffic Service) service from its early inception and the management of safety related activities will be undertaken in a planned manner over the lifecycle of the service.

8.2 The safety plan may be a discrete element of a project management plan, if applicable, or it may stand-alone. Either way, the safety plan should provide the basis for developing the parts of the safety argument at defined milestones as the development and implementation of the service progresses.

8.3 For those services that have a lifecycle consisting of several distinct phases, the hazards and associated risks may differ in type and degree in each phase, and their identification and control treatment will be more appropriately undertaken at a particular phase in the lifecycle. Accordingly, safety arguments need to be developed to separately consider the safety situation in each of the lifecycle phases. This may require several parts of the safety argument, with each part building on the previous part.

8.4 Some services which are essentially procedurally-based or less complex may have less distinct life-cycle phases, or the phases may merge, or essentially occur at a similar time. For these types of service, the safety argument might be defined in one document part.

8.5 The distinct phases in the development of a new service or service change that would be covered by a safety argument are normally:

- **the operational requirements phase**, when the role and broad functionality of the new service or service change is determined. This phase should identify the safety objectives of the service and its applicable safety requirements, (these may be based on ICAO SARPS, CAAP regulatory requirements, and the service provider's internal safety standards);
- **the design phase**, when the new service or service change is designed and developed to meet the specified operational requirements. In this phase, the configuration and operation is defined, incorporating the safety objectives and requirements within the evolving design. A full hazard and risk assessment is usually undertaken;
- **the pre-commissioning phase,** when the service is subject to procedural and/or operational readiness testing against the design specifications, followed by operational trials, such as ghosting or mimicking. At this phase, the risk assessment is tested and validated by actual trials and testing, and specific safety related operational and/or management procedures are developed to obviate or control the identified risks; and
- **the commissioning and routine operations phase,** when the safety of the service continues to be monitored and improved as any hazards are identified as they arise, and the risks are mitigated during actual operations.

8.6 The safety argument should describe the historical and current safety status of

the service as it develops throughout its entire lifecycle.

9. PURPOSE AND SCOPE OF THE SAFETY ARGUMENT

9.1 A safety argument is essentially a structured, comprehensive statement of the hazards surrounding the provision of an operational service, including the significance of the hazards in terms of their likelihood of occurrence and potential effects on aviation safety, and the means whereby they are to be managed. The essential features of a safety argument are that it should fully describe the service which it covers (i.e. the configuration and the boundaries of the system), identify the hazards, assess the associated risks, and establish the controls necessary to ensure the risks are tolerable. Hazard/risk management should ensure that all possible failure and fault modes have been identified and appropriate controls put in place so safe operation of the system is preserved under all modes.

9.2 The purpose and scope of the safety argument should be clearly stated in its introductory paragraphs, and should include:

- A statement of the purpose and role of the service under consideration including the system Operational Requirement and a description of how it operates. The description of the service should include:
  - its location;
  - its configuration including the sub-system elements;
  - the service boundaries; the elements of the service which have been considered within the scope of the document, i.e., whether it covers equipment, procedures, personnel, etc.; and
  - the interfaces with other external services and systems.
- A statement of the assumptions upon which the safety case is based. This should include the defined or known levels of safety, or integrity, of each of the interfacing or support systems/services, and those other services externally provided by third parties, such as those provided by telecommunications service providers, electrical power service providers, etc.

9.3 The relevant phases of the new service or service change, covered by the particular part/s of the safety argument should also be defined.

10. SAFETY OBJECTIVES AND SAFETY REQUIREMENTS

10.1 The overall safety objectives of the system, consistent with, and in support of, the Operational Requirement, should be defined.

10.2 The safety requirements to achieve the overall safety objectives then need to be defined. These safety requirements should be derived by assessing the effect of possible functional failure or fault modes as the source of safety hazards and the associated effect on the operation of the system.

10.3 The functional failure or fault modes analysis should cover conceivable faults or eventualities affecting service performance including the possibility of human errors, common mode failures, simultaneous occurrences of more than one fault, and external eventualities which cause or result in the loss of, or affect the integrity of, external data, services, security, power supply, or environmental conditions. The assessment of the safety requirements may then result in an iterative process of revision and further development of the service design, the adoption of modified operational procedures, or the establishment of contingency arrangements. For this reason, the safety requirements should be expressed in a form that is clear and unambiguous.

10.4 The selection of an appropriate way of expressing the safety requirements is important.

Quantitative statements of safety requirements should be used where possible, however, in many areas (e.g. where people and procedures are involved) it may not be feasible to define quantitative values. For these areas, qualitative values can be established. Where possible, these should be equated to corresponding quantitative values, within an accepted risk tolerability classification scheme (refer to the next section).

11. RISK MANAGEMENT

11.1 Methodology

11.1.1 The methodology for risk management may vary depending upon the type and safety implications of the proposed new service or service change, and the use of different methods, or combinations thereof, may be appropriate for the different elements and lifecycle phases included in the safety case.

11.2 Hazard identification and risk assessment

11.2.1 Techniques for hazard identification/risk assessment may include:

- the use of data or experience with similar services/changes undertaken by overseas or other respected providers of similar Part 11 services (ATS);
- quantitative modeling based on sufficient data, a validated model of the change, and analyzed assumptions;
- the application and documentation of expert knowledge, experience and objective judgment by specialist staff (qualitative);
- trial implementation of the proposed change by simulation, or under surveillance and with sufficient backup facility to revert to the existing service before the change, if risks cannot be mitigated;
- a formal analysis in accordance with ICAO SARPs on "Risk management", or another accepted standard or text on risk analysis/system safety such as but not limited to the following:
    - event tree analysis (ETA);
    - quantified risk analysis (QRA);
    - failure modes and effects analysis (FMEA);
    - human factors analysis (HFA);
    - hazard and operability studies (HAZOPs).

11.3 Safety risk assessment criteria

11.3.1 In order to ensure that the range of possible safety risks are appropriately classified and controlled, service providers should develop criteria for safety risk assessment. Such a safety risk classification scheme provides a structure for deriving the safety requirements for services, as well as the criteria for risk control decisions. Typically, such schemes provide a standard relationship between the probability of occurrence of each risk and the categorized severity of the risk in terms of its potential impact on safety, finally equating that to a risk acceptability criterion. The acceptability rating thus indicates the necessity for, and extent of control required for each risk.

11.3.2 A safety argument document should include the risk assessment criteria (also termed a risk tolerability classification scheme) adopted by the service provider for safety management. CAAP does not intend to impose any specific risk assessment criteria or risk

tolerability classification scheme.

11.4 Risk control

11.4.1 A risk control process to eliminate or mitigate all risks categorized as intolerable, to a tolerable level, should also be defined. Risk controls may vary considerably, and employ any or a combination of, the following:

- service redesign, modification or replacement;
- process or procedures redesign;
- personnel education or training; and
- various management controls on personnel, procedures and equipment.

11.4.2 Any identified risks that cannot be controlled to a tolerable level should be explicitly included in a separate section of the safety argument that includes a discussion on all relevant aspects. The rationale for any decision to proceed with the development or operation of the service while the risk prevails is to be stated.

11.5 Precedence of risk controls

11.5.1 In the application of the above, or other, risk control processes, a safety precedence sequence should be adopted and applied. For instance, control of identified hazards should normally be sought first through improved design or facility/equipment changes, followed then by specific procedures or training. Whichever means of control is implemented, the control process should demonstrate how the risks are being brought within the limits of the safety objectives.

12. SAFETY ARGUMENT COVERAGE OVER THE LIFECYCLE OF THE SERVICE

12.1 As previously discussed, safety arguments should be developed in separate parts to define the safety situation of the service over the discrete stages of its lifecycle. A four part Safety Argument has been used to define the safety situation:

- at the Operational Requirements stage,
- at the completion of the Design phase,
- at Installation and Pre-Commissioning, and
- for the day-to-day Operational phase.

12.2 The contents of the safety argument will differ for each part. For some services, it may be appropriate to have fewer parts of the safety argument. For all parts, the level of description and detail included should be sufficient to provide a reasonably informed reader with an understanding of the safety situation, without the need to refer extensively to supporting references.

12.3 A guide to the coverage of each part of a four-part Safety Argument is included in Appendix A to this AC - *"Coverage for a Four-Part Safety Argument"*.

13. AUTHORITY FOR ISSUE AND CHANGE OF THE SAFETY ARGUMENT

13.1 Safety Arguments should be placed under a documentation control process.

13.2 The Safety Argument should be authorized by a competent authority designated by the service provider. For Part 11 services (ATS), an authority or authorities covering the operational requirements phase, the design phase, the pre-commissioning phase, and the

commissioning and routine operations phase should be appointed, and the issue of the parts of the safety argument should be made under the authority of one or more of these designated bodies, as appropriate to the content of each part.

14. AUDITS OF SAFETY ARGUMENTS

14.1 Internal monitoring and audit

14.1.1 It is expected that air traffic service providers will internally monitor and audit the safety aspects of their major air traffic service, airways and airspace projects under their internal monitoring and quality/safety audit programs. Monitoring may entail a specific means of safety reporting and analysis, or may be integrated with the existing processes already established by the service provider for incident and fault reporting and investigation, etc. The results of the internal monitoring should be incorporated into reviews and updates of the safety case, as necessary.

14.2 CAAP audits

14.2.1 CAAP, under its Audit, Inspection and Surveillance Program and Procedures Manual, may carry out audits of safety issues and concerns relating to Part 11 services (ATS). The relevant documentation pertaining to the safety argument may be a focus of such audits.

LTGEN WILLIAM K HOTCHKISS III AFP (Ret)
Director General
Civil Aviation Authority of the Philippines

June ____, 2014

APPENDIX A

COVERAGE FOR A FOUR-PART SAFETY ARGUMENT

The following is a guide to the information to be included in a four-part safety argument.

Safety Argument Part 1 - Operational Requirements Phase

A safety argument Part 1 contains the Safety Objectives and the corresponding Safety Requirements for the proposed service, and will normally be the initial document provided to CAAP to advise of the proposed project's existence and its safety significance. The safety argument at this stage should be an evaluation of the proposed system (such as that carried out by means of a system level Failure Modes and Effects Analysis or FMEA), supplemented as necessary by overseas or previous experience, and in-house expertise and knowledge of deficiencies in existing systems the new service is to replace.

Safety Argument Part 2 - Design Phase

Safety argument Part 2 is essentially to assure that the proposed new service or service change meets any necessary safety requirements. Demonstrations and documentation to support the design rationale of the service, and to verify and validate that such satisfies the safety requirements should be provided. The human factors aspects of the design, and the safety implications of the design of the procedures, and the ability of personnel to apply the procedures, should also be considered. Here, a full hazard and risk evaluation of the detailed design, including hardware, software, man/machine interface, human factors, equipment and administrative interfaces and external factors, should be undertaken.

Safety Argument Part 3 - Pre-Commissioning Phase

Part 3 should provide an analysis of the safety situation following the commissioning of the service. The functional testing to be carried out for installation and pre-commissioning evaluation of the safety situation is detailed in this part. A testing regime aimed at validating the risk assessment made in Part 2, and identifying safety hazards not previously identified at Part 2 which arise during testing and integration and related activities should be defined, with the strategy for assessing and managing these hazards and the safety issues which arise from such testing also specified.

Safety Argument Part 4 - Normal Operations Phase

Part 4 of the safety argument should provide the complete evidence that the service is safe in operational service. It should address all relevant operational and management issues, and take account of the safety findings from the preceding three parts of the safety argument. This part of the safety argument should be maintained as a living document for the life of the service, to define and document any further hazards, identified at post-commissioning or during routine operations, and the risk control actions taken to maintain compliance with safety objectives, in the light of actual day-to-day knowledge and experience with the service.

Note in respect to all Parts (1-4)

It is important that all parts of the safety argument be retained and maintained as necessary over the life of the service, reflecting the safety situation for any approved modifications or changes. Such amendments to the safety argument should be authorized by the appropriate approval authority.

APPENDIX B

SAFETY RISK MANAGEMENT PROCESS

I. HAZARD IDENTIFICATION

(Note: The following discussion and examples are from the ICAO Safety Management Manual, Third Edition, 2012. The original paragraph numbers were modified to align with the format of this document.)

1. HAZARDS

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

1.1 Understanding Hazards and Consequences

A hazard is generically defined by safety practitioners as a condition or an object with the potential to cause death, injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function. For the purpose of aviation safety risk management, hazard should be focused on those conditions that could cause or contribute to unsafe operation of aircraft or aviation safety related equipment, product and services.

Consider, for example, a 15-knot wind, which is not necessarily a hazardous condition. In fact, a 15-knot wind blowing directly down the runway improves aircraft takeoff and landing performance. However, a 15-knot wind blowing in a direction ninety degrees across a runway of intended take-off or landing creates a crosswind condition that may be hazardous due to its potential to contribute to an aircraft operational occurrence, such as lateral runway excursion.

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

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

In the crosswind example above, an immediate outcome of the hazard could be loss of lateral control followed by a consequent runway excursion. The ultimate consequence could be an accident. The damaging potential of a hazard materializes through one or many consequences. It is therefore important for safety assessments to include a comprehensive account of all likely consequences described accurately and in practical terms. The most extreme consequence, loss of human life, should be differentiated from those that involve the potential for lesser consequences such as increased flight crew workload, passenger discomfort or reduction in safety margins. The description of consequences

according to their plausible outcomes will facilitate the development and implementation of effective mitigation strategies through proper prioritization and allocation of limited resources. **Proper hazard identification leads to appropriate evaluation of their potential outcomes.**

.

1.2 Hazard Identification and Prioritization

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

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

Hazards may be categorized according to their source, or location. Objective prioritization of hazards may require categorizations according to the severity/ likelihood of their projected consequences, which will facilitate the prioritization of risk mitigation strategies, so as to use limited resources in the most effective manner.

1.3 Hazard Identification Methodologies

The three methodologies for identifying hazards are:

1. Reactive – Through analysis of past outcomes or events. Hazards are identified through investigation of safety occurrences. Incidents and accidents are clear indicators of system deficiencies and therefore can be used to determine the hazards that were both contributing to the event or are latent.

2. Proactive – Through analysis of existing or real time situations. This is the primary job of the safety assurance function with its audits, evaluations, employee reporting, and the associated analysis and assessment processes. This involves actively seeking hazards in the existing processes.

3. Predictive – Through data gathering in order to identify possible negative future outcomes or events. Analyzing system processes and the environment to identify potential future hazards and initiating mitigating actions**.**

The following may be considered while engaged in hazard identification process:

a) design factors, including equipment and task design;
b) human performance limitations (e.g. physiological, psychological and cognitive);
c) procedures and operating practices, including their documentation and checklists, and their validation under actual operating conditions;
d) communication factors, including media, terminology and language;
e) organizational factors, such as those related to the recruitment, training and retention of

personnel, the compatibility of production and safety goals, the allocation of resources, operating pressures and the corporate safety culture;

f) factors related to the operational environment of the aviation system (e.g. ambient noise and vibration, temperature, lighting and the availability of protective equipment and clothing);
g) regulatory oversight factors, including the applicability and enforceability of regulations;
h) the certification of equipment, personnel and procedures;
i) performance monitoring systems that can detect practical drift or operational deviations; and
j) human-machine interface factors.

Hazards may be identified through proactive and predictive methodologies or as a result of accident or incident investigations. There are a variety of data sources of hazard identification that may be both internal and external to the organization.

Examples of the internal hazard identification data sources include:

a) normal operations monitoring schemes (e.g. flight data analysis for aircraft operators);
b) voluntary and mandatory reporting systems;
c) safety surveys;
d) safety audits;
e) feedback from training; and
f) investigation and follow-up reports on accidents/ incidents.

Examples of external data sources for hazard identification include:

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

The type of technologies used in the hazard identification process will depend upon the size and complexity of the service provider and its aviation activities. In all cases the service provider's hazard identification process is clearly described in the organization's SMS/ safety documentation. The hazard identification process considers all possible hazards that may exist within the scope of the service provider's aviation activities including interfaces with other systems, both within and external to the organization. Once hazards are identified, their consequences (i.e. any specific events or outcomes) should be determined.

II. RISK ASSESSMENT AND MANAGEMENT

(Note: The following discussion and examples are from the ICAO Safety Management Manual, Third Edition, 2013. The original paragraph numbers were modified to align with the format of this document.)

2. SAFETY RISK

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

a) definition of safety risk
b) safety risk probability
c) safety risk severity
d) safety risk tolerability
e) safety risk management

2.1 Safety Risk

Safety risk is the projected probability (or likelihood) and severity of the consequences or outcomes from an existing hazard or situation. While the outcome may be an accident, an intermediate unsafe event/ consequence may be identified as the most credible outcome. Provisions for the identification of such layered consequences are usually associated with more sophisticated risk mitigation software.

2.2 Safety Risk Probability

The process of controlling safety risks starts by assessing the probability that the consequences of hazards will materialize during aviation activities performed by the organization.

Safety risk probability is defined as the likelihood or frequency that a safety consequence or outcome might occur. The determination of likelihood can be aided by questions such as:

a) Is there a history of occurrences similar to the one under consideration, or is this an isolated occurrence?
b) What other equipment or components of the same type might have similar defects?
c) How many personnel are following, or are subject to, the procedures in question?
d) What percentage of the time is the suspect equipment or the questionable procedure in use?
e) To what extent are there organizational, managerial or regulatory implications that might reflect larger threats to public safety?

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

Figure 1 presents a typical safety risk probability table, in this case, a five-point table. The table includes five categories to denote the probability related to an unsafe event or condition, the description of each category, and an assignment of a value to each category.

It must be stressed that this is an example only and that the level of detail and complexity of tables and matrixes should be adapted to be commensurate with the particular needs and complexities of different

organizations. Also, it should be noted that organizations may include both qualitative and quantitative criteria that may include up to fifteen values.

Likelihood (Probability)	Meaning	Value
Frequent	Likely to occur many time (has occurred frequently)	**5**
Occasional	Likely to occur sometimes (has occurred infrequently)	**4**
Remote	Unlikely to occur, but possible (has occurred rarely)	**3**
Improbable	Very unlikely to occur (not known to have occurred)	**2**
Extremely Improbable	Almost inconceivable that the event will occur	**1**

Figure 1— Safety Risk Probability Table

2.3 Safety Risk Severity

Once the probability assessment has been completed, the next step is to assess risk severity, taking into account the potential consequences related to the hazard.

Safety risk severity is defined as the extent of harm that might reasonably occur as a consequence or outcome of the identified hazard. The severity assessment can be based upon:

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

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

SEVERITY	MEANING	VALUE
Catastrophic	• Equipment destroyed • Multiple deaths	**A**
Hazardous	• A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely • Serious injury • Major equipment damage	**B**
Major	• A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of increase in workload, or as a result of conditions impairing their efficiency • Serious incident • Injury to persons	**C**

Minor	• Nuisance • Operating limitations • Use of emergency procedures • Minor incident	**E**
Negligible	• Little consequence	**F**

Figure 2 — Safety risk severity table

2.4 Safety Risk Tolerability

The safety risk probability and severity assessment process can be used to derive a safety risk index. The index created through the methodology described above consists of an alpha-numeric designator, indicating of the combined results of the probability and severity assessments. The respective severity / probability combinations are presented in the safety risk assessment matrix in *Figure 3.*

The third step in the process is to determine risk tolerability. Safety risks are conceptually assessed as acceptable, tolerable or intolerable. Risks assessed as initially falling in the intolerable region are unacceptable under any circumstances. The probability and/or severity of the consequences of the hazards are of such a magnitude, and the damaging potential of the hazard poses such a threat to safety, that immediate mitigation action is required.

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

Safety risks assessed as initially falling in the acceptable region are acceptable as they currently stand and require no action to bring or keep the probability and/or severity of the consequences of hazards under organizational control.

For example, consider a situation where a safety risk probability has been assessed as occasional (4) and safety risk severity has been assessed as hazardous (B). The composite of probability and severity (4B) is the safety risk index of the consequence.

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

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

Risk Probability	Risk Severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely Improbable 1	1A	1B	1C	1D	1E

Figure 3 — Safety risk assessment matrix

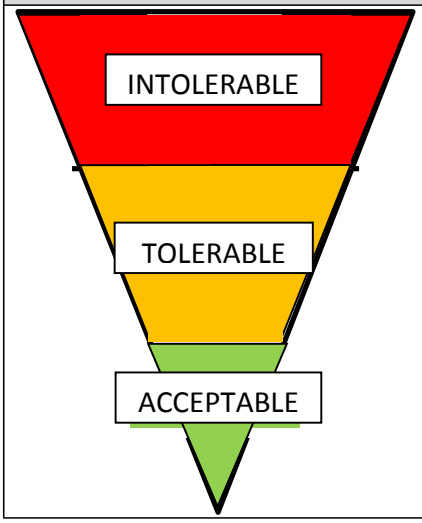
Suggested Criteria	Assessment Risk Index	Suggested Criteria
	5A, 5B, 5C 4A, 4B 3A	Unacceptable under the existing circumstances
	5D, 5E 4C, 4D, 4E, 3B, 3C, 3D 2A, 2B, 2C 1A	Acceptable based on risk mitigation. It may require management decision.
	3E 2D, 2E 1B, 1C, 1D, 1E	Acceptable

Figure 4 — Safety risk tolerability matrix

Risk Index Range	Description	Recommended Action
5A, 5B, 5C 4A, 4B 3A	HIGH Risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the MODERATE or LOW range.
5D, 5E 4C, 4D, 4E, 3B, 3C, 3D 2A, 2B, 2C 1A	MODERATE Risk	Schedule for performance of safety assessment to bring down the risk index to the LOW range if viable.

3E **2D, 2E** **1B, 1C, 1D, 1E**	**LOW Risk**	Acceptable as is. No further risk mitigation required.

Alternate to Figure 4 — Safety risk tolerability matrix

2.5 Risk Mitigation Strategy

A risk mitigation strategy may involve one of the approaches described above, or may include multiple approaches. It is important to consider the full range of possible control measures to find an optimal solution. The effectiveness of each alternative strategy must be evaluated before a decision can be taken. Each proposed safety risk mitigation alternative should be examined from the following perspectives:

a) ***Effectiveness.*** The extent to which the alternatives reduce or eliminate the safety risks Effectiveness can be determined in terms of the technical, training and regulatory defenses that can reduce or eliminate safety risks.

b) ***Cost/benefit.*** The extent to which the perceived benefits of the mitigation outweigh the costs.

c) ***Practicality.*** The extent to which the mitigation is implementable and appropriate in terms of available technology, financial and administrative resources, legislation and regulations, political will, etc.

d) ***Acceptability.*** The extent to which the alternative is consistent with stakeholder paradigms.

e) ***Enforceability.*** The extent to which compliance with new rules, regulations or operating procedures can be monitored.

f) ***Durability.*** The extent to which the mitigation will be sustainable and effective.

g) ***Residual safety risks.*** The degree of safety risk that remains subsequent to the implementation of the initial mitigation, and which may necessitate additional risk control measures.

h) ***Unintended consequences.*** The introduction of new hazards and related safety risks associated with the implementation of any mitigation alternative.

Once the mitigation has been approved and implemented, any associated impact on safety performance provides feedback to the service provider's safety assurance process. This is necessary to ensure integrity, efficiency and effectiveness of the defenses under the new operational conditions.

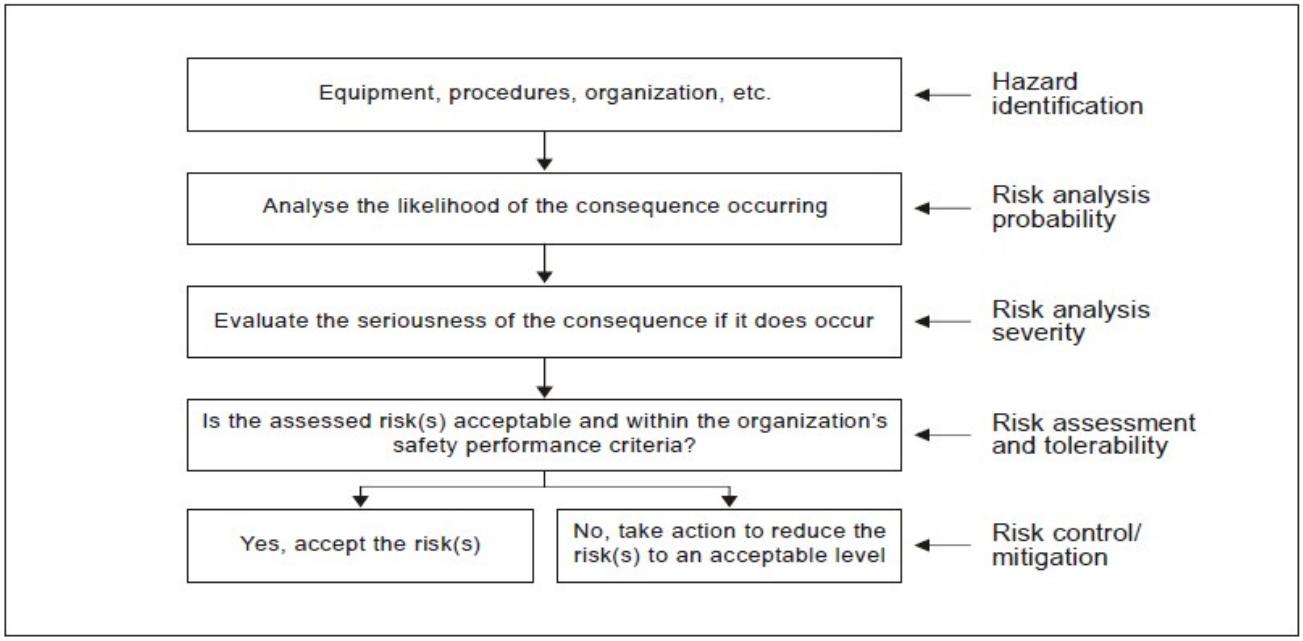


Figure 5 Process of Safety Risk Management

2.5.1 Risk Management Documentation/ Worksheet

Each risk mitigation exercise will need to be documented as necessary. This may be done on a basic spread sheet or table for risk mitigation involving non-complex operations, processes or systems. For hazard identification and risk mitigation involving complex processes, systems or operations, it may be necessary to utilize customized risk mitigation software to facilitate the documentation. Completed risk mitigation documents should be approved by appropriate level of management. (For an example of a basic risk mitigation worksheet, refer to ICAO Doc 9859 3rd ed., Appendix 2 to Chapter 2)

FURTHER READING & REFERENCES

- Bishop, P.G. and Bloomfield, R.E. (1998**) A methodology for safety case development.** [Online]. Available at www.adelard.co.uk/resources/papers/pdf/sss98web.pdf
- Health & Safety Executive (UK). (2005). **More about safety cases.** [Online]**.** Available at www.hse.gov.uk/railways/safetycases.htm
- National Offshore Petroleum Safety Authority. **Safety Case Approach.** Available at http://www.nopsa.gov.au/safety.asp
- Profit, R. (1995). **Systematic Safety Management in the Air Traffic Services**, ISBN 1 85564 470 3. Euromoney Publications PLC: London, UK.
- Risk Engineering Society, Victoria Chapter. (2002) **Safety Case Guideline.** Available for purchase online at www.standards.com.au
- Standards Australia. (2004). **Australian/New Zealand Standard AS/NZS4360:2004: Risk management**. ISBN: 0-7337-5904-1. Available for purchase online at www.standards.com.au