APPENDIX

DRAFT

MANUAL ON SAFETY MANAGEMENT FOR AIR TRAFFIC SERVICES

MANUAL ON SAFETY MANAGEMENT FOR AIR TRAFFIC SERVICES

(Doc XXXX)

DRAFT

Version 0.19

5 September 2003

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION TO SAFETY MANAGEMENT

1.1 ICAO REQUIREMENTS FOR ATS SAFETY MANAGEMENT

1.1.1 Safety has always been an important consideration in all aviation activities. This is reflected in the aims and objectives of ICAO as stated in Article 44 of the *Convention on International Civil Aviation* (Doc 7300), commonly known as the Chicago Convention, which charges ICAO with ensuring the safe and orderly growth of international civil aviation throughout the world.

1.1.2 The standards and recommended practices relating to the implementation by States of safety management programmes for Air Traffic Services (ATS) were introduced in Section 2.26 of Amendment 40 to Annex 11 – *Air Traffic Services*, which became applicable on 1 November 2001. Further provisions relating to the implementation of these safety management programmes, applicable from the same date, are contained in Chapter 2 of *Procedures for Air Navigation Services – Air Traffic Management* (PANS-ATM, Doc 4444).

1.2 STATE RESPONSIBILITIES

1.2.1 The implementation of these provisions has implications for both providers of air traffic services, and the regulatory bodies within the States. It will become clear, from the later chapters of this manual, that the day-to-day management of safety can only be done by the organization providing ATS. Increasingly, ATS is provided by independent corporatized or privatized bodies which are not under the direct control of the State. However, it is the State, as the signatory to the Chicago Convention, which is responsible for implementation of ICAO SARPS within the airspace and at aerodromes for which it has responsibility.

1.2.2 The discharge of this responsibility with regard to the ATS safety management provisions requires first that States put in place the legislative and regulatory provisions needed to provide the authority for requiring ATS providers to implement systematic safety management practices and procedures. It will also be necessary for States to establish appropriate oversight mechanisms to ensure that providers comply with these legislative and regulatory requirements, and that they maintain an acceptable level of safety in their operations.

1.2.3 It is important, even where the regulatory function and the provision of ATS are both under the direct control of the one body (e.g. a civil service department, or a State controlled authority), that a clear distinction be maintained between these two functions.

1.2.4 The formal, systematic procedures and practices for the management of safety are generally referred to collectively as a *safety management system*. The overall ATS safety management programme within a State can therefore be seen as having two components; a safety regulatory and oversight function, which will always be the direct responsibility of the State, and an active safety management component, implemented through the safety management system(s) of the ATS provider(s).

1.3 PURPOSE OF THE MANUAL

1.3.1 The purpose of this manual is to assist States in implementing the provisions of Section 2.26 of Annex 11 and Chapter 2 of the PANS-ATM, by providing guidance concerning both the regulatory requirements and the implementation of safety management systems by ATS providers.

1.3.2 Extensive literature is available concerning safety and safety management systems. This manual is not intended to be a comprehensive text on safety management. Its aim is to provide an

introduction to the functions of a safety management system and the associated supporting organizational requirements, with a particular emphasis on the application of safety management techniques to ATS.

1.3.3 The approach to safety management recommended in the manual is based on what has come to be regarded as "best practice" in industries where safety management has long been an integrated part of their operations.

1.4 BASIC CONCEPTS OF SAFETY AND RISK

1.4.1 In order to understand the procedures used in safety management, it is necessary to examine exactly what is meant by "safety". In the aviation context, safety is generally thought of, by the public, as being an absence of aircraft accidents. While the elimination of accidents would be desirable, it must be recognized that such "perfect safety" is an unachievable goal; failures and errors can still occur, in spite of the best efforts to avoid them. This is true of all forms of human endeavour, and will be discussed in more detail in Chapter 3.

1.4.2 While it is not possible to completely eliminate the likelihood of harm or damage, it is possible to control the processes which could lead to hazardous events, and so ensure that the likelihood of being exposed to harm or damage is as low as possible. These concepts of what is meant by "safe" are reflected in the following definition of safety (which is also used in the *Safety Oversight Audit Manual* (Doc 9735)).

> ***Safety***. A condition in which the risk of harm or damage is limited to an acceptable level.

1.4.3 The achieved level of safety can only be assessed after the event. A good past safety record is not a guarantee of freedom from future accidents, particularly given that major aircraft accidents in which the ATS system is a contributory factor are rare events. An effective safety management system should adopt a proactive approach, incorporating procedures for:

a) Identification, before an accident occurs, of potential system weaknesses which could contribute to an accident;

b) Estimation, in advance, of the risk of accidents occurring; and

c) Implementation of risk mitigation measures to reduce risk where unacceptable levels of risk have been identified.

1.4.4 It is important to note that the acceptability of risk is not the same for all types of accidents. In general, society will tolerate a higher level of risk for occurrences where each event may result in a small number of deaths (e.g. automobile accidents), than for those where a single event may result in a large number of deaths (e.g. a nuclear power station accident). Because accidents involving commercial aircraft can potentially result in very large death tolls, the acceptable level of risk for such accidents is very low.

1.4.5 How risk is expressed, and the factors to consider in determining what constitutes an "acceptable" risk of harm or damage, are addressed in Chapter 2. The assessment of risk and the use of mitigation measures to control risk are addressed in Chapter 6.

1.4.6 The practices and procedures necessary to ensure that risk is acceptably low collectively form the basis of the organization's safety management system. It should, however, be noted that the effective implementation of the procedures and practices requires more than just publishing them in a manual of ATS operations, or similar document. It can also require a change in the attitudes of staff at all

levels in the organization, in order to achieve what is generally called a "safety culture". This, and other organizational issues critical to effective safety management, are addressed in Chapter 4.

1.5 THE SCOPE OF ATS SAFETY MANAGEMENT

1.5.1 An ATS safety management system can only provide a means of controlling those hazards which originate within the ATS system, or in which some element of the ATS system is a contributory factor.

1.5.1.1 As an example of the latter, the ATS system cannot directly address the causes of an in-flight emergency due to an aircraft system malfunction. However, it is important that the ATC procedures for handling an in-flight emergency do not contribute to the possibility of the emergency resulting in an accident.

1.5.2 Within this manual, the term *ATS System* includes all of the people, technology and procedures required for the provision of ATS, and the interfaces between them. The scope of the ATS system is illustrated in Figure 1-1.

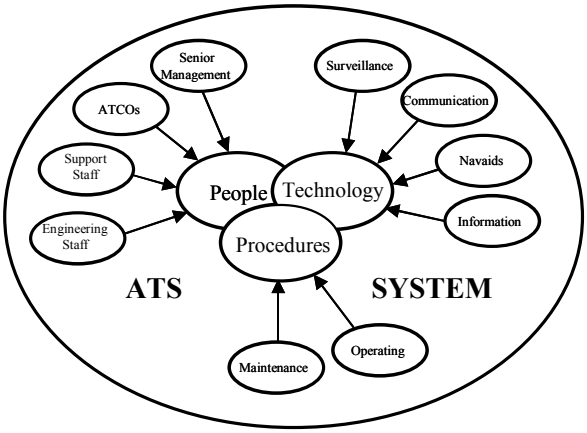


Figure 1-1. The ATS System

1.5.3 It should be noted that in some circumstances, not all of the functions shown in Figure 1-1 will necessarily be under the direct control of the ATS provider. For example, communications services may be provided by a separate telecommunications authority. The evaluation of the overall safety of the system must, nevertheless, take into account any impact on safety which could arise from such externally provided services.

CHAPTER 2 - MEASURES OF RISK AND SAFETY PERFORMANCE TARGETS

2.1 INTRODUCTION

2.1.1 Before commencing any form of assessment to determine whether the safety performance of a system, or the safety impact of planned changes to it, is acceptable, a decision must be made concerning what criteria will be used to judge acceptability. The ICAO provisions relating to safety management, for both aerodromes and ATS, incorporate requirements relating to the establishment and use of such criteria.

2.1.2 Annex 11, paragraph 2.26.2, requires States to establish the *acceptable level of safety and safety objectives* applicable to the provision of ATS within their airspace and at their aerodromes.

2.1.3 The corresponding requirement in respect of non-ATS operations at aerodromes is contained in the *Manual on Certification of Aerodromes* (Doc 9774). Appendix 1 specifies the particulars to be included in State regulations concerning the content of an Aerodrome Manual. Part 5 of these model regulations requires, *inter alia*, the setting of safety performance targets.

2.1.4 While the terminology is different, the underlying concepts behind these requirements are the same. Both refer to the need, prior to undertaking any assessment of safety, to specify in advance the criteria on which the acceptability of the safety performance will be based.

Note.- There is not total standardization in the terminology found in texts on risk management for these concepts. Other terms which may be encountered include "risk criteria", "acceptability criteria" and "tolerability criteria".

2.1.5 This manual will, for standardization, and as a step towards the goal of a unified system-wide approach to safety management, adopt a performance oriented approach to this question of the how levels of safety should be expressed. This is in line with the *Global ATM Operational Concept* contained in the report of the Eleventh Air Navigation Conference (Montreal, 22 September to 3 October 2003). This concept emphasized the importance of establishing performance indicators to assess whether the ATM system was meeting the expectations of the aviation community and the general public. Safety performance was seen as the most important of these indicators.

2.1.6 The terminology used in this manual will be:

Safety Performance Indicator. A measure (or metric) used to express the level of safety performance required or achieved in a system.

Safety Performance Target. The required level of safety performance for a system. A safety performance target comprises one or more safety performance indicators, together with desired outcomes expressed in terms of those indicators.

2.1.7 A safety performance target, as defined above, is a criterion against which the results of monitoring of the safety performance of a system are assessed.

2.1.8 It is necessary to draw a distinction between the criteria used to assess the safety performance as assessed through monitoring, and the criteria used for the assessment of the safety of new systems or procedures. This will be addressed in more detail later in this chapter, but for now, it should be noted that this form of safety assessment often employs a hazard analysis approach. A hazard analysis

approach involves estimating qualitatively or quantitatively the degree of risk associated with each identified hazard, and incorporating mitigation measures, as necessary, to ensure that the risk associated with each hazard is adequately controlled. The hazard analysis approach does not necessarily produce quantitative estimates of safety which can be directly compared to the same safety performance indicators which are used to assess the results of monitoring.

2.1.9 To make this distinction clear, the term *safety assessment criteria* will be used when referring to this form of safety assessment. This is defined as follows:

> *Safety Assessment Criteria*. The set of quantitative or qualitative criteria to be used in a safety assessment to determine the acceptability of the assessed level of safety.

2.2 THE CONCEPT OF RISK

2.2.1 Safety was defined in Chapter 1 as a condition in which the risk of harm or damage is limited to an acceptable level. Since safety is defined in terms of risk, any measure of safety performance must necessarily involve the concept of risk.

2.2.2 There is no such thing as absolute safety. Before any assessment of whether or not a system is safe can be made, it is first necessary to determine what is an acceptable level of risk.

2.2.3 Risks are often expressed as probabilities, however the concept of risk involves more than this. To illustrate this with a hypothetical example, let us assume that the probability of the supporting cable of a cable-car failing and allowing the car to fall was assessed as being the same as the probability of slipping and falling down stairs. While the probabilities of the events occurring may be the same, the consequences of the cable car accident are much more severe. Risk is therefore two dimensional. Evaluation of the acceptability of a given risk associated with a particular hazard must always take account of both the likelihood of occurrence of the hazard, and the severity of its consequences.

2.2.4 The perceptions of risk can be derived into three broad categories:

a) Risk that are so high that they are unacceptable;

b) Risk that are so low that they are acceptable; and

c) Risks in between these two categories, where consideration needs to be given to the various tradeoffs between risks and benefits.

2.2.5 If the risk does not meet the pre-determined acceptability criteria, an attempt must always be made to reduce it to a level that is acceptable, using appropriate mitigation procedures. If the risk cannot be reduced to or below the acceptable level, it may be regarded as tolerable if:

a) the risk is less than the pre-determined unacceptable limit;

b) the risk has been reduced to a level which is as low as reasonable practicable (ALARP); and

c) the benefits of the proposed system or changes are sufficient to justify accepting the risk.

Note.- All three of the above criteria should be satisfied before a risk is classed as tolerable.

2.2.5.1 Even where the risk is classed as acceptable, if any measures which could result in further reduction of the risk are identified, and these measures require little effort or resources to implement, they should be implemented.

2.2.6 The acronym ALARP is often used to describe a risk which has been reduced to a level that is as low as reasonably practicable. In determining what is “reasonably practicable” in this context,

consideration should be given to both the technical feasibility of further reducing the risk, and the cost. All such cases should be evaluated individually.

2.2.7 Showing a system is ALARP means that any further risk reduction is either impracticable or grossly out-weighted by the costs. It should, however, be remembered that when an individual or the society 'accepts' a risk, this does not mean that the risk is eliminated. The risk remains, however, the individual or society has accepted that the residual risk is sufficiently low that the risk is outweighed by the benefits.

2.2.8 These concepts are illustrated diagrammatically in the tolerability of risk (TOR) triangle shown in Figure 4-1. (In this diagram, the degree of risk is represented by the width of the triangle.)

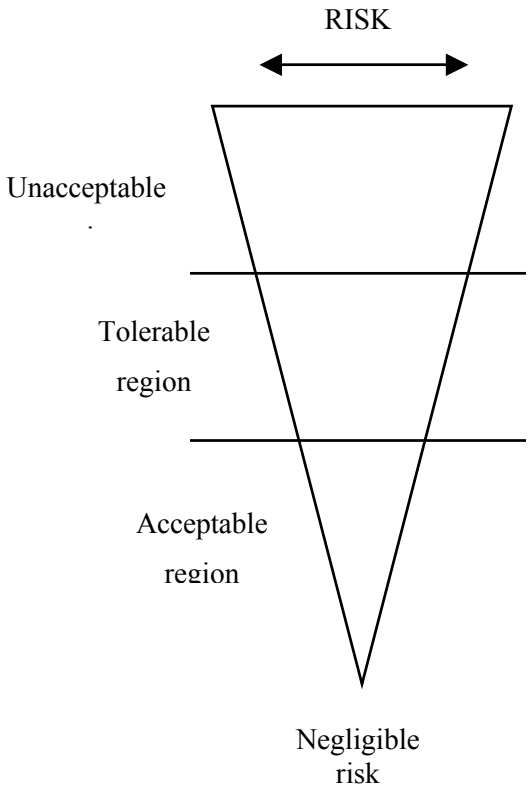


Figure 2-1. Tolerability of Risk (TOR) Triangle

2.3 INDIVIDUAL RISK VERSUS SOCIETAL RISK

2.3.1 The acceptability of a risk can be assessed from two different points of view.

2.3.1.1 The first is, does an individual who is exposed to the risk judge the risk to be acceptable? Risk criteria developed from this perspective are called *individual risk criteria*.

2.3.1.2 The second is, how does society in general view the risk? This involves society's perception of the acceptability of events which may cause death and injury to persons other than themselves. Risk criteria developed from this perspective are called *societal risk criteria.*

Individual risk criteria

2.3.2 Individual risk criteria are set and assessed on the basis of the risk to a single individual. The severity of the consequences of an event are therefore assessed in terms of the degree of harm which an individual could suffer, but do not take account of the number of people who may be affected any given event. The concepts underlying individual risk criteria are those involved in the processes used by an individual in deciding whether or not to undertake a particular activity.

2.3.3 In practice, each individual will make his or her own judgement as to what they regard as an acceptable level of risk. However, the inherent degree of risk aversion can vary quite markedly from one person to another. An individual's perception of the risk can also be influenced by his or her familiarity with the activity generating the risk.

2.3.4 An example of this is the degree of unease which people who do not fly frequently often feel about undertaking a flight, although they feel quite comfortable travelling by car, which accident statistics invariably show to be the higher risk activity. People will also often accept a higher degree of risk in activities which they are undertaking voluntarily compared to what they will accept when the risk is being imposed on them as the result of some activity over which they have no control.

2.3.5 Acceptability criteria based on individual risk cannot therefore be based on the risk as assessed by any single person, but rather should be based on how the risk would be viewed by a hypothetical individual representative of the population for which the risk acceptability is being assessed.

2.3.6 An individual's risk of suffering harm from a particular activity in any one year will depend on the degree of exposure to that activity. When using annual risk measures, the exposure of aircraft crew to flying is considerably more than that of most passengers. The crew, in this instance, would be regarded as the *critically exposed group*. The risk to the flying public could be assessed based on a hypothetical typical passenger; for example, a business passenger who flies 100 hours per year.

2.3.7 Individual risk criteria are generally set by examining attitudes to various activities for which statistical data on deaths resulting from these activities is available. Two key items are road deaths, and deaths resulting from lightning strike. It is generally accepted that anything involving a risk greater than the risk of being killed in a road is totally unacceptable. The likelihood of this varies markedly from one country to another, but for the major western nations is typically of the order of 10^{-4} per year (or one chance in 10,000). The likelihood of being killed by lightning, by comparison, is of the order of 10^{-7} per year (or one chance in 10,000,000). This is regarded as a negligible risk.

Societal risk criteria

2.3.8 *Societal risk criteria* address the question of what the society regards as an acceptable risk. In assessing individual risk, the severity dimension of the risk was based solely on the severity of the outcome for a single individual. However, as already noted in Chapter 1, the way in which society in general views risk is also influenced by the number of people who could suffer harm as the result of the occurrence of a particular event. The assessment of the severity of the consequences of a hazard will therefore need to take this into account.

2.3.9 This basic difference between individual and societal tolerance of risk is easily understood, but this still does not answer the question of what is acceptable. A number of States have published criteria indicating what can be regarded as acceptable level of risk, within their particular societies. Much of the original work on these matters originated from the nuclear and chemical industries, but these criteria could be used as guidance for aviation related accidents as well. Figure 4-2 shows examples of such criteria. The "severity" measure used is number of fatalities, therefore diagrams of this type are referred to as *fN curves*, since they take the form of a graph of frequency of occurrence (f) versus number of fatalities (N).

Note.- In some texts on risk management, there will be references to consequences other than fatalities. for example, in assessing the risks associated with a chemical plant, it could be necessary to take into account other outcomes, such as environmental damage or long term non-fatal health effects. However, for ATS safety assessment, this is not generally necessary.

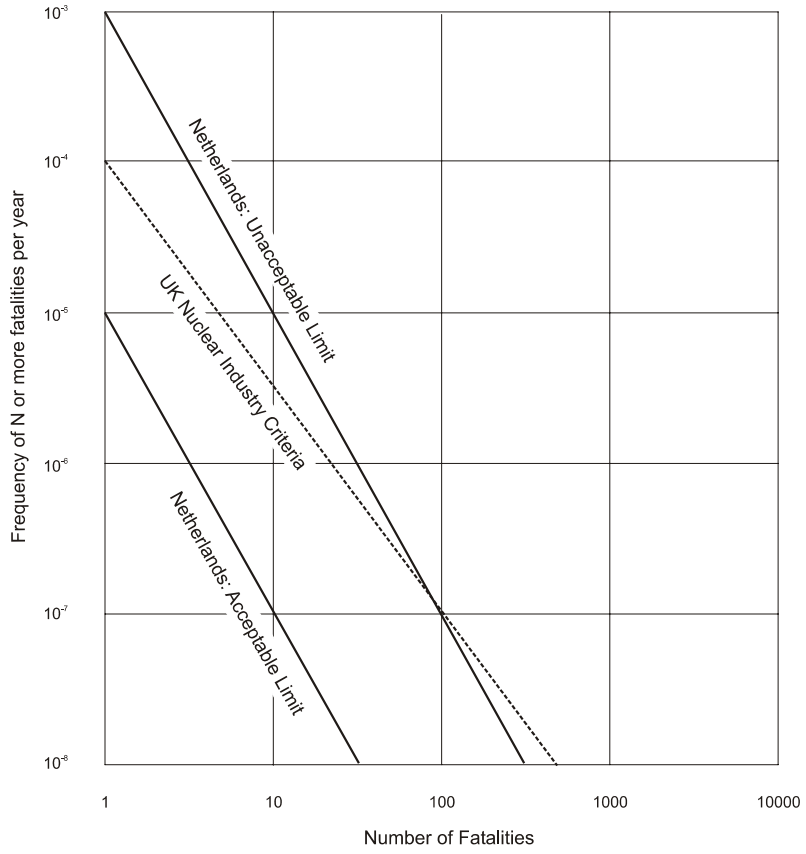


Figure 2-2. Examples of societal risk criteria

(Based on a diagram from Chapter 4 of Robinson, R. M. *et al*, *Risk and Reliability – an introductory text*)

2.3.10 The acceptability criteria adopted may vary from one State to another. Figure 2-2 shows examples of societal risk criteria adopted by two States. The U.K. nuclear industry criteria are specified by a single line, so they effectively define a "pass/fail" criterion for each level of potential fatalities. The Netherlands criteria, on the other hand, specify separate acceptable and unacceptable limits. The region between these two lines is the tolerable region, within which the ALARP principle must be applied.

When applying societal risk criteria in aviation, it is important to recognize that public perception of risk is based on the total risk, from all causes, associated with flying, rather than the risk associated with separate components of the aviation system. These criteria would therefore be appropriate as guidance in setting global, regional or national safety performance targets for the overall aviation system. However, the risk associated with the introduction of new ATS procedures, or changes to airport operating procedures, could not be compared directly to societal acceptability criteria, since the risk associated with each of these represents only a part of the total risk.

2.4 SAFETY PERFORMANCE INDICATORS

2.4.1 *Safety performance indicators* are generally expressed in terms of the frequency of occurrence of some event causing harm. Typical measures which could be used include:

- fatal aircraft accidents per flight hour;
- fatal aircraft accidents per movement;
- fatal aircraft accidents per year;
- serious incidents per flight hour;
- fatalities due to aircraft accidents per year.

2.4.2 Risk measures expressed in terms of fatal aircraft accidents are indicators of individual risk, since they do not take account of the number of people affected. A risk measure expressed in terms of number of fatalities would be more appropriate for expressing societal risk.

2.4.3 These risk measures specify only the frequency of occurrence, whereas we noted earlier that risk involves both frequency and severity. In this form of risk measure, the severity is implicit in the occurrence whose frequency is being specified. Therefore it could be expected that an acceptable limit expressed in terms of incidents would be significantly different from a limit expressed in terms of fatal aircraft accidents.

2.5 SAFETY PERFORMANCE TARGETS

2.5.1 In order to set a safety performance target, it is necessary to first decide on an appropriate safety performance indicator, and then to decide on what represents an acceptable outcome. The safety performance indicator chosen needs to be appropriate for the application, taking into account the issues raised in section 2.4.

2.5.2 ICAO has set a global safety performance target in the specification of the objectives of the Global Aviation Safety Programme (GASP). These are:

a) to reduce the number of accidents and fatalities, irrespective of the volume of air traffic; and

b) to achieve a significant decrease in worldwide accident rates, placing the emphasis on regions where these remain high.

2.5.3 Regional and national safety performance targets for ATS should take these objectives into consideration, to ensure that they will contribute to the achievement of these global objectives.

Choice of the safety performance indicator

2.5.4 There is no single safety performance indicator which is appropriate in all circumstances. The indicator chosen to express a safety performance target must be matched to the application in which it will be used, so that it will be possible to make a meaningful evaluation of safety in the same terms as those used in defining the safety performance target.

2.5.5 The safety performance indicator(s) chosen to express global, regional and national targets will not generally be appropriate for application to individual ATS units. The ICAO global target, for example, is expressed in terms of accidents, However, aircraft accidents are relatively rare events. Even at the global level, accident rates vary considerably from year to year. An increase or decrease in accidents from on year to the next does not necessarily indicate a change in the underlying level of safety.

2.5.6 Observed accident rates are even less useful as an indicator of safety when applied to individual aerodromes or FIRs. For a single FIR, for example, the expected time between en-route

accidents could be in excess of 100 years. When we are trying to achieve safety levels of this order, the absence of accidents, even over 10 or 20 years, does not necessarily mean that there are no potential safety deficiencies in the system which, given particular set of circumstances, could lead to an accident.

2.5.7 The frequency of occurrence of certain types of incidents may provide a better indicator of the "safety health" of an ATS system. While these will not have resulted in a fatal accident, given a slightly different set of circumstances, they may have. Incidents may therefore reveal the existence of latent failures in the system.

2.5.8 There is also a need to consider the possibility that there may be other occurrences within the system which do not come within the definition of an incident, but could have safety implications. This manual will therefore use the term *safety occurrence* for any event which could have a negative impact on safety.

2.5.9 An indicator based on safety occurrences is only as good as the reporting or monitoring systems through which such occurrences are recorded. For this to be effective, the culture of the organization must encourage the filing and recording of the required reports. Examples of possible impediments to this are:

a) the willingness of individuals to submit reports can affected by their perceptions of the likely consequences; and

b) the use of safety occurrences as a performance indicator could potentially result in a reluctance to see the results published, leading to, for example, actions such as individual managers discouraging the filing of reports, because of a perceived adverse impact on their unit.

2.5.10 These issues are closely connected with the concept of a safety culture. The requirements for an effective system for reporting safety occurrences will be discussed further in Chapter 5.

Setting the desired outcome

2.5.11 The second part of the process of setting a safety performance target is deciding on the desired outcome. This may be expressed either in absolute or relative terms. The ICAO global target set within the GASP objectives is an example of a relative target. A relative target could also incorporate a desired percentage reduction in accidents or particular types of safety occurrences in a defined time period.

2.5.12 In setting safety performance targets based on fatal aircraft accidents for use at the national or regional level, and encompassing all causes, use could be made of societal risk acceptability criteria which have been developed for other industries.

2.5.13 If fatal accidents are to be used as the safety indicator for application to a limited aspect of the overall system, such as a instrument approach or departure procedures, or an en-route procedures, the individual risk criteria developed for other industries could be used as a guide. Another technique which has been used for this sort of application is to look at historical data. Accidents rates have generally been decreasing over time, so it is possible to periodically revise safety performance targets to ensure that, if the targets are achieved, there will be a continuing downward trend in accident rates.

2.5.14 Whenever quantitative safety performance targets are set, it must be possible to measure, or estimate, the achieved level of safety in quantitative terms. If a target of this type is to be applied to en-route operations within a single FIR, or instrument approaches at a single aerodrome then, as noted in 2.5.5 and 2.5.6, the expected frequency of accidents is so low that data on actual accidents will not give a valid indication of whether the target is being met.

2.5.15 Quantitative targets are used, for example, in assessing the on-going safety of operations in RVSM airspace. However, in this case, the assessment of the achieved level of safety is done using mathematical collision risk models which can estimate the expected rate of accidents from data on aircraft height deviations which did not result in an accident. Similar models are used in the estimation of collision risk as the result of lateral deviations from track in the north Atlantic MNPS airspace, and oceanic airspace where RNP based separation minima are used.

2.5.16 The techniques used in this form of safety assessment are beyond the scope of this manual. Further information on collision risk models can be found in the *Manual on airspace planning methodology for the determination of separation minima*, (Doc 9689).

2.5.17 In any application of quantitative safety targets to components of the overall system, it is necessary to consider the impact on the entire system. If the overall safety performance target for a system is to be met, it is necessary that the contribution to the overall risk of each of the components of the system be less than the acceptable level of risk specified in the overall safety performance target.

2.5.18 This process of determining what are appropriate acceptable risk criteria for components of a system is sometimes referred to as partitioning the risk.

CHAPTER 3 - FACTORS AFFECTING SYSTEM SAFETY

3.1 INTRODUCTION

3.1.1 This section considers the factors affecting the safety of ATS systems from two points of view; first, a discussion of those factors which may result in situations in which safety is compromised, and second, an examination of how an understanding of these factors can be applied to the design of ATS systems to reduce the likelihood of occurrences which may compromise safety.

3.1.2 The search for factors which could compromise safety will have to include all levels of the organization responsible for the provision of air traffic services, not just the operational levels. As it will be introduced in chapter 4, the need for safety starts from the highest level of the organization.

3.1.3 Safety is the primary goal of the ATS system. Any situation, which results in safety standards being compromised, can therefore be considered a failure of the system to meet this primary goal. We will commence the examination of factors affecting safety with an examination of the possible sources of such failures.

3.2 SOURCES OF SYSTEM SAFETY

3.2.1 A system failure is any occurrence, which results in the inability to provide the level of service, which the system is intended to provide.

3.2.2 It should be noted here that failure of one element of the system does not always result in a system failure as defined above. If an alternate that provides the required level of service is available, and there is no interruption of service in the changeover, the system as a whole has not failed.

3.2.3 A failure rarely has a single cause. There will always be at least one (and often more than one) initiating event. Initiating events occur close in time to the failure, and are obviously linked to it. There are usually also a number of contributory events. Sometimes the link between contributory events and the failure may be obvious (at least after the event), however there is another group of contributory events where the link is not always obvious. These may include decisions regarding system design or organizational policy, taken months, or even years, before the failure.

3.2.4 The causal factors for a system failure may be related to equipment, or the result of human error, or a combination of both.

3.2.5 In this document, the term *failure* will be reserved for system failures as defined above. The term *fault* will be used to describe malfunctions in equipment or facilities. The term *error* will be used only in the context of human error.

> A *system failure* is any occurrence, which results in the inability to provide the level of service, which the system is intended to provide.
>
> A *fault* is any occurrence, which results in an equipment malfunction.
>
> An *error* is a failure in human performance.

3.3 ACTIVE AND LATENT FAILURES

3.3.1 When a failure actually occurs in a system, its results can be observed. Such a failure is classified as an *active failure*. The term *latent failure* is used to describe the existence, in a system, of conditions which, given a particular sequence of triggering events, could lead to a failure of the system.

3.3.2 The direct causes of active failures are generally the result of equipment faults or errors committed by operational personnel. Latent failures, however, always have a human element. They may be the result of undetected design flaws. They may be related to unrecognized consequences of officially approved procedures. There have also been a number of cases where latent failures have been the direct result of decisions taken by the management of the organization. For example, latent failures will often be present when the culture of the organization, which may not always be in accordance with the organizations officially stated policy, encourages taking short cuts rather than always following approved procedures. The direct cause of a failure associated with taking short cuts would be the failure of a person at the operational level to follow correct procedures. However, if there is general acceptance of this sort of behaviour amongst operational personnel, and management are either unaware of this or take no action, there is a latent failure in the system at the management level.

3.4 EQUIPMENT FAULTS

3.4.1 The determination of the likelihood of system failures due to equipment faults is the domain of reliability engineering. The reliability engineering approach assesses the probability of system failure by analyzing the failure rates of individual components making up a piece of equipment The causes of the component failures include electrical, mechanical and software faults.

3.4.2 A safety analysis must consider more than just the likelihood of failures during normal operation of the system. In particular, it must consider the effects of continued unavailability of one element of the system on other aspects of the system, and the implications of any loss of functionality or loss of redundancy as the result of equipment being taken out of service for routing maintenance. It is therefore important that the scope of the analysis, and the definition of the boundaries of the system for purposes of the analysis, be sufficiently broad that all necessary supporting services and activities are included.

3.4.3 As a minimum, a safety assessment should consider the following sources of faults:

- Hardware faults
- Software malfunctions
- Environmental conditions
- Dependencies on external services
- Operating and maintenance procedures.

3.4.4 It is possible that a single fault may cause the loss of more than one service, or system function. An example would be a situation where both primary and secondary VHF communications equipment shared common primary and stand-by power supplies. In the event of a failure of both primary and stand-by power, both primary and secondary VHF would not be available. Such multiple failures resulting from a single fault are called *common mode failures*.

3.4.5 The above example is a very simple one. However, the linkages, which can cause a common mode failure, are not always obvious. The possibility of common mode failures needs careful investigation in the early stages of system design.

3.4.6 The techniques for estimating the probability of overall system failure as a result of equipment faults and estimating parameters such as availability and continuity of service are well established and are described in standard texts on reliability and safety engineering. These issues will not be addressed further in this manual.

3.5 HUMAN ERROR

Human performance

3.5.1 An error occurs when the outcome of a task being performed by a human is not the intended outcome. In order to understand human error and how it occurs, it is therefore necessary to understand the mechanisms involved in human performance.

3.5.2 The way in which a human operator approaches a task depends on the nature of the task, and how familiar with it the operator is. There are three generally recognized levels of performance; the *skill-based* level, the *rule-based* level, and the *knowledge-based* level. The characteristics of each of these performance levels are shown in Table 3-1.

Note.- The term "rule" as used here has a specific meaning (explained in Table 3-1) in the context of human performance. It should not be confused with more general meanings of the word in everyday usage.

Performance level	Characteristics of performance at this level
Skill-based	This is the method used to perform tasks, which are routine, and highly practiced. The performance of such tasks is largely automatic. No conscious decision-making is required.
Rule-based	This is a method used where the person has encountered the problem before, and already knows a suitable method for achieving a solution. The rules referred to here comprise a series of actions for solving a problem. Performance at this level involves recalling rules describing solutions, which have been used previously, consciously identifying a rule, which is appropriate to the situation, and correctly applying the actions specified by the rule.
Knowledge-based	Knowledge-based performance involves reasoning based on knowledge of general principles in order to develop a course of action. This is the approach adopted when a new situation, for which the person does not have a ready-made answer, is encountered. If a problem can be satisfactorily resolved using skill-based or rule-based methods, a person will generally not resort to knowledge-based reasoning.

Table 3-1. Levels of human performance

3.5.3 There is not always a clear distinction between these different levels of performance. For example, a situation may not exactly fit one of the rules describing previous solutions, but if the conditions are similar, it may be possible to develop a course of action by modifying an existing rule. This will generally be a quicker and simpler process than developing a totally new solution using knowledge-based reasoning, and would involve elements of both rule-based and knowledge-based performance

Errors and violations

3.5.4 Before discussing the various types of errors, there is a need to draw a distinction between errors and violations. Both can lead to a failure of the system. Both can result in a hazardous situation. The difference lies in the intent.

3.5.5 A violation is a deliberate act, while an error is unintentional. Take, for example, a situation in which a controller allows an aircraft to descend through the level of a cruising aircraft when the DME distance between them is 18 NM, and this occurs in circumstances where the correct separation minimum is 20 NM. If the controller made a mistake in calculating the difference in the DME distances advised by the pilots, this would be an error. If the controller calculated the distance correctly, and allowed the descending aircraft to continue through the level of the cruising aircraft knowing that the required separation minimum did not exist, this would be a violation.

3.5.6 Violations should not be tolerated. There have been a number of accidents where the existence of a corporate culture, which tolerated or in some cases even encouraged taking short cuts rather than following published procedures in full, has been a major contributory cause in an accident. The ICAO *Human Factors Digest No. 10 – Human Factors, Management and Organization* (Circular 247) contains a number of examples of such accidents.

Classification of errors

3.5.7 Human actions, other than automatic or reflex actions, can generally be described as the execution of a series of steps according to some pre-determined plan. Errors may first be classified according to whether they occur at the planning stage, or during the execution of the plan. Errors in the formulation of the plan of action will be the result of *mistakes* at either the rule-based or knowledge-based level. Errors in the execution of the plan will be the result of *slips or lapses* at the skill-based level.

3.5.8 The human factors literature on human error generally draws a distinction between slips and lapses. A slip is an action which is not carried out as planned, and will therefore always be observable. A lapse is a failure of memory, and may not necessarily be evident to anyone other than the person who experienced the lapse.

	Characteristics		
	Skill-based slips and lapses	**Rule-based mistakes**	**Knowledge-based mistakes**
Type of activity	Routine actions	Problem-solving activities	
Focus of attention	Something other than the task in hand	Directed at problem-related issues	
Predictability	Largely predictable		Variable
Situational factors	Low to moderate importance. Frequency of prior use of the action or rule the dominant factor		External factors likely to dominate
Ease of detection	Detection usually rapid and effective	Difficult, and often achieved only as the result of external intervention	

Table 3-2. Characteristics of different classes of errors

3.5.9 An understanding of these various ways in which errors may arise will help in identifying possible sources of error in an ATM system. The characteristics of the different classes of errors are listed in Table 3-2

Skill-based slips and lapses

3.5.10 Actions at the skill-based level are routine, highly practiced tasks, which are carried out in a largely automatic fashion, except for occasional checks on progress. Slips and lapses at the skill-based level can occur as the result of:

- *Attentional slips* occur as the result of a failure monitor the progress of a routine action at some critical point. These are particularly likely when the planned course of action is similar to a routinely used procedure, but not identical. If a distraction occurs, or attention is allowed to wander, at the critical point where the action differs from the usual procedure, the result can be that the operator will follow the usual procedure rather than the one intended in this instance.
- *Memory lapses* occur when we either forget what we had planned to do, or omit an item in a planned sequence of actions.
- *Perceptual errors* are errors in recognition. They occur when we believe we saw or heard something which is different from the information actually presented.

Rule-based mistakes

3.5.11 Rule-based problem solving involves first the identification of a set of procedures, known and used before (these constitute the rule), which will be appropriate to the problem in hand. Mistakes at the rule-based level can occur in two ways; the application of a rule which is not appropriate to the situation, or the correct application of a rule which is flawed.

- *Misapplication of good rules*. This usually happens when an operator is faced with a situation which exhibits many features common to the circumstances for which the rule was intended, but with some significant differences. If the significance of the differences is not recognized, an inappropriate rule may be applied.
- *Application of bad rules*. This involves the use of a procedure which past experience has shown to work, but contains unrecognized flaws. If such a solution works in the circumstances under which it was first tried, it may become part of the individual's regular approach to solving that type of problem.

3.5.12 Note that both types of rule based mistake relate to the appropriateness of the rule which is selected. If an operator selects a correct rule for the situation, but an error in the execution of the rule occurs, e.g. a necessary step is overlooked, this would be classified as a slip or lapse, rather than a rule-based error.

Knowledge-based mistakes

3.5.13 Knowledge-based reasoning is generally used only when a person does not have a ready-made solution based on previous experience and/or training. Developing a solution to a problem using this method will inevitably take longer than applying a rule-based solution, as it requires reasoning based on knowledge of basic principles. Mistakes can occur because of lack of knowledge, or because of faulty reasoning. The application of knowledge-based reasoning to a problem will be particularly difficult in circumstances where the controller is busy, as his or her attention is likely to be diverted from the

reasoning process to deal with other issues. The probability of a mistake occurring becomes greater in such circumstances.

3.6 DESIGN OF SAFETY SYSTEMS

3.6.1 The complete elimination of risk is an unachievable goal. Even in organizations with the best of training programmes and a positive safety culture, human operators will occasionally make errors. The best-designed and maintained equipment will occasionally fail. The ATS system must therefore take account of the inevitability of errors and failures. It important that the system be designed and implemented in such a way that, to the maximum extent possible, errors and equipment failures will not result in an accident. A system, which meets these criteria, is called an *error tolerant system*.

3.6.2 The hardware and software components of an ATS system are generally designed to meet specified levels of availability, continuity and integrity. The techniques for estimating system performance in terms of these parameters are well established. When necessary, redundancy can be built in to the system, to provide alternatives in the event of failure of one or more elements of the system.

3.6.3 The performance of the human element of an ATS system cannot be specified as precisely as this, however it is essential that the possibility of human error be considered as part of the overall design of the system. This requires an analysis to identify potential weaknesses in the procedural aspects of the system, taking into account the various shortcomings in human performance described in the previous section. The analysis should also take into account the fact that accidents rarely have a single cause. As noted earlier, they are usually the result of a sequence of events, so the analysis needs to consider combinations of events and circumstances, to identify sequences, which could possibly result in safety being compromised.

3.6.4 Any weaknesses in the system, which could lead to an accident, represent latent failures in the system (actual or proposed). Maurino *et al.* (1995) describe a matrix approach, which may be used for the identification of latent failures.

3.6.5 Developing a safe and error tolerant system requires that the system contains multiple defences, barriers and safeguards, to ensure that, as far as possible, no single failure or error will result in an accident, and that when a failure or error occurs, it will be recognized, and remedial action taken, before a sequence of events leading to an accident can develop. The need for a series of defences, rather than just a single defensive layer, arises from the possibility that the defences themselves may not always work perfectly. This design philosophy is called *defences-in-depth*.

3.6.6 Failures in the defensive layers of an operational system can be thought of as creating gaps in the defences. Gaps may be the result of:

- Undiscovered and longstanding shortcomings in the defences. These represent latent failures.
- The temporary unavailability of some elements of the system as the result of maintenance action.
- Active failures of equipment.
- Human errors or violations.

3.6.7 For an accident to occur in a system designed and implemented in accordance with these principles, it will be necessary for gaps to occur in all the defensive layers of the system at the critical time when that defence should have been capable of detecting the earlier error or failure. This is illustrated diagrammatically in Figure 3-1. (after Maurino *et al.,* 1995).

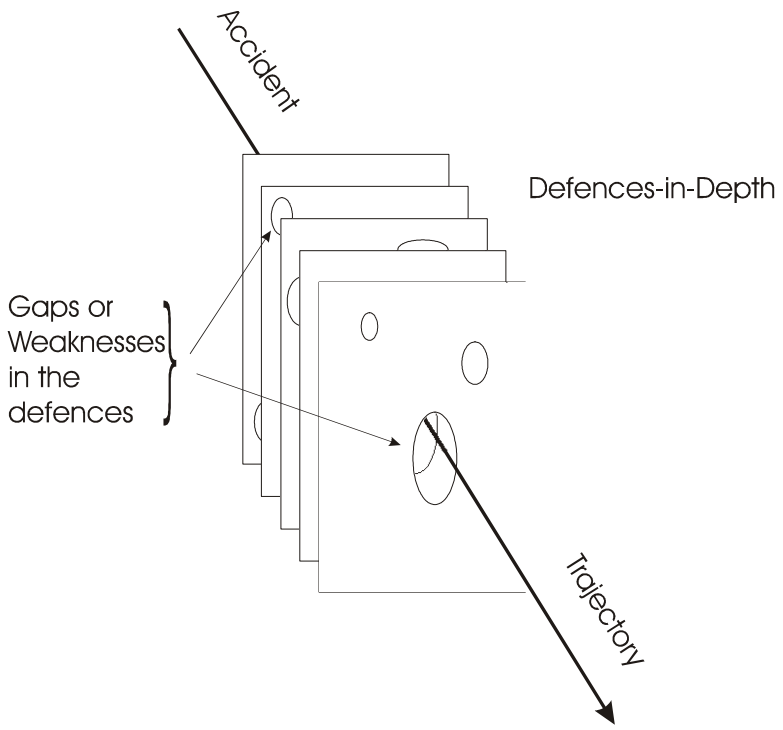


Figure 3-1. Defences-in-Depth – An illustration of how an accident event must penetrate all defensive layers.

3.6.8 The gaps in the system defences shown in Figure 3-1. are not static. Gaps will "open" and "close" as the operational situation changes, or equipment serviceability states change.

- A gap may sometimes be the result of nothing more than a momentary oversight on the part of a controller. The first defence against this type of occurrence should be to ensure that all controllers make a habit of periodically reviewing the whole traffic situation in their airspace. However for this can only happen if the controller is not overloaded, so the availability of this defence depends on decisions made at the organizational level, regarding sectorization, staffing levels and traffic acceptance rates.
- Other gaps may represent long-standing latent failures in the system. Identifying and closing these gaps requires an organizational culture, which encourages reporting of incidents, and effective procedures for the investigation of incidents, to establish the causes and enable rectification action to be taken.

3.6.9 Table 3-3 below shows some examples of defences, barriers and safeguards at the technology, operational and organizational levels.

1. Equipment

- Redundancy:
  - Full redundancy providing same level of functionality when operating on the alternate system.
  - Partial redundancy resulting in some reduction in functionality, e.g. local copy of essential data from a centralized network database.
- Independent checking of design calculations and assumptions.
- System designed to ensure a gradual degradation of capability (not total loss of capability) in the event of failure of individual elements.
- Policy and procedures regarding maintenance, which may result in loss of some functionality in the active system, or loss of redundancy.
- Automated aids, e.g. STCA, MSAW, Runway Entry Monitors, ACAS.
  - These should always be subsidiary to safe and effective operating procedures, which form the primary defence against the events, which these automated, aids, are designed to detect.

2. Operating Procedures

- Read back of critical items in clearances and instructions.
- Checklists and habitual actions, e.g. requiring a controller to follow-through the full flight path of an aircraft, looking for conflicts, immediately coordination is received from the handing-off sector.
- Inclusion of a validity indicator in designators for SIDS and STARS.

3. Organizational Factors

- Clear safety policy:
  - Must be implemented, adequate funding for safety management activities.
- Oversight to ensure correct procedures are followed:
  - No tolerance for violations or short-cuts.
- Adequate control over the activities of contractors.

Table 3-3. Examples of Defences, Barriers and Safeguards

3.6.10 The principles outlined in this chapter may be applied to the task of reducing risk in both proactive and reactive ways. By careful analysis of a system, it is possible to identify sequences of events where a combination of the faults and errors just discussed could lead to an accident, in advance of such an accident occurring. The same approach can also be used to analyze the chain of events, which led to an incident. Identification of the active and latent failures revealed by this type analysis will enable remedial action to be taken to strengthen the system's defences.

3.6.11 The successful application of many of the principles and techniques to be discussed in the remainder of this manual will depend on an understanding of the mechanisms leading to faults and errors, which have been presented in this chapter.

CHAPTER 4 - THE MANAGEMENT OF SAFETY

4.1 THE PHILOSOPHY OF SAFETY MANAGEMENT

4.1.1 Experience in other industries and lessons learned in investigation of aircraft accidents have emphasized the importance of managing safety in an *explicit*, *systematic* and *proactive* manner.

Explicit means that all safety management activities should be documented, visible and performed independently from other management activities.

Systematic means that safety management activities will be in accordance with a pre-determined plan, and will be applied in a consistent manner throughout the organization.

Proactive means the adoption of an approach which emphasizes prevention, through the identification of hazards and the introduction of risk mitigation measures before the risk-bearing event occurs and adversely affects safety performance.

4.1.2 Maurino *et al* (1995) have described this approach to safety management as being a change from a process dominated by retrospective repairs (i.e. fixing the stable door after the horse has bolted) to one in which prospective reform plays the leading part (i.e. making a stable from which no horse could run, or even want to).

4.1.3 Addressing safety in an explicit, systematic and proactive manner ensures, on a long-term basis, that safety becomes an integral part of the day-to-day business of the organization, and that the safety-related activities of the organization are directed to the areas where the benefits will be greatest.

4.1.4 To ensure that all possible sources of hazards which could affect safety are identified, safety management should be based on a total system approach, where the system, as introduced in Chapter 1, includes all the people, procedures and technology needed to operate or support the ATS system.

4.1.5 Modern approaches to safety management have also been shaped by the concepts introduced in Chapter 3 concerning the factors affecting system safety, and in particular, the role of organizational issues as contributory factors in accidents and incidents. Safety cannot be achieved simply by introducing rules or directives concerning the procedures to be followed by operational staff. Effective safety management requires that safety be addressed first at the organizational level.

4.1.6 The scope of safety management encompasses almost the whole range of activities of the organization concerned. It is for this reason that safety management must start from the senior level of management, and that potential effects on safety must be examined at all levels of the organization. Chapter 2 of *Human Factors Digest No. 10 – Human Factors, Management and Organization* (Circular 247) lists a number of examples where organizational factors, such as tolerance of unsafe practices or the lack of mechanism for monitoring safety related matters, were determined to be contributing factors to major accidents.

4.1.7 Only by having a system with adequate safeguards, and an organizational culture which ensures that these safeguards will not be circumvented, can acceptable levels of safety performance be assured.

4.1.8 The identification of hazards, implementation of safeguards and development of a safety-oriented organizational culture can only be done from within an organization. The safety management system must therefore be implemented and operated by the ATS provider. An external body, such as the Safety Regulator, can audit the system to see whether it complies with ICAO and national requirements, but it cannot actively manage the day-to-day operation of the safety management system.

4.2 SAFETY CULTURE

4.2.1 Effective safety management requires more than setting up an organizational structure and promulgating rules or directives specifying the procedures to be followed. It requires a genuine commitment to safety on the part of senior management, and an organizational culture such that staff at all levels are safety conscious in their approach to their tasks. This is the safety culture, which was referred to briefly in Chapter 1.

4.2.2 All organizations have an organizational culture. This can be defined as:

Organizational Culture. The shared values, attitudes and beliefs of the staff of the organization, which interact with the structure of the organization to shape the accepted patterns of behaviour. (Adapted from Reason, 1997)

4.2.3 There is a close correlation between the philosophy of safety management and this concept of a safety culture The philosophy defines a way of thinking about safety. The safety culture is result of this the way of thinking being translated into actions, so that the organizational culture becomes safety oriented. The safety policy provides the starting point for the development of a safety culture.

4.2.4 The characteristics of an organization with a positive safety culture include:

a) senior management places a strong emphasis on safety as part of the strategy of controlling risks;

b) decision makers and operational personnel hold a realistic view of the short- and long-term hazards involved in the organization's activities;

c) managers in top positions do not use their influence to force their views or to avoid criticism;

d) managers in top positions foster a climate with a positive attitude towards criticism, comments and feedback from lower levels of the organization;

e) awareness of the importance of communicating relevant safety information at all levels of the organization is present (both within it and with outside entities);

f) promotion of appropriate, realistic and workable rules relating to hazards, safety and potential sources of damage, with such rules being supported and endorsed throughout the organization;

g) personnel are well trained and understand the consequences of unsafe acts; and

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

4.2.5 There is also a significant degree of interdependence between the safety culture and other aspects of the safety management system. A positive safety culture is essential for the effective operation of the safety management system. However, the culture of the organization is also shaped by the existence of a formal safety management system, in particular, the safety promotion activities. An organization should not, therefore, wait until it has achieved a ideal safety culture before introducing a safety management system. The culture will develop as exposure to and experience with safety management increases.

4.2.6 Safety culture is examined in more detail in Appendix A to this Chapter.

4.3 BASIC SAFETY MANAGEMENT SYSTEM CONCEPTS

4.3.1 A safety management system designed in accordance with the principles of the philosophy of safety outlined above can be defined as:

Safety Management System. A system for the management of safety including the organizational structure, responsibilities, procedures, processes and provisions for the implementation of safety policies in order to provide for the control of safety.

Note.- This definition is based on the existing definition in the Manual on Certification of Aerodromes *(Doc 9774), with specific references to aerodromes removed to make it more generally applicable.*

4.3.2 The requirements, procedures and practices which make up the safety management system can be grouped under the following headings:

a) the organization's safety policy

b) the core safety management activities, which are:

- safety monitoring;
- safety assessment;
- safety auditing;
- safety promotion; and

c) the supporting organizational requirements, which include:

- the safety management organizational structure;
- the role of the safety manager;
- safety responsibility and accountability; and
- training and competency of personnel.

4.3.3 The relationship between these various components of a safety management system is illustrated in Figure 4-1 below.

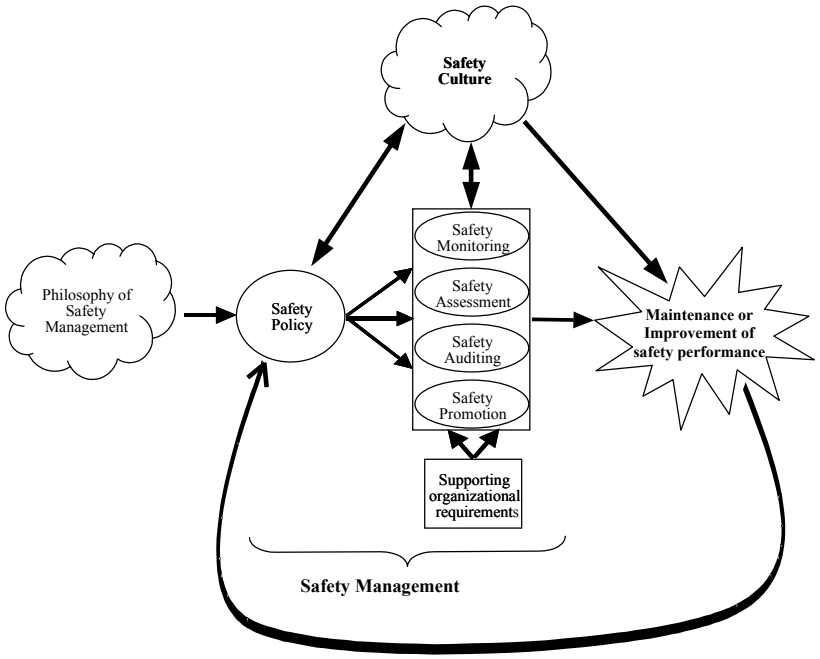


Figure 4-1. The Concept of Safety Management

4.3.4 Each of the components making up the safety management system will be discussed in detail in the succeeding sections.

4.4 THE SAFETY POLICY

4.4.1 The management commitment to safety should be formally expressed in a statement of the organization's *safety policy.* This should reflect the philosophy of safety management expressed in the beginning of this chapter and will, in turn, become the foundation on which the organization's safety management system is built.

4.4.2 The safety policy is a statement of what the organization expects to achieve in relation to safety performance. It is a written document, issued under the authority of the highest level of management of the organization, and presents a tangible indication of senior managements commitment to safety.

4.4.3 In preparing the safety policy, management should consult widely with the staff of the organization, both to ensure that the full range of experience and expertise within the organization is utilised in the development process, and to develop in the staff a sense of ownership of the policy, rather than seeing it as something imposed on them from above.

4.4.4 A safety policy may take different forms, but will typically include statements concerning:

a) the overall safety objective of the organization;

b) the commitment of senior management to the goal of ensuring that all aspects of operation of the ATS system meet safety performance targets;

c) a commitment by the organization to a proactive and systematic approach to the management of safety;

d) a commitment by the organization to making the maintenance of safety its highest priority;

e) the organization's policy concerning responsibility and accountability for safety at all levels of the organization;

4.4.5 Two examples of safety policies are given below in Table 4-1.

4.5 SAFETY PERFORMANCE MONITORING

4.5.1 The purpose of a safety performance monitoring system is to collect data on accidents, incidents, and other safety-related occurrences, to enable the safety performance of the system to be assessed.

4.5.2 A safety occurrence reporting and investigation system is an integral part of safety monitoring. All staff should be encouraged to report occurrences which could result in safety being compromised. All such reports should be investigated, in order to identify any measures which need to be taken to prevent similar occurrences in the future.

4.5.3 Implementation of a safety performance monitoring programme requires that the organization:

a) specify the safety performance indicators to be used to measure safety performance;

b) set safety performance targets;

c) develop and implement appropriate data collection procedures, including a safety occurrence reporting and investigation system; and

d) develop and implement procedures for the analysis and assessment of the results of monitoring.

Safety Policy – Example 1

<*The organization*> will provide the highest reasonable standard of safety within the air traffic systems which it plans, provides and operates by identifying and minimising those risks arising from <*the organization's*> activities which could contribute to aircraft accidents.

<*The organization*> will regard the safety of the air traffic system as the most important consideration throughout all its activities.

Safety is an integral part of the provision of an efficient, effective air traffic system. All managers are accountable for the performance of their areas of responsibility.

<*The organization*> will continue to adopt explicit safety standards which comply with statutory obligations and with the safety requirements of the Safety Regulatory Authority.

<*The organization*> will develop a culture among all managers and staff which fosters an increasing understanding of the importance of safety in all out activities and the resultant responsibility of each individual. "The organization" will provide the environment, support and training necessary to achieve this goal.

<*The organization*> will ensure that the systems and technology it uses, whether developed internally or bought externally meet specified and appropriate system safety standards.

Table 4-1. Example 1 of a safety policy statement

Safety Policy Statement – Example 2

Safety is the first priority in all our aviation activities. We are committed to implementing, developing and improving appropriate strategies, management systems and processes to ensure that all our aviation activities uphold the highest level of safety performance and meet national, european and international standards.

Our commitment is to:

- develop and embed a safety culture across all our aviation activities that recognises the importance and value of effective aviation safety management and acknowledges, at all times, that safety is paramount;
- clearly define for all staff their accountabilities and responsibilities for the development and delivery of aviation safety strategy and performance;
- minimise the risk associated with an aircraft accident or incident to a point which is As Low As Reasonably Practicable/Achievable;
- ensure externally supplied systems and services that impact upon the safety of our operations meet appropriate safety standards;
- actively develop and improve our safety processes to conform to world-class standards;

- comply with and wherever possible exceed legislative and regulatory requirements and standards;
- ensure that all staff are provided with adequate and appropriate aviation safety information and training, are competent in safety matters and are only allocated tasks commensurate with their skills;
- ensure sufficient skilled and trained resources are available to implement safety strategy and policy;
- establish and measure our aviation safety performance against objectives and/or targets;
- achieve the highest levels of safety standards and performance in all our aviation activities;
- continually improve our safety performance; and
- conduct safety and management reviews and ensure relevant action is taken.

We all have a responsibility for working in a safe manner. The application of effective aviation safety management systems is integral to all our aviation activities with the objective of achieving the highest levels of safety standards and performance.

Table 4-2. Example 2 of a safety policy

4.5.4 The monitoring system should cover both the operational and engineering aspects of the system, and include provisions for monitoring the performance of services provided by external providers.

4.5.5 Guidance on monitoring of safety performance and the implementation of a safety occurrence reporting and investigation scheme is contained in Chapter 5.

4.6 SAFETY ASSESSMENT

4.6.1 Annex 11, paragraph 2.26.5, requires States to undertake a safety assessment prior to the implementation of any new separation minimum or procedure, in order to demonstrate that it meets an acceptable level of safety. More specific information on the circumstances in which a safety assessment could be required can be found in the PANS-ATM, Chapter 2, Section 2.6.

4.6.2 Safety assessment is a structured and systematic process for the identification of hazards and assessment of the risk associated with each hazard. The acceptability of the risks is determined by comparing the assessed level of risk to the pre-determined safety assessment criteria.

4.6.3 If the result of an assessment is that the system under review does not satisfy the safety assessment criteria, it will be necessary to find some means of modifying the system in order to reduce the risk. This process is called *risk mitigation*. The development of mitigation measures becomes an integral part of the assessment process, since the adequacy of the proposed mitigation measures must be tested by re-evaluating what the risk would be with the mitigation measures in place.

4.6.4 The safety assessment process should start at a very early stage in the life cycle of a new system, well before it enters operational service. For large and complex projects, a series of safety assessments should be undertaken at various stages of the development and implementation process.

4.6.5 More detailed guidance on safety assessment procedures is contained in Chapter 6.

4.7 INTERNAL SAFETY AUDITS

4.7.1 A system can only achieve the level of safety indicated by the safety assessment if it is operated as intended. The safety audit process provides a means of verifying that this is indeed the case,. Safety auditing is therefore a further important proactive safety management tool.

4.7.2 The safety audits referred to here are internal audits of particular units or sections, conducted by staff of the ATS provider itself. All safety management systems should make provisions for such internal audits, in addition to any audits of the organization as a whole conducted by the Safety Regulatory Authority.

4.7.3 A safety audit programme established in accordance with the guidelines in this manual will satisfy the requirements of PANS-ATM, Section 2.5, for safety reviews of ATS units to be conducted on a regular and systematic basis.

4.7.4 A safety audit should verify compliance with standards and procedures, including compliance with the organization's safety management procedures. However, compliance with standards and procedures is not necessarily sufficient to ensure safety. One of the advantages of a safety audit is that the audit team may be able to identify hitherto unforeseen hazards in the system, or in other words, identify latent failures. (See Chapter 2).

4.7.5 The safety audit programme, together with the safety monitoring procedures, provides feedback to both managers of individual units and senior management concerning the safety performance of the organization. This feedback provides evidence of the level of safety performance being achieved and, where safety deficiencies have been identified, enables appropriate corrective measures to be developed.

Note.- The terminology used for the processes described here is not standardized. Similar processes may be described in some systems as safety surveys, or safety reviews. The most important issue is the content of the programme, rather than the name. The use of the term audit is consistent with the terminology used in the ICAO Universal Safety Oversight Audit Programme, and the Manual on Certification of Aerodromes *(Doc 9774).*

4.7.6 More detailed guidance on safety audit programmes is contained in Chapter 7.

4.8 SAFETY PROMOTION

4.8.1 Safety promotion refers to those activities which the organization carries out in order to ensure that the staff understand why safety management procedures are being introduced, and what safety management means. It is the mechanism by which the organization's safety policy is communicated to staff. It also provides a means of encouraging the development of a positive safety culture and ensuring that, once established, the safety culture is maintained.

4.8.2 Safety promotion activities are particularly important during the initial stages of implementation of a safety management system. However, it is also important that safety promotion is maintained as on on-going activity. It is the means by which safety issues are communicated within the organization.

4.8.3 Some of these issues will be addressed through the inclusion of modules on safety management in staff training programmes. However, the safety promotion process also involves less formal mechanisms.

4.8.4 Safety promotion is not limited just to the dissemination of information about the organization's safety policies and procedures to staff. It is also the mechanism through which lessons learned from safety occurrence investigations and other safety related activities are published and made available to all relevant personnel. This could take the form of regular newsletters or safety bulletins.

4.8.4.1 Where the lessons learned could also be significant to other States and ATS providers, consideration should be given to wider dissemination of the information.

4.8.5 Publication of a safety policy, procedures, newsletters and bulletins alone will not necessarily bring about the development of a positive safety culture. While it is important that staff are well informed, it is also important that they see evidence of the commitment of management to safety. The attitudes and actions of management will therefore be a significant factor in promotion of safe work practices and development of a positive safety culture.

4.8.6 Safety information and concerns must not only be communicated downwards to the operational levels, there must also be effective communication upwards in the organization. All staff should be encouraged to bring any potential safety related issues to the attention of the levels of management responsible for addressing them, and should also be encouraged to propose possible solutions.

4.8.7 In order to propose solutions to identified hazards, staff must be aware of the hazards which have already been identified and the corrective actions which have already been implemented. The safety promotion activities and training programmes should therefore address the rationale behind the introduction of new procedures resulting from a safety assessment.

4.8.8 It is important that management acknowledge any significant safety concern or suggestion originating from staff. Management must provide appropriate feedback to the originators of such concerns or suggestions.

4.9 SUPPORTING ORGANIZATIONAL REQUIREMENTS

4.9.1 The organizational requirements needed to support the core safety management functions must address:

a) responsibility and accountability;

b) the need for and the role of a safety manager;

c) training and competency of personnel; and

d) safety documentation.

Responsibility and accountability

4.9.2 Responsibility and accountability are closely related concepts. Each individual member of staff has a responsibility for his or her actions. Air traffic controllers are responsible for ensuring that appropriate separation minima exist between all aircraft in their airspace. Maintenance personnel are responsible for ensuring that the equipment on which they are working is fully serviceable before being returned to service.

4.9.3 Accountability is determined by the structure of the organization. Each individual is accountable to his or her supervisor or manager and may be called on to justify the actions taken. Managers and supervisors may also be accountable for the overall performance of the group which

reports to them. Safety accountabilities should be explicitly specified, for example in the organization's safety management manual.

4.9.3.1 It is important that responsibilities and accountabilities for safety are clear, with no overlap or omission.

4.9.4 Changes to the organizational structure should be assessed to determine whether there is any effect on safety responsibilities and accountabilities. Any necessary amendments to previous responsibilities and accountabilities should be properly documented.

Organizational structure

4.9.5 Safety must be supported from the very top of the organization and must be seen as an integrated strategic aspect of the overall business management, to ensure that safety is given the necessary priority by the organization.

4.9.6 One of the first tasks in establishing a safety management system is to appoint a safety manager. The safety manager is responsible for the development and maintenance of an effective safety management system for the whole organization.

4.9.7 The safety manager should report directly to the Chief Executive of the organization. This position needs a high level of authority to be effective and needs to be seen to have a high level of importance and the support of the senior management. Having the safety manager to report directly to the Chief Executive will demonstrate that safety has an equal level of importance in the decision making process to other divisions.

4.9.8 The safety manager is responsible for managing all aspects of the operation of the safety management system. This would include ensuring that safety documentation accurately reflects the current environment, monitoring the effectiveness of corrective actions, providing periodic reports on safety performance, and providing independent advice to the Chief Executive, senior managers and to other personnel on safety-related matters.

4.9.9 While the safety manager would be held accountable for any deficiencies in the safety management system, the safety manager will not in general be accountable for the safety performance of the organization.

4.9.10 Figure 4-2 below illustrates one possible way of incorporating safety management into the organizational structure.

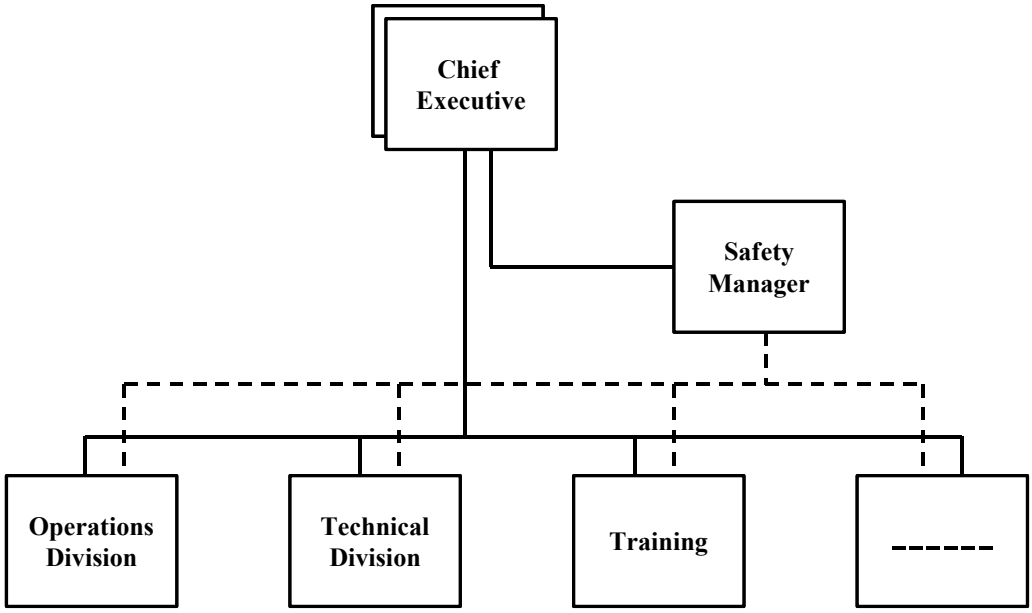


Figure 4-2. Safety Management Organization

4.9.11 Under the arrangement shown in Figure 4-2, line managers report to the Chief Executive, and are accountable to him for the performance, including the safety performance, of their divisions. However, on certain safety related issues, for example the development of corrective actions following a safety audit, or progress of implementation of such actions, they would report directly to the safety manager. However, even in these cases, it is the line manager who is accountable for the implementation of the corrective actions.

The safety manager

4.9.12 The safety manager should ideally have no responsibilities other than safety. This would generally be the case in large organizations where a full time safety manager position can be justified. In smaller organizations, safety management may have to be the responsibility of a manager who also has other duties. It would be preferable, in such cases, that the person responsible for safety management did not also have direct responsibility for any of the operational or engineering areas, to avoid possible conflicts of interest.

4.9.12.1 Whether the safety manager position is a full time one, or forms only part of the responsibilities of the designated manager, the duties and responsibilities of the position will be the same.

4.9.12.2 Irrespective of the size of the organization, the safety manager should possess extensive operational management experience and have an adequate technical background to understand the systems that support the ATS operations. The safety manager should also have a good understanding of safety management principles, either through training or practical experience (and preferably both).

4.9.12.3 When a candidate with all the required qualifications is not available, which may well be the case when establishing a safety management system for the first time, it may be necessary to make provision for training in safety management for the person who is to take up the safety manager position.

4.9.13 Large organizations may require a small staff of dedicated safety specialists to assist the safety manager. These specialists could undertake a variety of tasks, such as maintenance of safety documentation, reviewing safety assessments, and taking part in safety audits.

- *To develop, maintain and promote an effective safety management system;*
- *To provide assurance that the safety management system is being implemented and operated effectively throughout the organization;*
- *To act as focal point for dealings with the Safety Regulatory Authority*
- *To provide specialist advice and assistance where required regarding safety issues;*
- *To develop a safety management awareness and understanding throughout the entire organization;*
- *To act as a proactive focal point for safety issues.*

Table 4-3. Example of terms of reference for the safety manager

Safety committees and safety groups

4.9.14 The objective of safety committees and safety groups is to provide forums, at different levels within the organization, to discuss issues related to the safety performance of the organization and the health of the safety management system

4.9.14.1 A safety committee would typically be established at senior management level, while a safety group would be established at line manager level.

4.9.15 The members of the safety committee would be the safety manager and other senior managers. The objective of the safety committee is to make recommendations concerning safety policy decisions, and to review the results and recommendations received from the safety audit programme and the safety performance monitoring programme. During the initial implementation phase, the would also review the progress of the implementation process.

4.9.15.1 Terms of reference for the safety committee should be documented in the organization's safety management manual.

4.9.16 A safety group would typically be established at line manager level. The objective of a safety group is to provide an expert forum for the development or revision of safety management procedures, to initiate safety promotion programmes and to review safety improvement proposals. Depending on the size and complexity of the organization, more than one safety group could be established.

4.9.16.1 Terms of Reference of the safety group(s) should be documented in the organization's safety management manual.

4.9.17 The need for and structure of such safety committees and safety groups depends on the size of the organization. In small organizations, where the distance in the organizational structure from

the working level to the management level is relative short, there may be less need for establishing either a safety committee or a safety group.

4.9.18 Where no separate safety committee is established, safety performance and safety management should be a regular agenda item at general management meetings. The safety manager would be one of the participants in these meetings.

Training and Competency

4.9.19 Having staff who are competent for the job they are performing is a fundamental pre-requisite for achieving safety. Competency requirements, and where appropriate licensing requirements, should be documented in the job description for each safety-related position. These requirements should then be reflected in the recruitment requirements and internal training course content for these positions.

4.9.20 Each line manager should be accountable for ensuring the continuing competency of the personnel in safety related positions within his or her area of responsibility. This includes ensuring that any periodic continuation training requirements are met, and that staff in need of refresher training receive such training.

4.9.21 The head of the training section should be responsible for ensuring that appropriate proficiency and refresher training programmes exist, and for maintaining records of training.

4.9.22 All training programmes should include training in those aspects of the safety management system and associated procedures that are relevant to the position in question.

4.10 SAFETY MANAGEMENT DOCUMENTATION

4.10.1 All ATS providers should document their safety management system in a Safety Management Manual.

4.10.2 It is also important that the organization be able to provide evidence of the measures taken to control risks, and ensure that adequate levels of safety are maintained. The safety management system should therefore incorporate provisions to ensure that all safety-related decisions and actions are adequately documented. Records should be maintained of all:

a) safety occurrence and investigation reports;

b) safety audit reports;

c) periodic analyses of safety trends; and

d) safety assessment documentation.

The Safety Management Manual

4.10.3 The safety management manual should contain detailed descriptions of all aspects of the safety management system, including the safety policy, safety procedures and individual safety accountabilities.

4.10.4 The safety management manual should include, *inter alia:*

a) document identification and validity;

b) document control procedures;

c) scope of the safety management system;

d) the safety policy;

e) safety performance monitoring;

f) safety assessment;

g) safety auditing;

h) safety promotion; and

i) safety organizational structure.

4.10.5 The safety management manual is a living document, and must, at any given time, reflect the current status of the safety management system.

4.10.6 The safety management manual provides management with a key instrument for communicating the organization's approach to safety of the whole organization.

4.10.7 Appendix B to this Chapter illustrates a framework for a safety management manual, including guidelines concerning the content of individual chapters.

APPENDIX A TO CHAPTER 4

SAFETY CULTURE

This Appendix is based on *Human Factors Guidelines for Safety Audit Manual*.(Doc 9806)

1. Safety culture is a term that came into prominence in the nuclear industry following the Chernobyl accident. Paraphrasing the International Nuclear Safety Advisory Group (INSAG), safety culture may be defined as follows:

   Safety culture. That assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, safety issues receive the attention warranted by their significance.

2. Safety culture in aviation refers to the personal dedication and accountability of individuals engaged in any activity that has a bearing on the safe provision of ATS. It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters.

3. Safety culture then is both attitudinal as well as structural, relating to both individuals and organizations. It concerns the requirement to not only perceive safety issues but to match them with appropriate action. Safety culture relates to such intangibles as personal attitudes and the style of the organization. It is therefore difficult to measure, especially when the principal criterion for measuring safety is the absence of accidents and incidents. Yet, personal attitudes and corporate style do enable or facilitate the unsafe acts and conditions that are the precursors to accidents and incidents.

4. Safety culture goes beyond mechanistic adherence to ATS procedures. It requires that all duties important to safety be carried out correctly, with alertness, due thought and full knowledge, sound judgement and a proper sense of accountability.

5. Attention to safety involves many elements:

   - individual awareness of the importance of safety;
   - knowledge and competence, conferred by training and instruction of personnel and by their self-education;
   - commitment, requiring demonstration by senior management of the high priority of safety and adoption by individuals of the common goal of safety;
   - motivation, through individual's own attitudes as influenced by management in the setting of objectives and systems of rewards and sanctions;
   - supervision, including audit and review practices, and a receptiveness to questioning attitudes by subordinates; and
   - responsibility, through formal assignment and description of duties and follow-up to ensure their understanding by individuals.

Tangible evidence

6. Organizations with effective safety cultures demonstrate many facets of tangible evidence. The following characteristics may be indicative that an organization is fostering an effective safety culture.

ATS Service Provider – Management Level

7. Safety culture flows down more from the actions of senior management than from their words. The attitudes, decisions and methods of operation at the corporate policy-making level demonstrate the real priority given to safety. Sometimes key strategic decisions of the operator reflect inadequate attention to the safety implications in line operations. The initial indication of corporate commitment to safety is in their public statement safety policy and objectives, specifically, whether the objectives have been clearly stated and communicated to all personnel in an understandable way, and particularly, whether staff believe that concern for safety might, on occasion, override production objectives.

8. A key indicator of management's commitment to safety is the adequacy of resource allocations. Establishment of a management structure, assignment of responsibilities within that structure, and allocation of resources must be consistent with the organization's stated safety objectives. In particular, sufficient, experienced staff, relevant and timely training, and funding for essential equipment and facilities are fundamental to creating a working environment in which everyone takes safety seriously.

9. In effective safety cultures, there are clear reporting lines, clearly defined documentation of assigned duties, and clearly established, well-understood ATS procedures. Personnel are fully cognizant of their responsibilities and know what to report, to whom, and when. Further, senior management reviews not only the financial performance but also the safety performance of the organization on a regular basis with respect to such aspects as:

    - training, to ensure that it is meeting user requirements and that training resources are adequate;
    - documentation systems, to ensure that necessary records are being properly prepared and retained, and that resources for this are adequate; and
    - personnel selection and promotion systems, to ensure that individuals in key safety positions have demonstrated attitudes towards safety consistent with their positions.

Service Provider – Line Management

10. On a day-to-day basis, it is the line managers who mould the work environment, fostering attitudes conducive to safety. They convert senior management's policies and decisions into action. Managers must ensure that their staff are competent and understand what is expected of them and how their responsibilities relate to those of others. Managers must be vigilant about systemic deviations from ATS procedures in day-to-day operating and maintenance practices.

11. Factors that shape people's safety attitudes include how operational services are routinely provided by line management. The quality and timeliness of the following services are examples of this:

    - initial and recurrent training;
    - rostering;
    - dissemination of safety information.

12. In safe operating cultures, ATS supervisors avoid creating a work environment that promotes cutting corners, such as encouraging exceeding controllers duty hours, deviations of ATS procedures or pressing weather limits. They must be prepared to take disciplinary measures for deliberate violations of ATS procedures. On the other hand, good managers appreciate the potential for excessive sanctions leading to the deliberate concealment of errors.

13. In this respect, safe operating cultures in aviation promote a blame-free environment. In other words, errors are recognized as a normal part of human behaviour and as such, are tolerated. Indeed, employees are encouraged to report their errors in order that others may learn from the experience. For example, confidential reporting programs foster disclosure of a safety-related issue while protecting the person reporting it from disciplinary action or embarrassment.

14. Of particular concern is how local line management prepares for and deals with change and to what extent safety is a planning factor when faced with such events as:

    - introduction of new equipment or modifications;
    - expanding operations, including new, relatively inexperienced controllers;
    - changes to ATS procedures.

15. Arising from such changes are questions about whether potential safety problems have been identified in consultation with the affected staff and whether identified problems have been dealt with in ways that will reduce or eliminate the inherent safety risks.

16. Line management continues to demonstrate its commitment to safety through regular inspections, audits and staff contact. How this is done will affect individuals' attitudes, e.g. frequency, openness, constructive versus punitive approach (i.e. personnel development versus compliance checking).

17. How line management deals with the day-to-day line experience is fundamental to a sound safety culture. Are the correct safety lessons being drawn from actual line experience and appropriate actions being taken? Are the affected staff constructively involved in this process or do they feel they are the victims of management's unilateral action?

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

Individual Attitudes

19. Individuals' attitudes in line operations are often the most visible indication of the degree of success or failure of the corporate safety culture. Some early indicators include:

    - discipline in following ATS procedures versus departing from ATS procedures in favour of quicker or easier methods;
    - willingness to analyse unforeseen situations rather than resorting to rote reaction;
    - availability of line managers to line personnel;
    - openness of communications with line managers;
    - staff initiative in communicating safety concerns and recommending viable remediation;
    - spirit of cooperation between line managers and personnel for mutually satisfactory resolution of safety issues.

Supporting Agencies

20. The organization's safety culture must extend to those supporting agencies that interface with line operators day-to-day in the provision of ATS. The lowest bidder for contractual services may not be the safest bidder. Here again line management must ensure that quality services are being delivered in a way that does not compromise safety. This should be a routine part of management's safety monitoring process. Identified safety problems require prompt attention to safeguard the belief that management cares about safety.

APPENDIX B TO CHAPTER 4

The objective of this Appendix is to provide guidelines for the preparation of the safety management manual. It presents a framework to be used and a brief description of the structure and contents.

The safety manager is responsible for the development of the safety management manual. The development of a safety management manual is an iterative process. The safety management manual should be written so that it reflects the intent and processes of the safety management system. Thus, a significant change to the safety management system will require an update of the safety management manual.

The safety management manual should be kept as short and concise as possible. Too much and too complex text will discourage personnel and management from reading and understanding the document. Moreover, it may also require more frequent updates.

The safety management manual should be kept under configuration management and should include a well-defined distribution list and trace of change history.

Any information that changes regularly should be put into appendices. This includes, for example, names of assigned members of the personnel assigned specific safety responsibilities and safety procedures.

The following exemplifies a framework that may be used when structuring the safety management manual.

Structure of a Safety Management Manual

1. Documentation Identification and Validity

The document documenting the safety management system should have a unique and clearly identifiable title, such as a safety management manual. The validity of the safety management manual should be stipulated.

2. Documentation Control Procedure

A system, which ensures that the status of the documentation can be ascertained, should be implemented. This can usually be achieved by a version numbering scheme.

3. Scope of the Safety Management System

The scope of the safety management manual should be clearly identified. All elements of the ATS system, to which the safety management system is applicable, should be listed

4. Safety Policy

The safety policy should be included in the safety management manual.

Safety Performance Monitoring

Each of the four core functions should be described. The following should be detailed:

a) The **objective** of safety performance monitoring;

b) The **requirements** of safety performance monitoring;

c) Who is **responsible** for the requirements related to safety performance monitoring; and

d) Appropriate **reference** to where a detailed safety performance monitoring procedures are contained.

The following procedures should be developed and included as appendixes to the safety management manual:

a) Safety Performance Targets

This appendix should describe the process leading to the definition of safety performance indicators and safety performance targets. Appropriate safety performance targets should be contained in this appendix.

b) Safety Occurrence Reporting and Investigation Procedure

This procedure should document the structure of the safety occurrence reporting and investigation system. This includes the reporting procedures, the investigation process, the risk classification scheme and the categorizing of causes.

c) Safety Performance Monitoring Procedure

This procedure should document the monitoring process and techniques used to detect deviations in operation. A description of how the results of the safety performance monitoring will be used as feedback to improve the safety should be included.

5. Safety Assessment

The following should be detailed:

a) The **objective** of safety assessment;

b) The **requirements** of safety assessment;

d) Who is **responsible** for the requirements related to safety assessment; and

c) Appropriate **reference** to where detailed safety assessment procedures are contained.

The following procedure should be developed and included as an appendix to the safety management manual:

a) Safety Assessment Procedure

This procedure should document the safety assessment process and should contain the risk classification scheme to be used. It should also detail how to develop a safety assessment document.

6. Safety Auditing

The following should be detailed:

a) The **objective** of safety auditing;

b) The **requirements** of the safety auditing;

c) Who is **responsible** for the requirements related to safety auditing; and

d) Appropriate **reference** to where detailed safety auditing procedures are contained.

The following procedure should be developed and included as an appendix to the safety management manual:

a) Safety Auditing Procedure

This procedure should document the safety auditing process. This includes the competence and performance of those responsible for executing the safety audits.

7. Safety Promotion

a) The **objective** of safety promotion;

b) The **requirements** of safety promotion;

c) Who is **responsible** for the requirements related to safety promotion; and

d) Appropriate **reference** to where detailed safety promotion procedures are contained.

The following procedure should be developed and included as an appendix to the safety management manual:

a) Reporting process of safety concerns/proposals

It is important that the organization establishes a process for communicating safety concerns. This includes a feedback process from the management to the individual who raised the concern. The reporting process, including feedback process should be described in this appendix.

8. Safety Organization

The organizational structure should be illustrated using an organizational diagram. It should illustrate where in the organization the safety manager is placed. Safety accountabilities appear from the organizational diagram and should be explained in more detail.

Competency requirements should be documented in the manual, preferable as appendices. This should also include specific safety responsibilities assigned to respective safety related functions within the organization.

APPENDIX C TO CHAPTER 4

EXAMPLES OF ACCOUNTABILITIES AND RESPONSIBILITIES

General Manager ATS

Safety Accountabilities

The General Manager ATS is accountable to the Chief Executive to provide services and facilities, for customers and stakeholders, for the purpose of giving effect to the Chicago Convention or otherwise in relation to the safety, regularity or efficiency of air navigation to permit the safe navigation of aircraft within <State name>-administered airspace, including:

- airspace management;
- air traffic control;
- traffic and flight information;
- aviation rescue and fire fighting (ARFF);
- provision of navigation aids;
- aeronautical information;
- aviation information centre;
- air traffic services OJT training;
- ARFF training;
- asset management of physical assets (including land, buildings, and ATM systems) used to deliver aerodrome, approach, departure and en-route air traffic services, rescue and fire fighting services, aeronautical information services and aeronautical radio navigation services;
- definition of a base-line specification for those components of the ATM system controlled by ATS Division;
- ensuring that the management of human resources by ATS Division is appropriate to facilitate safe operations;
- the initiation, implementation and completion of projects of operational or strategic importance including:
    - coordination of operational projects throughout the Division;
    - ensuring that policies, procedures and systems are in place to guide and support the delivery of operational projects; and
    - ensuring that project management skills and knowledge are developed across the group;
- developments and opportunities for adopting new technologies, such as the Global Navigation Satellite System (GNSS).

Safety Responsibilities

In discharging these accountabilities the General Manager ATS is responsible for:

- safety management within ATS Division that complies with the requirements of the <organisation name> Safety Management Manual including arrangements for identifying, reporting, tracking and correcting safety issues and for the initiation of preventive or improvement action where necessary;
- ensuring that safety considerations are given the appropriate priority, and that fitness for service has been declared and properly accepted by the responsible authority, in relation to the development of plans, policies, procedures, processes and systems, including tenders and contracts;
- overseeing the performance ATS Division safety activities and ensuring that managers and staff are aware of and held accountable for their safety performance;
- ensuring safety issues are reported in a timely manner to the Executive Safety Committee;
- ensuring that ATS Division managers and staff are trained, qualified and competent to discharge their safety related obligations.

General Manager Infrastructure

Safety Accountabilities

The General Manager Infrastructure Division is accountable to the Chief Executive to provide services and facilities to the ATM Division to permit the safe navigation of aircraft within <State name>--administered airspace, including:

- specialist engineering and maintenance, including:
    - calibration of navigation aids;
    - maintenance of the specified base-line of ATM and other national airways system assets and monitoring the overall integrity and performance of those assets, as managed and used by business centers in commercial operations;
- provision of reliable telecommunications systems;
- provision of reliable information management systems to support the operational requirements of Infrastructure Division and the Head Office;
- logistics planning and support;
- ensuring that the management of human resources of Infrastructure Division is appropriate to facilitate safe operations;
- where appropriate, implementing on behalf of ATM Division, projects of operational or strategic importance;
- coordinating the management and resourcing of projects throughout Infrastructure Division;
- ensuring that policies, procedures and systems are in place to guide and support the management and delivery of projects;
- ensuring that project management skills and knowledge are developed across the Division;

- technical training;
- ab initio air traffic controller training;
- air traffic control management training;
- undertake research and development;
- staff support services including staff counselling and redundancy support;

development and coordinated delivery of supervisory and management training;

Safety Responsibilities

In discharging these accountabilities the General Manager Infrastructure Division is responsible for:

- safety management within the Infrastructure Division that complies with the requirements of the <organisation name> Safety Management Manual including arrangements for identifying, reporting, tracking and correcting safety issues and for the initiation of preventive or improvement action where necessary;
- satisfying the safety management requirements of the ATM Division where Infrastructure Division activities can be identified as having an impact on safe operation of the National Airways System;
- ensuring that safety considerations are given the appropriate priority, and that fitness for service has been declared and properly accepted by the responsible authority, in relation to the development by Infrastructure Division of plans, policies, procedures, processes and systems;
- overseeing the performance of Infrastructure Division safety activities and ensuring that managers and staff are aware of and held accountable for their safety performance;
- ensuring safety issues are reported in a timely manner to the Executive Safety Committee;
- ensuring that Infrastructure Division managers and staff are trained, qualified and competent to discharge their safety related obligations.

Chief Financial Officer

Safety Accountabilities

To support the activities for the safe operation of the National Airways System the Chief Financial Officer is accountable to the Chief Executive for:

- development, implementation and monitoring of financial strategies;
- taxation and treasury management and advice;
- purchasing policy;
- corporate financial control;
- insurance management and policies; and
- revenues collection policy.

Safety Responsibilities

In discharging these accountabilities the Chief Financial Offer is responsible for:

- ensuring that safety considerations are given the appropriate priority during the development of financial strategies, policies and planning processes;
- ensuring that revenue raised by <organisation name> is sufficient to maintain the safe operation of the National Airways System;
- providing advice to senior management on Corporate financial management strategies that will enable them to manage the safe operation of the National Airways System;
- providing advice to senior management on aviation industry economics, including forecasts of industry activity that will enable them to implement strategies for the continued safe operation of the National Airways System;
- ensuring that Finance and Administration managers and staff are aware of and are held accountable for their safety performance; and
- ensuring that Finance and Administration managers and staff are trained, qualified and competent to discharge their safety related obligations.

CHAPTER 5 - SAFETY PERFORMANCE MONITORING AND INVESTIGATION

5.1 INTRODUCTION

5.1.1 Safety performance monitoring provides the means by which an ATS provider can verify that it is meeting its safety performance targets. To do this, data must be collected and analysed, to enable the achieved level of safety performance to be assessed. In addition, an effective monitoring programme increases the probability of detecting any weaknesses in the system defences before an active failure leads to an accident or serious incident.

5.1.2 Identifying weaknesses in the system defences requires more than just collecting data and producing summary statistics. The underlying causes of reported occurrences are not necessarily immediately apparent, therefore investigation of safety occurrence reports, and any other information concerning possible hazards, should go hand in hand with safety performance monitoring.

5.1.3 Safety performance monitoring and investigation activities play both a reactive and a proactive role in the safety management system.

5.1.3.1 The analysis and investigation of data derived from monitoring, and the comparison of the achieved safety performance to the safety performance targets, is a reactive process. The application of the lessons learned from the analysis and investigation of these occurrences in order to prevent similar occurrences in the future is a proactive process.

5.2 REQUIREMENTS FOR IMPLEMENTATION OF SAFETY PERFORMANCE MONITORING AND INVESTIGATION

5.2.1 Some of the requirements for a safety performance monitoring system will already be in place in many States.

5.2.1.1 States would normally have already published regulations relating to mandatory reporting of accidents and incidents, in accordance with *Annex 13 – Aircraft Accident and Incident Investigation*, and would have procedures in place for processing and investigating these reports.

5.2.2 The implementation of an effective safety performance monitoring programme will, in addition, require that ATS providers:

a) determine appropriate safety performance indicators;

b) set safety performance targets;

c) establish a safety occurrence reporting system;

d) establish a system for the investigation of safety occurrences;

e) develop procedures for the integration of safety data from all available sources; and

f) develop procedures for the analysis of the data and the production of periodic safety performance reports.

5.2.2.1 Defining safety performance indicators and setting safety performance targets were discussed in Chapter 2 and will not be discussed further in this chapter.

5.2.3 The requirements and procedures for safety performance monitoring and investigation should be fully documented in the organization's safety management manual.

5.3 SOURCES OF DATA

5.3.1 If the safety performance monitoring is to provide data which will allow the achieved level of safety performance to be assessed, the type of data collected must be matched to the safety performance targets. If, for example, these are expressed in terms of the rate of occurrence of certain categories of safety occurrences, the data collected must allow the determination of the number of occurrences in the relevant categories. However, the data collected should not be limited to just what is needed to meet this objective. To enable weaknesses in the system defences to be identified, the scope of the data collected must be as wide as possible. As already noted in Chapter 2, the scope of data collected should cover both operational and engineering aspects of the system, and should also take into account any services provided by external organizations where these could have an impact on safety.

5.3.2 The sources of data include:

a) mandatory accident and incident reporting and investigation systems;

b) voluntary reporting systems;

c) special purpose monitoring programmes such as RVSM height monitoring, and the navigation error monitoring programmes implemented in certain airspace where MNPS or RNP approval is required; and

d) system maintenance records.

5.3.2.1 Where airspace with special requirements such as RVSM height monitoring or navigation error monitoring exists, the special monitoring programmes applicable to such airspace should already have been established.

5.4 SAFETY OCCURRENCE REPORTING

5.4.1 Hazards can only be controlled if their existence are known. A system for reporting safety occurrences is one of the key tools available for identifying previously undetected hazards.

5.4.2 There are two types of reporting schemes. They are:

a) mandatory reports of accidents and incidents required by State regulations; and

b) voluntary reports of safety occurrences which would not be reported under the mandatory reporting provisions.

5.4.3 The quality of the data obtained from any reporting scheme depends on the extent to which safety occurrences are reported and investigated. A report by the Flight Safety Foundation estimated that for each major accident, there are 360 incidents that, if reported, might have identified underlying problems in time to prevent the accident. (Flight Safety Foundation Icarus Committee, 1999)

5.4.4 The primary responsibility for reporting saftey occurrences lies with the individual staff members who are involved in or observe the occurrence. Whether or not a report is submitted will depend on the individual's perception of the potential risks associated with the event. If the individual is directly involved, it will also depend on his or her perception of the likely consequences. The effectiveness of a reporting system will therefore be dependent on the existence of an organisational culture which encourages the submission of reports.

Mandatory accident and incident reporting

5.4.5 Annex 13 requires all States to establish mandatory accident and incident reporting systems, and specifies the high level requirements for mandatory reporting. It also recommends that all States establish voluntary reporting schemes. Specific details regarding reports to be submitted to the ICAO ADREP system are contained in the *Accident and Incident Reporting Manual (ADREP Manual)*,

(Doc 9156). These topics will not be addressed in detail here, although the need for internal investigation of these reports and inclusion of the information obtained from them in the overall monitoring results will be addressed in the appropriate parts of this chapter.

Voluntary reporting programmes

5.4.6 Mandatory reporting requirements generally apply only to accidents and serious incidents, (where a serious incident is defined in Annex 13 as an incident involving circumstances indicating that an accident nearly occurred).

5.4.7 There are many occasions when human errors or system failures occur, but the circumstances are such that there is little danger of an accident. However, given a different combination of circumstances, for example a different disposition of traffic, a similar event could well result in an accident. A voluntary reporting scheme is designed to capture data on these sorts of occurrences.

5.4.8 Annex 13 only recommends the establishment of voluntary reporting systems, but it requires that where such a system is established, it shall be non-punitive and afford protection to the sources of the information.

5.4.9 The Aviation Safety Reporting System (ASRS) in the United States is an example of a voluntary reporting programme. It was implemented in 1975 as a result of a recommendation made by the National Transportation Safety Board (NTSB).

5.4.9.1 The ASRS is designed to encourage the identification and reporting of deficiencies and discrepancies in the United States national airspace system, and to assist the FAA and the aviation community in lessening the likelihood of aviation accidents.

5.4.9.2 To encourage reporting, the ASRS provides limited immunity from certain types of enforcement action. The programme is administered by the National Aeronautics and Space Administration. It is a voluntary, confidential incident reporting system. Reports can be submitted by anyone involved in aviation. While anonymity of the person submitting the report is assured, and all published information is "de-identified" by removing names and other identifiable items such as aircraft registrations, the originators are required to provide names and contact details. This enables investigators to verify details, and obtain clarification or additional information where necessary.

5.4.9.3 Further information about ASRS can be found in FAA Advisory Circular AC 00-46D, and the ASRS web site, at *http://asrs.arc.nasa.gov*.

5.4.10 A similar programme called the Confidential Aviation Information Reporting system (CAIR) has been introduced in Australia. It is operated by the Australian Transport Safety Bureau (ATSB). Further information on this programme can be found on the ATSB website, at *http://www.atsb.gov.au./*

Establishment of a Reporting Culture

5.4.11 Persuading staff to file reports on occurrences in which they have been involved can be a difficult task, particularly where this involves an admission of error on their part. An organization with a positive safety culture will already have many of the characteristics needed to encourage the submission of such reports.

5.4.11.1 The disincentives to submission of such reports include fear of disciplinary action, scepticism that the report will be acted on, and overly complex reporting procedures.

5.4.11.2 No organization can overlook repeated gross errors, or deliberate violations of standards and procedures. In these cases, disciplinary action must be taken. However, in order to promote an environment in which staff will be prepared to submit reports:

a) the policy regarding disciplinary action, and the way in which it is applied, must be seen to be just; and

b) an atmosphere of trust must exist between management and staff.

5.4.11.3 The organization should document its policy concerning disciplinary action, and apply this policy consistently. Cases where the error is within the bounds of normal human fallibility should not be subject to disciplinary action. As was seen in Chapter 3, human fallibility is a factor which should be taken into account in the design of the system. Occurrences of this type should be approached from the point of view of trying to determine how safeguards in the system could be improved, to ensure that errors of this type will not lead to an accident, rather than allocating blame.

5.4.11.4 Separation of the body responsible for the collection and investigation of reports from the body responsible for initiation of disciplinary measure will also help build staff confidence in the system.

5.4.12 Another significant disincentive to the submission of reports, as mentioned in 5.4.11, is scepticism that submitting a report will have any effect. To ensure that staff do not develop this type of attitude, it is necessary not only to ensure that reports are investigated and acted upon where necessary, but also to ensure that the originator is provided with feedback concerning the outcome of the investigation and the action taken.

5.4.12.1 This does not imply that all safety occurrence reports need to be investigated as though they were serious incidents. Some reports, for example a report of a brief failure of a communication link, may be assessed quickly and a decision reached that the only immediate action required is to monitor the situation to determine whether this was an isolated case, or a recurrent problem. However, the originator should still be advised of the decision, so that he or she will know that the report is not being ignored.

5.4.13 The third disincentive is overly complex procedures. The report form should be a simple as possible, but a balance must be reached between ease of submission, and the need for adequate information for investigation purposes. O'Leary and Chappell (1996) summarized the requirements as follows:

> If a form is long and requires a great deal of time to complete, reporters are less likely to make the effort. If the form is too short, it is difficult to obtain all the necessary information about the incident. In general, the more specific the questions, the easier it is to complete the questionnaire; however, the information provided will be limited by the choice of questions. More open questions about the reporter's perceptions, judgements, decisions and actions are not subject to this limitation and give the reporter a greater chance to tell the full story. This method is more effective in gathering all the information about an incident, but usually requires more analytic resources within the reporting system.

5.4.13.1 In addition, the reporting form should capture sufficient data to assist the investigators in classifying the occurrence. (Classification of an occurrence is addressed further in section 5.5.)

5.4.14 In summary, the requirements of a positive reporting culture are:

a) The reporting system is simple and user-friendly.

b) Management encourages the reporting of safety occurrences.

c) The treatment of staff who submit reports is seen to be just.

d) Each occurrence report received is investigated.

e) Feedback is provided to the originator of the report.

f) Staff see that the submission of reports results in corrective action to prevent recurrence.

g) Confidentiality is maintained, insofar as possible, in relation to disclosure of information concerning individuals.

h) Lessons learned are disseminated to all staff to enable them to learn from other's errors.

5.4.15 A more detailed discussion of the issues involved in establishing an organizational culture which encourages reporting of safety occurrences can be found in Chapter 9 of Reason (1997).

5.5 INVESTIGATION OF SAFETY OCCURRENCES

5.5.1 The investigation of safety occurrences often reveals the there were a number of warning signs, or precursors, which could have been observed before the incident or accident. Investigation of occurrences can allow the identification of such warning signs, and the dissemination to staff of information which could enable similar warning signs to be recognized in the future before they lead to safety occurrence.

5.5.1.1 Identifying the lessons to be learned from a safety occurrence requires an understanding not just of what happened, but why it happened. A complete understanding of why an occurrence happened requires an investigation which looks beyond the obvious causes and focuses on identifying all contributory factors, some of which may be related to weaknesses in the systems defences or other organizational issues.

5.5.2 The objectives of the investigation process are to:

a) establish the primary causes and all other factors that contributed to the occurrence;

b) identify actions to reduce the probability of a recurrence; and

c) provide an accurate and factual description of the circumstances surrounding the occurrence, and the lessons to be learned.

5.5.3 The investigation of serious incidents and accidents is the responsibility of the body nominated by the State in accordance with the provisions of Annex 13.

5.5.4 The responsibility for investigation of reports submitted through a voluntary reporting system will depend on how the system is structured. In both the United States and Australian examples, the collection of reports and the subsequent investigation are the responsibility of bodies separate from both the ATS provider and the safety regulator. However, this is not the only possibility. Reason (1997) describes a system operated by British Airways where the collection and investigation of reports is an internal function within the company.

5.5.4.1 Where the investigation of voluntary reports is an internal function within an organization, it is important that this be the responsibility of a department separate from the ones responsible for operational and engineering management, and disciplinary functions.

5.5.5 Irrespective of where the formal responsibility for investigation of reports lies, there are advantages in the ATS provider having its own internal procedures for processing and investigating safety occurrence reports. These include:

a) an internal investigation can be started immediately after the event occurs, so that accounts of what occurred can be obtained while it is still fresh in the minds of those involved; and

b) prompt internal investigation may enable the identification of areas where immediate risk mitigation measures should be introduced, in advance of the conclusion of the formal investigation.

The Investigation Process

5.5.6 The size and complexity of the investigation process will depend on the nature and seriousness of the occurrence being investigated.

5.5.6.1 The same general principles apply in all cases. However, since the voluntary programmes specifically prohibit the submission of reports of occurrences which should have been the subject of reports through the mandatory accident and incident reporting system, it could be expected that the occurrences reported through these programmes will be less serious, and the investigation process less complex.

5.5.7 In all investigations, it is important to remember that safety occurrences rarely have a single cause. There will always be at least one initiating event, and there will also usually be a number of additional contributory factors. It is important that the investigation process identify not only the direct causes, but also all contributory factors.

5.5.8 The identification of all contributory factors will be aided by the use of a structured top-down approach. Profit (1995) proposes the following steps, as an example of such an approach.

a) As a first stage, establish all the factors which may have had a potential bearing on the incident. It is advisable not to attempt to define a priority or hierarchy of factors at this stage, but list them chronologically as short statements;

b) Work backwards from the incident and produce a chart of the factors which contributed to the incident, in reverse chronological order. Note beside each factor the evidence that supports it. List separately the other factors that have been explored and discounted together with the reasons;

c) The framework for the diagnosis of causes can now be made and written up. Start by discounting the factors that have been considered which have no bearing on the incident. Each factor should be considered separately on its own, and where possible the team's argument should be supported by evidence. The wording might read: "There was no evidence to suggest that….. contributed to the incident….." or "The team discounted….. because….." etc;

d) Having discounted the irrelevant factors, the findings should discuss chronologically the causes of the incident. One approach is to describe the cause in one paragraph and then to analyse it in a second paragraph entitled "Team Comment". The Comment should summarise the analysis argument with cross reference to the relevant evidence for each of the causes. The argument should conclude with an assessment of each cause's relative importance as a primary or contributory cause;

e) Finally, some of the factors which were discounted as causes of the incident may well be Observations. Observations are noteworthy features, including deficiencies discovered, which were not primary or contributory causes of this incident, but which might have safety significance under other circumstances and remedial action may be a good investment for the future; and

f) Except in simple incidents where the diagnosis is short, it is helpful if the diagnosis of causes section of the final report is concluded with separate summaries of the primary causes and the contributory causes, each in chronological order.

Classification of safety occurrences and causal factors

5.5.9 A written report in plain language can give a comprehensive overview of a single occurrence and the circumstances surrounding it; however, plain language reports do not easily provide the information needed to answer questions such as, "How many runway incursions occurred at aerodrome X during the last year?" or "On how many occasions was a failure of ground-based communications equipment a contributory factor in reported safety occurrences during the last six months?". Providing answers to these sorts of questions becomes much easier if events and causal factors are classified using a standard scheme, and the classified data are entered into a data base.

5.5.10 A classification scheme (also called a *taxonomy*) is comprised of a hierarchy of classes of events. The top levels are very broad in scope, while each succeeding lower level becomes more specific. A detailed discussion of classification schemes is beyond the scope of this manual; however, the following example illustrates the principles.

> The class *Air Navigation Services* would be at a high level in the hierarchy, and would include *Air Traffic Management, Aeronautical Information Service, Search and Rescue Service, Meteorological Service, and Communications, Navigation and Surveillance Services*.
>
> *Air Traffic Management* would include the sub-classes of *Air Traffic Control Service, Air Traffic Advisory Service, Flight Information Service, Alerting Service, Air Traffic Flow Management Service*, and *Airspace Management Service*.
>
> Still lower levels of the hierarchy would allow differentiation between aerodrome, approach and enroute ATC services, and at a lower level still, whether the service was being provided using radar or procedural methods.

5.5.11 ICAO has, for many years, maintained a global data base of accidents and serious incidents notified by States through the Aircraft Accident Data Reporting System (ADREP). The latest version of this system, called ADREP 2000, contains a greatly expanded taxonomy including many ATS-related categories It was developed in conjunction with the European Coordination Centre for Aviation Incident Reporting Systems (ECCAIRS). Information on this system, including copies of the taxonomies, can be found on the internet at *http://eccairs-www.jrc.it/*

5.5.12 It is recommended that these taxonomies be used for classification of ATS-related safety occurrence data for internal investigation and analysis purposes, as well as for reporting accident and incident data to ADREP.

5.5.13 In all cases where safety occurrence data is entered into a data base, it should be borne in mind that the validity of the information derived from any data base will only be as good the data on which it is based. Therefore, it is important that the accuracy of the entered data is verified.

Disclosure of information

5.5.14 In recent years, information from accident and incident records, and safety monitoring and data acquisition systems, has been admitted as evidence in judicial proceedings. These proceedings have also resulted in criminal charges being brought against the individuals involved.

5.5.15 Annex 13, paragraph 5.12, establishes certain types of records from the investigation of an accident or incident shall not be made available for purposes other accident or incident investigation, unless "the appropriate authority for the administration of justices in that State determines that their disclosure outweighs the adverse domestic and international impact such action may have on that or any future investigations". Paragraph 8.3 of Annex 13 requires that voluntary incident reporting systems shall

be non-punitive and afford protection to the sources of the information. For these provisions of Annex 13 to have effect, they must be enacted in the relevant legislation of the State.

5.5.15.1 ICAO Assembly Resolution A33-17, urged Contracting States to "examine and if necessary to adjust their laws, regulation and policies to protect certain accident and incident records in compliance with paragraph 5.12 of Annex 13, in order to mitigate impediments to accidents and incident investigations".

5.6 ANALYSIS OF MONITORING DATA

5.6.1 One of the principal functions of safety performance monitoring is to provide the organization with an assessment of the achieved level of safety performance. This requires integration and analysis of the data gathered by all the components of the safety performance monitoring and investigation system.

5.6.2 At the simplest level, data concerning the numbers of different types of safety occurrences, and their rates of occurrence (for example, number of occurrences of a particular type per 1,000 flight hours, or per 1,000 movements) could be tabulated. In deciding what types of occurrences to include, consideration should be given to the safety performance indicators that have been adopted by the organization. However, the analysis should not be limited to just these indicators, as monitoring may reveal that there are additional factors, which were not included in the original safety indicators, which are raising safety concerns.

5.6.3 Plotting the data on a graph will show visually how the frequency and rate of occurrence of these events has changed from month to month, or year to year. However, if there is a high degree of variability over time in the data, the underlying trend in the frequency of occurrence of the events may not be immediately obvious. In these cases, some form of further analysis should be undertaken to determine the trend.

5.6.3.1 Techniques for analysing trends include moving averages, and regression analysis. These techniques are beyond the scope of this manual. Further information on them can be found in basic texts on statistical methods.

5.6.4 In addition to tracking trends in types of safety occurrences, comparisons should be made between types of occurrences in order to identify common elements. Where such common elements are found, appropriate corrective actions should be developed and implemented.

5.7 OTHER METHODS OF MONITORING SAFETY

Observation of normal operations

5.7.1 The monitoring methods discussed so far have all relied on staff identifying actual or potential hazards to the safe operation of the system, and submitting reports. If unsafe practices have become part of the normal method of operating, it is unlikely that the staff involved will recognize these as being unsafe, and file reports through the safety occurrence reporting system.

5.7.2 Observation-based methods provide an additional means of gathering data, that does not rely on the individuals involved. Several airlines have introduce a programme called Line Operations Safety Audit (LOSA) to monitor operations under normal operating conditions. The aim of the monitoring is to gather data on operational threats, crew errors, and their management. The observations are made by a trained observers, trained in the LOSA techniques, sitting in the jump seat on regular scheduled flights.

5.7.3 The key difference between this programme and check flights is that the observations are without jeopardy for the crew, therefore the observer is more likely to see the normal behaviour of the

crew. Experience to date has indicated that this programme does provide reliable data on flight crew behaviour and performance in normal operations. LOSA was specifically designed for use by airlines; however, the same principles could be applied to observing ATS operations. At the time of writing of this manual, the possibility of this was under investigation. The term proposed for the programme was Normal Operations Safety Survey (NOSS).

5.8 LESSON DISSEMINATION

5.8.1 The effort put into safety performance monitoring and investigation will only produce dividends, in the form of improved safety performance, if the lessons learned from the investigation and analysis of all the data are taken on board by the organization, and translated into actions. The action required can range from changes at the organizational level, to procedures or structure, through to changes in individual patterns of behaviour.

5.8.2 All information with safety implications should be disseminated widely, and should be clear, concise and easy to read. Information can be disseminated by means of formal reports to management, and by safety newsletters, bulletins and seminars for all staff. However, the lessons associated with a particular occurrence will not really have been learned until action is taken to reduce the probability of similar occurrences in the future. Management must therefore ensure that, where necessary, procedures are modified, and the lessons learned are reflected in relevant training courses.

5.8.3 Safety data that could be of interest to other organizations or States should be shared as widely as possible. States should promote the establishment of safety information sharing mechanisms among all users of the aviation system in order to facilitate the free exchange of information on actual and potential safety deficiencies.

5.8.3.1 The *Global Aviation Information Network* (GAIN) is one example of such an information sharing mechanism. It is an industry-led international coalition of airlines, manufacturers, employee groups, governments and other aviation organizations, formed to promote and facilitate the voluntary collection and sharing of safety information in order to improve aviation safety. The ICAO ADREP system also provides a mechanism by which safety data can be shared among States.

CHAPTER 6 - SAFETY ASSESSMENT

6.1 AN OVERVIEW OF SAFETY ASSESSMENT

6.1.1 In Chapter 1, Safety management was introduced as the means by which organizations could control the processes which could lead to hazardous events, in order to ensure that the risk of harm or damage is limited to an acceptable level. Safety assessment, which is one of the core functions of a safety management system, provides a mechanism for identifying the potential hazards and finding ways to control the risk associated with them.

6.1.2 Annex 11 requires that any significant safety-related change to the ATC system shall only be implemented after a safety assessment has demonstrated that an acceptable level of safety will be maintained. It is not possible to specify all the circumstances in which a safety assessment could be required; however, the PANS-ATM gives the following examples:

a) a reduced separation minimum to be applied within an airspace or at an aerodrome;

b) a new operating procedure, including departure and arrival procedures, to be applied within an airspace or at an aerodrome;

c) a reorganization of the ATS route structure;

d) a resectorization of an airspace;

e) physical changes to the layout of runways and/or taxiways at an aerodrome; and

f) implementation of new communications, surveillance or other safety-significant systems and equipment, including those providing new functionality and/or capabilities.

6.1.2.1 These examples can be used as a guide to aid States ATS providers in assessing when a safety assessment should be conducted.

6.1.3 The acceptable level of safety is specified by the safety assessment criteria, which should have been set in advance.

6.1.4 The scope of the safety assessment must be wide enough to cover all aspects of the ATS system that will be affected by the change, either directly or indirectly.

6.1.5 The safety assessment process should start early in the life cycle of a new system. For a large and complex project, there will be several phases of safety assessment, each becoming more detailed as the design and development of the system progresses. The final pre-implementation safety assessment then forms the basis for the periodic safety reviews of the operational system, which should continue throughout its life cycle until decommissioning.

6.2 THE SAFETY ASSESSMENT PROCESS

6.2.1 Chapter 2 introduced the concept that risk is two-dimensional. The perceived risk associated with a hazardous event depends on both the likelihood of occurrence of the event, and the severity of its consequences. The safety assessment process will therefore need to address both these factors.

6.2.1.1 The safety assessment criteria used to evaluate the acceptability of the risk will also need to incorporate both severity and likelihood.

6.2.2 A safety assessment based on these concepts is essentially a process for finding answers to three fundamental questions:

- What could go wrong?
- What would be the consequences?
- How often is it likely to occur?

6.2.3 Once the person or team undertaking the assessment are satisfied that all the hazards (i.e. the things that could go wrong) have been identified, the last tow questions have been answered for each hazard, the acceptability of risk associated is evaluated against the pre-determined safety assessment criteria. Where the risk is found not to be acceptable, methods of reducing and managing it must be found.

6.2.4 There are many possible ways in which risk may be controlled. These include changes to the hardware or software, changes to existing procedures, and the introduction of new procedures. The general term for the process of developing and implementing measures of this type to control risk is *risk mitigation*.

6.2.5 Once a safety assessment is completed, it must be *accepted*. This refers to signing-off of the safety assessment by the responsible manager, to indicate that he or she is satisfied that the assessment has been properly performed, and that the level of risk is, indeed, acceptable. For the manager to be able to make an informed decision concerning this, the safety assessment must be well documented. The documentation should be retained to provide a record of the basis on which the acceptance decision was made.

6.2.6 Safety assessment requires a systematic approach. The complete process can be divided into seven steps. These are:

Step 1 – Development (or procurement) of a complete description of the system to be evaluated and of the environment in which the system is to be operated;
Step 2 – Identification of hazards;
Step 3 – Estimation of the severity of the consequences of hazard occurring;
Step 4 – Estimation of the likelihood of the hazard occurring;
Step 5 – Evaluation of risk;
Step 6 – Mitigation of Risk;
Step 7 – Development of safety assessment documentation.

Table 6-1. Seven steps for safety assessment

6.2.7 If the initial assessment of the risk indicates that it does not satisfy the safety assessment criteria, requiring the introduction of mitigation measures, it will be necessary to re-evaluate the risk in order to determine whether the proposed mitigation measures will have the desired effect. This means that some of the previous steps will need to be repeated. The process may, in fact, need to be repeated more than once, until a satisfactory combination of mitigation measures is found.

6.2.7.1 Figure 6-1 illustrates the safety assessment process diagrammatically, and shows this possible need to perform a number of cycles of the process until a satisfactory method of mitigation is found.

6.2.8 The remainder of this chapter will examine each of these seven steps in more detail. In addition, Appendix C to this chapter contains an extract from the Safety Management Manual of Airservices Australia. It contains descriptions of some standard techniques used in the identification and assessment of hazards, and guidance concerning the application of these techniques to the assessment of ATS procedures. It includes an example of an actual application of these techniques. Appendix D contains a further example of an actual safety assessment.

6.3 STEP 1 – SYSTEM DESCRIPTION

6.3.1 The "system", as defined for the purpose of risk assessment will always be a sub-component of some larger system. Even if the analysis encompasses all services provided within a whole FIR, this can still be considered a sub-component of a larger regional system, which in turn is a sub-component of the global ATS system.

6.3.2 If all potential hazards are to be identified, the persons involved in the safety assessment must have a good understanding of the proposed new system or changes, and how it will interface with the other components of the overall ATS system of which it is a part. This is why the first step in the safety assessment process is to prepare a description the proposed system or change, and the environment in which it will operate.

6.3.3 The hazard identification process can only identify hazards which come within the scope of the system description on which the analysis is based. The boundaries of the system, as defined for the purposes of the risk assessment, must therefore be sufficiently wide to encompass all possible impacts which the system could have. In particular, it is important that the description includes the interfaces with the larger system of which the system being assessed is a part.

6.3.4 The system description phase should also address to what extent the system need to be divided into sub-systems for risk analysis purposes. A detailed description of the system should include:

a) the purpose of the system;

b) how will the system will be used;

c) a description of system functions;

d) the system boundaries and the external interfaces; and

e) a description of the environment in which the system will operate.

6.3.5 The safety impact of a potential loss or degradation of the system will be determined, in part, by the characteristics of the operational environment in which the system will be integrated. The description of the environment should therefore include any factors which could have a significant effect on safety. These factors will vary from one case to another. They could include, for example, traffic characteristics, airport infrastructure and weather-related factors, such as the frequency of diversions due to sever weather.

6.3.6 The description of the system should also address contingency procedures and other non-normal operations, for example, failure of communications or navigation aids.

6.3.6.1 For large scale projects, the system description should address the strategy for transition from the old to the new system. For example, will the existing system be de-commissioned and replaced immediately with the new system, or will the two be operated in parallel for a period of time?

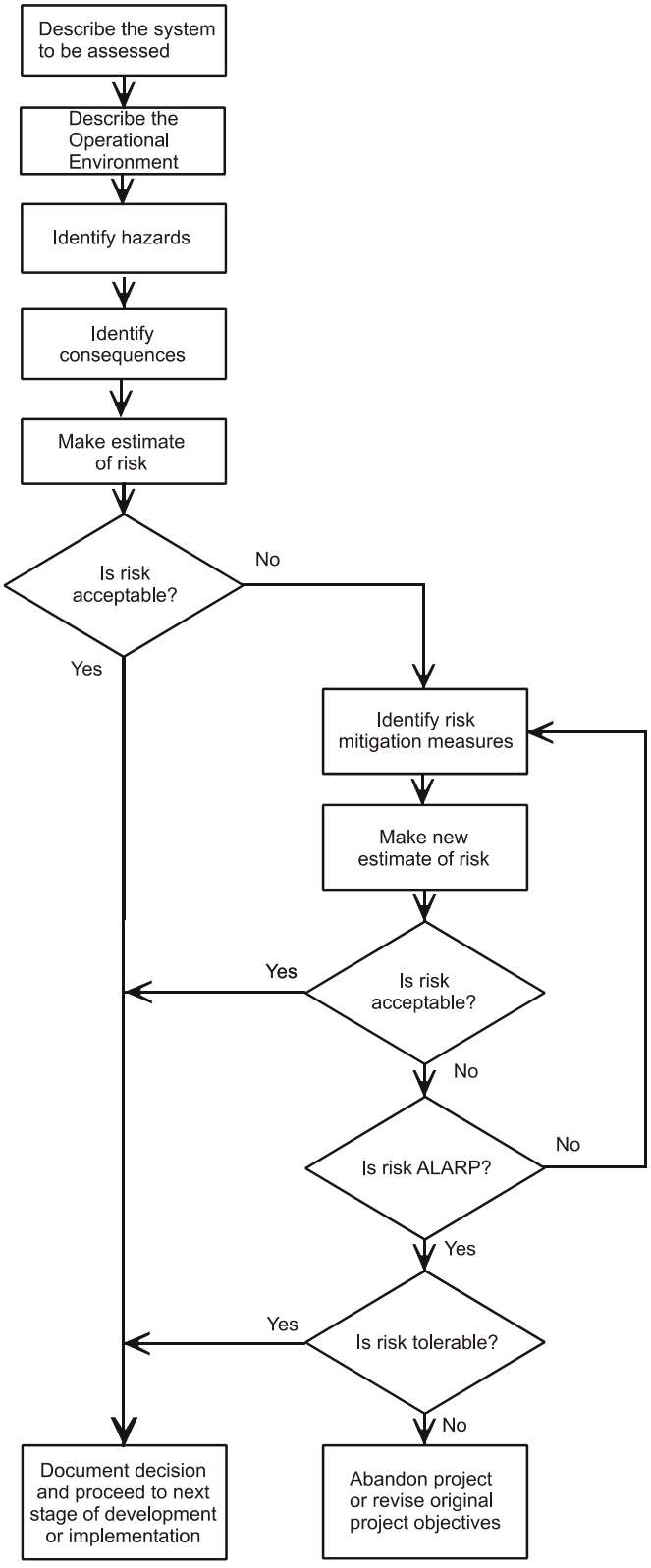


Figure 6-1. The Safety Assessment Process

6.4 STEP 2 – HAZARD IDENTIFICATION

6.4.1 The hazard identification step should be initiated at the earliest possible stage in the project life cycle. For large scale projects, there may be several hazard identification sessions at different stages of the project development. The level of detail required will depend on the complexity of the system under consideration and the stage of the system life cycle at which the assessment is being done. In general, it could be expected that less detail would be required for an assessment carried out during the operational requirement definition stage than for one during the detailed design stage.

6.4.2 The hazard identification step should consider all the possible sources of system failure. Depending on the nature and size of the system under consideration these could include:

a) The equipment (hardware and software);

b) The operating environment (including physical conditions, airspace and air route design);

c) The human operators;

d) The human machine interface (HMI);

e) Operational procedures;

f) Maintenance procedures;

g) External services.

6.4.3 All possible configurations of the system should be considered. For example, if staffing levels and sectorization of airspace are different at night than during the day, both configurations should be examined for hazards. Operations when equipment is off-line for regular maintenance should be considered separately.

6.4.4 All persons involved in the hazard identification process should be aware of the significance of latent failures, as these are not usually obvious. The process should specifically address questions such as, "how might staff misinterpret this new procedure," or "how might a person misuse this new function/system (intentionally or unintentionally)?".

Hazard Identification Sessions

6.4.5 It is important to ensure a structured approach to the identification of hazards, in order to ensure that, as far as possible, all potential hazards are identified.. This is a task that requires input from a range of experienced operational and technical personnel, and is usually done through a form of managed group discussion. A facilitator who is familiar with the techniques should manage the group sessions.

6.4.6 The role of the facilitator not an easy one. He or she must guide the discussions towards a consensus, but at the same time ensure that all participants have the opportunity to put their view, and allow sufficiently wide-ranging discussion to ensure that all possible hazards are identified.

6.4.7 The other group participants should be chosen for their expertise in fields relevant to the project being assessed. The range of expertise needs to be sufficiently broad to ensure that all aspects of the system are addressed, however it is also important to keep the group to a manageable size. The number of participants needed for the hazard identification sessions depends on the size and complexity of the system under consideration. Usually the number of participants is between 6-10 persons. Apart from the facilitator, the participants do not necessarily need prior experience in hazard identification.

6.4.8 Appendix B to this chapter contains detailed guidance on the conduct of group sessions for hazard analysis.

Note.- While the use of group sessions has been addressed here in the context of hazard identification, the same group would also address the assessment of the likelihood and severity of the hazards they have identified.

6.4.9 It is often difficult to define the boundary between a *worst* credible case and one so dependent on coincidence that it should not be taken into account. The following definitions can be used as a guide in making such decisions.

Worst: - The most unfavourable conditions expected, e.g. extremely high levels of traffic, extreme weather disruption.
Credible: - This implies that it is not unreasonable to expect the assumed combination of extreme conditions will occur within the operational life cycle of the system.

6.4.10 The assessment of hazards should take into consideration all possibilities, from the least to the most likely. It has to make adequate allowance for "worst case" conditions, but it is also important that the hazards to be included in the final analysis must be *credible* hazards.

6.4.11 The assessment should always consider the most critical phase of flight within which an aircraft could be affected by the system failure under consideration, but it should not generally be necessary to assume that simultaneous **unrelated** failures will occur.

6.4.11.1 It is, however, important to identify any potential *common mode failure*, which occurs when a single event causes multiple failures of more than one function within the system.

Common Mode Failure – Multiple failures resulting from a single fault.

6.4.12 All identified hazards should be assigned a hazard number, and recorded in a *hazard log*.

6.4.13 The hazard log should contain a description of each hazard, its consequences, the assessed likelihood and severity, and any required mitigation measures. It should be updated as new hazards are identified, and proposals for mitigation are introduced. Appendix A to this chapter contains a pro-forma for a typical hazard log. The example of a hazard assessment in Appendix D contains and extract from an actual hazard log.

6.5 STEP 3 – ESTIMATION OF HAZARD SEVERITY

6.5.1 Prior to the commencement of this step, the consequences of each hazard identified in Step 2 should have been recorded in the hazard log. This step involves the assessment of the severity of each of these consequences.

6.5.2 Risk classification schemes have been developed for a large number of applications where hazard analysis is regularly used. An example of one such scheme can be found in the *Joint Aviation Requirements - Large Aeroplanes* (*JAR-25)*, developed by the Joint Aviation Authorities (JAA).

6.5.2.1 JAR-25 is recognized by many Civil Aviation Authorities as an acceptable basis for showing compliance with their national airworthiness codes. JAR25.1309, and the associated advisory material, AMJ 25.1309*,* specify risk classification criteria to be used to determine acceptable levels for the risk associated with various failure conditions in aircraft systems.. The levels of acceptability take account of historical accident rates, and the need for there to be an inverse relationship between the probability of loss of function(s) and the severity of the hazards to the aircraft and its occupants arising from such an event.

6.5.3 While the criteria as specified in JAR-25 relate specifically to airworthiness of aircraft systems, they can be used as a guide to the development of similar classification schemes for other purposes. A number of States have already done this. Table 6-1 shows an example of a severity

classification scheme based on the JAR 25 approach, but adapted for ATS application, taken from the UK CAA *CAP 670, Air Traffic Services Safety Requirements*.

Note.- Examples of the classifications used in CAP 670 for the likelihood of occurrence and acceptability of the risk are provided in the following sections of this chapter.

6.5.4 The severity of the consequences is best assessed by the same group which performed the hazard identification. The guidelines for the conduct of the group sessions contained in Appendix B apply equally to the assessment of the severity.

6.5.4.1 While the assessment of severity of the consequences will always involve some degree of subjective judgement, the use of structured grouped discussions, guided by a standard risk classification scheme, and with participants who have extensive experience in their respective fields, should ensure that the outcome will be an informed judgement.

6.5.5 Once the assessment of severity has been completed for all the identified hazards, the results, including the rationale for the severity classification chosen, should be recorded in the hazard log.

6.6 STEP 4 – ESTIMATION OF THE LIKELIHOOD OF THE HAZARD OCCURRING

6.6.1 The estimation of the likelihood of a hazard occurring uses a similar approach to that adopted in Step 2 and Step 3; that is, by means of structured discussions using a standard classification scheme as a guide. Table 6-2 shows an example of a classification scheme for this purpose, based on JAR-25, taken from the UK CAA *CAP 670, Air Traffic Services Safety Requirements*.

6.6.2 This table specifies the likelihood as qualitative categories, but also includes numerical values for the probabilities associated with each category. In some cases, data may be available which will allow direct numerical estimates of the likelihood of failure to be made. For example, for the hardware elements of a system, extensive data is often available on historical component failure rates. Well established techniques exist for the estimation of the probability of loss of system functions from the failure rates for of individual components.

6.6.3 The estimation of the likelihood of occurrence of hazards associated with human error will generally involve a greater degree of subjective assessment (and it should be borne in mind that even when assessing hardware, there is always the possibility of failures due to human error; for example, incorrect maintenance procedures.) However, as with the estimation of severity, the use of structured group discussions with participants who have extensive experience in their respective fields, and the adoption of a standard risk classification scheme, should ensure that the outcome will be an informed judgement.

6.6.4 Once the assessment of likelihood has been completed for all the identified hazards, the results, including the rationale for the classification chosen, should be recorded in the hazard log.

	Classification				
	Catastrophic	***Hazardous***	***Major***	***Minor***	***Negligible***
Results in one or more of the following effects	• ATC issues instruction or information which can be expected to cause loss of one or more aircraft (no reasonable means exist for the aircrew to check the information or to mitigate against hazards. • Continued safe flight or landing prevented.	• The ATC separation service provided to aircraft that are airborne or inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, completely unavailable. • Provision of instructions or information which may result in a critical near mid-air collision or a critical near collision with the ground.	• The ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, severely degraded or compromised; (e.g. contingency measures required, or controller workload significantly increased such that the probability of human error is increased. • The ATC separation service provided to aircraft on the ground outside a runway protected area is suddenly, and for a significant period of time, completely unavailable. • Provision of instructions or information which may result in the separation between aircraft or aircraft and the ground being reduced below normal standards. • No ATS action possible to support aircraft emergency.	• The ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, impaired. • The ATC separation service provided to aircraft on the ground outside a runway protected area is suddenly, and for a significant period of time, severely degraded. • ATS emergency support ability is severely degraded.	• No effect on ATC separation service provided to aircraft. • Minimal effect on ATC separation service provided to aircraft on the ground outside a runway protected area. • Minimal effect on ATS emergency support ability.

Table 6-1. Severity Classification Scheme

	Probability of Occurrence Definitions				
	Extremely improbable	**Extremely remote**	**Remote**	**Reasonably probable**	**Frequent**
Qualitative definition	Should virtually never occur in the whole fleet life.	Unlikely to occur when considering several systems of the same type, but nevertheless has to be considered as being possible.	Unlikely to occur during the total operational life of each system but may occur several times when considering several systems of the same type.	May occur once during total operational life of one system.	May occur once or several times during operational life.
Quantitative definition	$< 10^{-9}$ per flight hour	10^{-7} to 10^{-9} per flight hour	10^{-5} to 10^{-7} per flight hour	10^{-3} to 10^{-5} per flight hour	1 to 10^{-3} per flight hour

Table 6-2. Probability Classification Scheme

6.7 STEP 5 – EVALUATION OF THE RISK

6.7.1 Since the acceptability of a risk is dependent on both its likelihood and the severity of its consequences, the criteria used to judge acceptability will always be two-dimensional. Acceptability is therefore usually based on comparison with a severity/probability matrix.

Note.- In the assessment of collision risk for enroute separation minima and instrument approaches, the acceptability criteria (in those applications generally called the Target Level of Safety) are expressed simply as probabilities. However, in both these cases the severity is implied, because the event whose probability is being assessed is always an aircraft accident with fatalities. This will always be catastrophic.

6.7.2 Table 6-3 shows an example of a matrix for the assessment of acceptability of risk. Once again, this is taken from the UK CAA *CAP 670, Air Traffic Services Safety Requirements*, and was adapted from the risk classification scheme in JAR-25.

6.7.3 Chapter 2 introduced the concept that while some risks are clearly acceptable, and some are clearly unacceptable, there is a zone in between where the decision concerning acceptability is not clear-cut. These latter risks form a third category, where the risk may be tolerable if it is reduced to a level as low as reasonable practicable (ALARP).

6.7.3.1 Where a risk is classed as ALARP, mitigation measures will always have been attempted, and those mitigation measures classed as feasible will have been implemented.

6.7.3.2 In Table 6-3, the risks which may be tolerable if ALARP are those which fall in the categories marked “Review”. Risks in this category are not automatically classed as tolerable. Every case must be reviewed on its merits, taking into account the benefits which will result from implementation of the proposed changes as well as the risk.

		Probability of Occurrence				
		Extremely improbable	**Extremely remote**	**Remote**	**Reasonably probable**	**Frequent**
Severity	Catastrophic	Review	Unacceptable	Unacceptable	Unacceptable	Unacceptable
	Hazardous	Review	Review	Unacceptable	Unacceptable	Unacceptable
	Major	Acceptable	Review	Review	Review	Review
	Minor	Acceptable	Acceptable	Acceptable	Acceptable	Review

Table 6-3. Risk Classification Scheme

6.7.4 Once the assessment of acceptability of the risk has been completed for all the identified hazards, the results, including the rationale for the classifications chosen, should be recorded in the hazard log. It is particularly important that all cases where the risk has been accepted as ALARP and tolerable are well documented, and that the justification for the decision is clearly specified.

6.8 STEP 6 – RISK MITIGATION

6.8.1 As already noted in Step 5, if the risk does not meet the pre-determined acceptability criteria, an attempt should always be made to reduce it to a level which is acceptable, or if this is not possible, to a level as low as reasonably practicable, using appropriate mitigation procedures.

6.8.2 The identification of appropriate risk mitigation measures, requires a good understanding of the hazard and the factors contributing to its occurrence, since any mechanism which will be effective in reducing risk will have to modify one or more of these factors.

6.8.3 Risk mitigation measures may work through reducing the probability of occurrence, or the severity of the consequences, or both. Achieving the desired level of risk reduction may require the implementation of more than one mitigation measure.

6.8.4 The possible approaches to risk mitigation include:

a) revision of the system design;

b) modification of operational procedures;

c) changes to staffing arrangements; and

d) training of personnel to deal with the hazard.

6.8.4.1 The earlier in the system life cycle that hazards are identified, the easier it is to change the system design if necessary. As the system nears implementation, changing the design becomes more difficult and costly. This could reduce the available mitigation options for those hazards which are not identified until a late stage of the project.

6.8.5 As noted in Chapter 5, the effectiveness of any proposed risk mitigation measures must be assessed by first examining closely whether the implementation of the mitigation measures might

introduce any new hazards, then repeating steps 3, 4 and 5 to evaluate the acceptability of the risk with the proposed mitigation measures in place.

6.8.6 Essential mitigation measures which are necessary for the system to meet the safety assessment criteria re often referred to as *safety requirements*. Implementation of the system cannot proceed until all these safety requirements are met.

6.8.7 Once the system is implemented, particular attention should be paid, when evaluating the results of safety performance monitoring, to verifying that the mitigation measures are working as intended.

6.9 STEP 7 – DEVELOPMENT OF SAFETY ASSESSMENT DOCUMENTATION

6.9.1 The purpose of the safety assessment documentation is to provide a permanent record of the final result of the safety assessment, and the arguments and evidence demonstrating that the risks associated with the implementation of the proposed system or change have been eliminated, or have been adequately controlled and reduced to a tolerable level.

Note.- This presentation of the arguments and evidence to demonstrate safety is referred to in many references on safety management as a safety case*. The term* safety argument *is also sometimes used with a similar meaning.*

6.9.2 While the documentation of the safety assessment is listed here as the last step, a significant amount of the documentation will already have been produced during the previous steps.

6.9.3 In addition to describing the outcome of the safety assessment, the documentation should contain a summary of the methods used, the hazards identified, and mitigation measures which are required to meet the safety assessment criteria. The hazard log should always be included. The documentation should be prepared in sufficient detail that anyone reading it will be able to see not just what decisions were reached, but what the justification was for classifying risks as acceptable or tolerable. It should also include the names of the personnel involved in the assessment process.

6.9.4 The individual who is responsible for ensuring that safety assessment is undertaken and signing the final acceptance of the safety assessment will vary depending on the size and complexity of the project, and the policy of the organization. In some cases it will be the project manager. Where no project manager has been appointed, it could be the line manager who is responsible for the system concerned. In some organizations, the acceptance may require the approval of a higher level of management in cases where the residual risk cannot be reduced to the acceptable level, but is to be accepted as tolerable and ALARP.

6.9.5 The signing of the safety assessment documentation by the responsible manager, to indicate acceptance is the final action in the assessment process.

APPENDIX A TO CHAPTER 6

ID	Hazard Identification	Consequences	Probability	Severity	Safety Objective (max. tolerable probability)	Risk Mitigation Measures	Re-Risk Assessment (Severity / Probability)	Remarks	Date of Identi-fication

APPENDIX B TO CHAPTER 6

GUIDANCE MATERIAL ON CONDUCT OF GROUP HAZARD IDENTIFICATION AND ASSESSMENT SESSIONS

(*From EUROCONTROL EATMP Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01-00*)

THE ROLE OF THE ASSESSMENT GROUP

It is usually best to initiate the assessment process in a group session, involving representatives of the various organisations concerned with the specification, development and use of the system.

The interactions between participants with varying experience and knowledge tend to lead to broader, more comprehensive and more balanced consideration of safety issues than if the assessment is conducted as a desk study by an individual.

While group sessions are usually good at generating ideas, identifying issues and making an initial assessment, they do not always produce these outputs in a logical order. Also, it is difficult for a group to analyse the ideas and issues in detail ─ it is hard to consider all the implications and inter-relationships between issues when these have only just been raised. Much time can be wasted in highly technical discussions which may turn out to be irrelevant.

It is therefore recommended that:

- The group session should be used to generate ideas and undertake preliminary assessment only (perhaps identifying factors which are important, rather than working through the implications in detail).
- The findings should be collated and analysed after the session. This should be done by one or two individuals with sufficient breath of expertise to understand all the issues raised, and a good appreciation of the purposes of the assessment. The person who facilitated or recorded the session will often be best able to perform this task.
- The collated results should be fed back to the group, to check that the analysis has correctly interpreted their input, and to provide an opportunity to reconsider any aspects once the 'whole picture' can be seen.

ASSESSMENT SESSION PARTICIPANTS

As illustrated in Figure I-4, the sessions need to involve representatives of all the main parties with an interest in the system and its safety. Typically, a session should involve:

- **System users:** ATCOs and Flight Crew (where necessary), to assess the consequences of failure(s) from an operational perspective;
- **System technical experts**, to explain the system purpose, interfaces and functions;
- **Safety and human factors experts**, to guide in the application of the methodology and to bring wider experience of the causes and effects of hazards;

- A '**moderator**' or '**facilitator**' to lead the session. His/her main tasks will be:
  - To guide the meeting through the different steps of the assessment process;
  - To keep the discussion centred on the question "What if?", i.e. on considering the effects of the different failure modes of the assessed functions;
  - To ensure comprehensive and balanced consideration of each function;
  - To encourage relevant contributions and ensure that all participants have an opportunity to put their views.
- A **meeting secretary**, to record the findings, and assist the facilitator in ensuring that all aspects have been covered.

Moderating sessions is not an easy task ― the challenges include:

- Keeping within the time schedule without omitting or rushing through important issues;
- Maintaining a structured approach, and keeping the discussion relevant, without suppressing new and unexpected ideas;
- Allowing all participants an equal opportunity to contribute.

Ideally a well experienced and trained moderator should be used.

SESSION PSYCHOLOGY

Some consideration of the individual and group psychology involved an assessment session is helpful in understanding how to run a successful session.

The mental processes required from each participant in order to produce the desired outputs can be categorised under two broad kinds of thinking:

- **Creative (inductive) thinking:** This is important in the identification of failure(s), sequence of events and the hazards that may result. The basic type of question being asked is **'What could go wrong?'**. Section A.3.1 provides additional guidance for this process.
- Judgmental (deductive) thinking. This is important in classifying the severity of hazards and in setting the Safety Objectives. The basic questions are **'How severe are the effects of this sequence of events'**. Section A.3.2 provides additional guidance for this process.

The above are cognitive processes, undertaken by each individual participant, but the **group dynamics** of the session are also important in determining its success. (see section A.3.3)

The Creative Process - Identifying What Could Go Wrong

Creative thinking is necessary to ensure that the identification of potential failures, and the potential resulting hazards is as comprehensive as possible. It is important to encourage participants to think widely and imaginatively around the subject, initially without analysis or criticism.

Typically, this is achieved by a process of structured brainstorming. The structure should both ensure completeness and encourage (not constrain) wide-ranging thinking about the system.

In an assessment session, the highest level of structure is dictated by the need for systematic consideration of each function of the system. To ensure completeness, it is often useful for the facilitator to lead the session through other, or more detailed, ways of considering the system. Examples of such lower-level structuring include:

- Consideration of other 'dimensions' of the problem, such as flight phases or operational scenarios. This helps to prevent participants becoming too 'locked in' to a mental model based purely on system functions.
- Prompt words, expressing what can go wrong, can be applied to each function of the system. Guidance Material B suggests prompt words for the identification of failures. Wherever the combination of function and prompt word leads to the identification of a credible failure, the session should go on to discuss what hazards may arise from that failure. { *Note.- Should these guide words be included as another appendix?*}
- Participants should be encouraged to think beyond their own experience, considering how others might used the system and the errors they might make. To help with this, and to overcome any inhibitions participants may have about mentioning errors which they themselves have made, it can be helpful to ask what errors others ― such as an inexperienced or fatigued controller or a pilot under stress ― might make.
- Participants can be prompted to recall relevant incidents they have experienced or heard about. It may be helpful for the facilitator to outline a few examples and ask for others.
- Participants should be encouraged to consider latent and organisational failures as well as the more obvious (active) failures manifested during operation. Some prompt words are suggested in Guidance Material B.
- Participants should also be encouraged to compare potential resulting effects considering the possibility to detect or not a failure occurrence.
- Where a comparative approach is being taken ('Is the system as safe as what currently exists?') it is useful to begin the session by brainstorming what are the key differences between the existing and proposed systems. This can also be helpful where a FHA has already been performed for a similar system, especially by the same group, or when considering a number of variants, as it helps avoid repetition.

A recurrent problem in designing FHA sessions is how to cover all the possible combinations of failures, prompt words and other ways of breaking down the problem in the time available. Rather than working through all combinations exhaustively, it may be adequate to talk through the detailed breakdown or prompt list in the introduction, but only work through a broader grouping in the session itself.

Judgements about how detailed a list of potential failure modes should be used, and hence how much time should be devoted to the FHA session, should take into account the status of the system development (how much detail is required) and its potential to cause significant risk.

More detailed prompts can always be introduced at later iterations of the assessment process as the design develops; the main danger to be avoided is that of overlooking significant failures at an early stage.

The session organiser should conduct a 'dry run' of the process before the session. By working through a few combinations of functions and keywords, either as a mental exercise or with one or two colleagues, the organiser should be able to check the applicability of the keywords and gauge how much information or discussion each combination is likely to generate. {*Does organiser = facilitator?*}

In such cases users may group the failure modes into a smaller number of prompts, taking care to ensure that the reduced list spans all the possibilities in the full list.

Reminders of the full list can be provided on posters around the room, or on handouts. The facilitator can draw specific attention to such lists if the flow of ideas seems to be exhausted prematurely.

Judgmental Thinking ─ Classifying Risks and Setting Safety Objectives

The aim of this part of the assessment session is to elicit subjective judgements, in such a way as to make the best use of people's knowledge and experience, and to minimise ─ or at least reveal ─ any biases or uncertainties.

Where the functions and hazards are complex and closely inter-linked, session designers should consider running the judgmental part of the session some time after the creative part, to give time to collate the results into a concise form. If this is not possible, the session leaders should make sure they have an opportunity (during a break, for example) to do some preliminary collation of the findings.

Where the functions and hazards can be simply expressed and are clearly distinct, it is generally better to make the risk classification judgements for each hazard at the same time as it is identified, since the participants will have the risks in mind.

The group may initially find it difficult to agree on any severity level. It is often easier to agree on the possible range of values which could be taken, or those which are clearly not correct. For example, all members of the group may agree that the hazard cannot possibly be above the severity level 2. This range can then be narrowed down to a single consensus value.

Where a consensus cannot be reached, this should be documented. However, lack of consensus often indicates that the hazard has not been clearly defined, such that participants have differing ideas of what it entails. It may be possible to resolve this in the meeting by defining the hazard more carefully, or by defining more than one hazard to represent each of the different interpretations.

The hazard classification judgements should be tested for consistency with those for other hazards. The relative order of severity implied by the classifications should also be looked at, as an indication of the overall balance and correctness of judgements.

In general, sessions do not need to elicit quantitative information in any detail, but there is a large body of literature on techniques for doing this if required.

Group Dynamics

These aspects apply to both the creative and the judgmental aspects of the session.

- **Understanding of the process and motivation for attendance.** It is important that participants have a common purpose. A pre-meeting briefing should be circulated explaining the purpose and importance of the session, and this should be underlined in the introduction on the day. Facilitators should be aware that, despite such briefings, individuals may still have other motivations for attendance.
- **Group size.** The size of group is principally determined by the areas of expertise required. However, groups of more than ten or so can be very difficult to control; they tend to break up into sub-groups, and there may be insufficient time for each individual to cover their points in adequate depth. A group of less than three (in addition to the facilitator and secretary) is unlikely to have sufficient breadth of expertise and experience.
- **Dominance and reticence.** Some individuals may dominate the conversation, others may be reticent, especially about dissenting from a perceived consensus view. Personality, and the hierarchical relationships between individuals, should be taken into account in selecting participants ─ the aim should be to have a reasonably equally-matched set of individuals.
- **Defensiveness.** Participants closely involved with the development of a system or its current equivalent may find it hard to admit that things could go wrong. It should be stressed that the

identification of a potential hazard should not be seen as a criticism of any work already carried out or of current practice.

- Giving positive feedback during the session is important. All contributions should be seen to be valuable. It is helpful to write down key points visibly (on a flipchart, for example) such that participants know their points are being recorded. This can also be used as a way of pointing out that an issue has already been covered. Irrelevant issues should be passed over quickly, but not criticised destructively.
- **Confidentiality.** Where representatives of different organisations are present, the facilitator should be aware of possible issues which may affect what participants feel able to say.

GENERAL PRACTICALITIES

The importance of the practical arrangements for the session should not be underestimated. Factors to consider include:

- Location and timing of the session to minimise inconvenience and travel cost.
- Space, comfort, visibility and audibility in the meeting room.
- Providing adequate breaks and refreshments. The attention span and fatigue of the facilitator and secretary should be considered, as well as that of the participants.
- Making allowance for participants being unavailable at the last minute. It is in the nature of FHA sessions that many participants will have operational responsibilities which may have to take precedence. As it can be extremely difficult to find another time when all can be present; potential substitute attendees should be kept in reserve.
- Provision of visual and other aids. An overhead projector, flipchart and whiteboard should be available. Electronic boards and computer projectors can be used to very good effect, enabling participants to see exactly what is being recorded and confirm that the points they make are correctly understood.
- Variety is important in maintaining attention and motivation. Where a session is longer than half a day, designers should consider using varying the structure of the session, for example by using a different 'dimension' as in Section A.3.1 in order to introduce variety, as well as for reasons of comprehensiveness.
- Varying the presentation of the session and its findings can also be helpful. For example, the facilitator and secretary could alternate roles for each session — this also helps maintain the facilitator's enthusiasm for the task. One session could be conducted using overhead slides and a flipchart, another using the computer projector. Participants should be encouraged to make use of the various aids, for example by inviting them to draw on the flipchart to explain a point.

GUIDANCE MATERIAL B

IDENTIFICATION OF POTENTIAL FAILURES

Failures can be identified by systematically applying a list of prompt words, expressing the various modes of failure, to each function of the system.

Some general categories of failure modes are listed in Table I-2.

Errors of input	Errors of output
Failure to start	Misdirection of data
Failure to stop	Delayed operation
Failure to switch	Inadvertent operation
Loss or unavailability of input	Intermittent or erratic operation
Loss or unavailability of output	Premature operation
Partial loss	Out of sequence
Corruption of data	Erroneous updating
Misunderstood	Misheard
Used beyond intent	Inconsistent information
Modified operation	

Table I-2. Examples of Generic Failure Modes

Virtually every type of failure mode can be classified into one or more of these categories, but the list is not necessarily exhaustive. The user should consider whether additional modes apply to the system being considered.

In addition these generic definitions will sometimes be too broad for definitive analysis. Consequently, they will need to be expanded and instantiated for the specific domain of application (e.g., communication, surveillance, ...)

It will be also necessary to distinguish “detected” and “undetected” failures.

The list of failure modes covers both active and latent failures. For example:

- MISUNDERSTOOD has both an ‘active’ interpretation (e.g., ‘how might a controller misunderstand this alert?') and a latent one (‘how might future users misinterpret the purpose of this procedure?').
- USED BEYOND INTENT should prompt ideas about how a future operator might try to use (or misuse) the system in a way not considered by the designers.
- MODIFIED should prompt consideration of how future users might try to modify the system, without appreciating the design rationale.

Latent failures require particular attention and emphasis in FHA sessions, as it is generally much easier to think of active failures.

Ideally, a detailed list of failure mode prompts, such as that in Table I-3 should be applied to each function, but it is recognised that this may not be practical, given the number of functions to be considered and the time available.

Where reduced lists of prompts are derived, it is helpful to draw the attention of FHA session participants to the full list, at least in the introduction to the session and possibly by providing handouts or other reminders for use during the session (see Guidance A).

APPENDIX C TO CHAPTER 6

TECHNIQUES FOR HAZARD ASSESSMENT

This Appendix contains an extract from the *Airservices Australia Safety Management Manual* (Specifically, Section 4 of *AA-REC-SAF-0105, Safety Assessment*). It describes several techniques which can be used in hazard analysis process, together with examples specific to their assessment of ATS systems.

There are some differences in terminology that used in the main body of the manual; however, the underlying principles are consistent with what is recommended in the manual.

This Appendix provides different examples of criteria for classifying the likelihood and severity of hazards, and the acceptability of risk. It also makes specific reference to Australian and New Zealand standards for safety management. Similar national standards exist in a number of other countries.

Note.- The Appendices in the original Airservices document have been re-named Attachments, and the references to them changed accordingly, to avoid confusion with the Appendices of the manual.

4. Specific Techniques (*For Hazard Assessment*)

4.1 Preliminary Hazard Analysis (PHA)

PHA is used to identify the hazards, hazardous situations and events that can cause harm for a given activity, facility or system. It is usually carried out early in the development of a project when there is little information on design details or operating procedures, and it can often be a precursor to further studies.

PHA can also be useful when analysing existing systems or prioritising hazards where circumstances prevent a more extensive technique from being used.

A PHA can use the FMEA technique to formulate a list of hazards and generic hazardous situations by considering characteristics such as:

- operating environment
- interfaces among system components etc
- equipment employed
- layout

The method then identifies possibilities for accidents, qualitatively evaluates the extent of injury or damage form these, and identifies possible remedial measures.

Reference AS/NZS 3931 : 1998

4.2 Fault Mode Effects Analysis (FMEA / FMECA)

4.2.1 Introduction

Fault Mode Effects Analysis or Failure Modes and Effects Analysis (FMEA) is a fundamental hazard identification and frequency analysis technique which systematically identifies all the fault modes of individual component and their effects on both on other components and the system.

It is primarily qualitative, although it can be quantified. It is sometimes supplemented with a Critical Items List (CIL) or criticality analysis, and then is termed FMEA/CIL or Fault Mode Effect and Criticality Analysis (FMECA).

4.2.2 Objectives

FMEA and FMECA are methods for working bottom-up from a fault or undesired action to estimate their top level effect on a system and/or procedure.

4.2.3 Value

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/FMECAs work bottom-up from an assumption of the occurrence of faults.

The techniques can be used to pinpoint the likely impact on safety as a result of failure anywhere in a system. The technique can also assist in quantifying the probability of occurrence of the hazard.

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

4.2.4 When to use FMEA

FMEAs and FMECAs are directly relevant to safety risk analysis of hardware, software, and system interfaces, and they are often the basis for hazard analyses. The techniques can be used to pinpoint the likely impact on safety as a result of failure anywhere in a system.

4.2.5 Limitations

The major disadvantages are that

- It is difficult to deal with redundancy - the process can only tolerate a small amount of redundancy before it becomes cumbersome to perform.
- It is difficult to deal with the incorporation of repair actions.
- The technique focuses on single component failures, and many of the faults and consequences analysed may not be safety-related so considerable effort must be expended to sift out those not relevant to safety.
- Typically human errors are not considered in these analyses, although this is just the practice - it is not inherent in the approach.

4.2.6 Procedure

FMEA/FMECA requires complete and accurate modeling of the system under consideration, along with detailed knowledge of the operation of the system and any associated systems.

The essential feature in any FMEA/FMECA is the consideration of each major part/component of the system, how it becomes faulty (the fault mode), and the effect of the fault mode on the system (the fault mode effect).

If criticality analysis is included, each fault mode is ranked according to the combined influence of its probability of occurrence and the severity of its consequences.

4.2.7 References

IEC 60812:1985-07, AS/NZS 3931:1998

4.2.8 Template

FMEA Template

4.3 Using AS/NZS 4360 for risk to provision of an Air Traffic Service

4.3.1 Background

This categorization scheme uses Australian Standard AS/NZS 4360, and relates to the **loss of a function, and its effect on the provision of an Air Traffic Service,** not individual components of a function. They are NOT directly related to aircraft collisions. HAZid is a more suitable

method when considering aircraft collision, as the consequence of collision would be presumed to be of the highest category.

4.3.2 Two types of ATS risks

ATS systems can be divided into two broad types :

Type	Are ATS systems which …..	Risk assessment
ATS systems for aircraft separation	support the primary air traffic service function of maintaining safe aircraft separation these include: • communications systems • radar • flight data • ATS staff, etc	Using AS/NZS 4360 The following likelihood classifications, severity categories, and acceptability criteria matrixes are available for application in Airservices Australia
Pilot interpreted ATS systems	do not support the separation function, for example • approach and landing aids Information from these systems is pilot interpreted	The JAR25 approach described elsewhere in this document may be used for Pilot interpreted ATS systems.

4.3.3 Quantitative and qualitative analysis

Risk analysis may be quantitative or qualitative depending on the risk information and data readily available, the magnitude of the hazard, and other factors.

Use of quantitative data helps clarify most decisions, and should be used where available, however some of the most important factors in a decision can be impractical to quantify. Care should be taken to consider these factors also.

Often when examining people and procedures in the provision of a separation service, in practice qualitative descriptions and comparison scales are all that are available.

4.3.4 Likelihood classification

The following table depicts the likelihood classification which may be used for ATS qualitative analysis, and presents associated quantitative likelihood values for the ability to continue to provide an air traffic separation service. Importantly, this classification relates to the **loss of a function,** not individual components of a function. These probability values are NOT directly related to the likelihood of a collision.

Likelihood Class	**Qualitative definition**	**More frequent than once per…**	**Quantitative value (likelihood per operational hour per sector/unit)**
Frequent	Likely to occur often	**hour**	$Ps > 10^{-3}$
Probable	Likely to occur many times during system life	**day**	$10^{-3} > Ps > 10^{-4}$
Occasional	Likely to occur sometimes during system life	**month**	$10^{-4} > Ps > 10^{-5}$
Remote	Unlikely to occur, but possible	**year**	$10^{-5} > Ps > 10^{-6}$
Improbable	Very unlikely to occur	**ten years**	$10^{-6} > Ps > 10^{-7}$
Extremely Improbable	Extremely unlikely, if not inconceivable, to occur	**hundred years**	$Ps < 10^{-7}$

4.3.5 Consequence/ severity categories

The following category definitions are related specifically to the ability to provide an air traffic separation service.

Note:

1. Before undertaking consequence analysis, the length of time failures need to last to result in an unacceptable reduction in service should be determined

Consequence Criteria

State Category	Air Traffic Control State	ATS System State	Barrier State	Operational State
Category 1	Sudden inability to maintain any degree of air traffic services (including contingency separation measures) within one or more airspace sectors for a significant time*.	Loss of ability to communicate with aircraft and controllers have no possible means of providing a separation service	If a Loss of Separation exists or results from this state, it can only be resolved by the pilot(s) relying on TCAS alerts, see and avoid or air/air communication	Pilots will have to resort to company or TIBA procedures. Previously established separation may remain effective for the duration of the state. Software is unlikely to cause such a catastrophic category one failure, given the levels of built in fail soft redundancy
Category 2	The ability to maintain air traffic services is severely compromised within one or more airspace sectors without warning for a significant time*.	• Loss of surveillance • Undetected credible corruption of control data • Incorrect procedures	ATC may be alerted to a Loss of Separation (e.g. by STCA, if available) and take appropriate action.	ATC may be relying on incorrect flight information to make control decisions, or following procedures which are wrong, such that a Loss of Separation could result. Contingency separation measures can be applied but the risk of infringing safe operations is extremely high until traffic has been curtailed to lower levels
Category 3	The ability to maintain air traffic services is impaired within one or more airspace sectors without warning for a significant time*.	• Human Factors Error • Loss of control or flight data • Loss of FDP (centralised)	If a Loss of Separation exists or results, it can be resolved by ATC	ATC workload is likely to be increased owing to loss of functions for maintaining planned separation or due to unplanned external factors and increased separation may be necessary. ATC procedures are able to compensate for the loss of function.
Category 4	No affect on the ability to maintain air traffic services in the short term, but the situation needs to be monitored and reviewed for the need to apply some form of contingency separation measures if the condition prevails.	• Reduced redundancy • Unplanned loss of backup system	If a Loss of Separation exists or results, it can be resolved by ATC	No loss of ATC functionality, but there is a lowering of risk margins. System failures in this state could lead to a higher state.

4.3.6 Risk matrix and decision criteria

When the likelihood and the severity of the hazard have been estimated using the previous two matrixes, the following risk matrix is available as a decision tool for management decisions. As well as decisions about existing ATS systems and procedures, this matrix may be of use in deriving functional level safety requirements for new systems (Document AA-PROC-SAF-0104 refers)

Likelihood of event per operational hour per sector/unit		**Severity Category**			
If qualitative estimated used	**If quantitative estimate used**	**Cat 1**	**Cat 2**	**Cat 3**	**Cat 4**
Frequent	$Ps > 10^{-3}$	A	A	A	C
Probable	$10^{-3} > Ps > 10^{-4}$	A	A	B	D
Occasional	$10^{-4} > Ps > 10^{-5}$	A	A	C	D
Remote	$10^{-5} > Ps > 10^{-6}$	A	B	D	D
Improbable	$10^{-6} > Ps > 10^{-7}$	B	C	D	D
Extremely improbable	$Ps < 10^{-7}$	C	D	D	D

4.3.7 Decision criteria

The following table sets out the decision criteria available for management use by Airservices.

Class	**Description**
A	Risk unacceptable, action required to treat the risk.
B	Undesirable, but may be accepted in exceptional circumstances with the approval of the Head Air Traffic Controller (HATC), Chief Engineer or Chief Fire Officer as appropriate. Contingency plans and procedures must be developed
C	May be accepted with the endorsement of the local Operating Authority. (Most often the Centre Manager, or Manager Towers). Contingency plans and procedures must be developed.
D	Acceptable

4.4 Risk Assessment of ATS Procedures

4.4.1 Background

ATC procedures are an integral element of the National Airways System. Air traffic controllers and other ATC staff use these procedures to:

- apply separation standards;
- provide efficient and orderly traffic flow;
- communicate between ATS and pilots; and
- coordinate between units or sectors to exchange information or transfer responsibility for aircraft;

Both ATC staff and pilots use a variety or procedures, equipment and systems to execute tasks associated with air traffic control. Each of these must be safe, and compatible with others they affect.

4.4.2 Purpose

This section provides general guidance on the risk assessment, risk management and development of these procedures.

4.4.3 Objective of risk assessment

The objective of assessing ATS procedures is to provide assurance that, as far as reasonably practicable, Airservices has identified and analysed potential hazards associated with the control of aircraft and put in place actions to mitigate the significant risks associated with the hazards.

4.4.4 References

The following is based on material from:

- ICAO Doc 9689-AN/953 Manual on Airspace Planning Methodology for the Determination of Separation Minima
- Mr. David Gleave of Aviation Hazard Analysis UK; and
- UK NATS Safety Management Manual.

4.4.5 General development of procedures

When management propose to develop, validate, change or introduce procedures into operational use, where practicable, they should:

- use simulation to develop and evaluate new procedures;
- utilise hazard identification, risk assessment and risk management techniques prior to introduction of the procedure;
- implement changes in relatively small, easily manageable steps to allow confidence to be gained that procedures are suitable; and
- commence changes in periods of low traffic density.

4.4.6 When to conduct risk assessments

Formal risk assessments must be performed for:

- significant changes to ATS procedures compared with current operations;
- significant changes to equipment used to execute ATS tasks compared with current operations; and
- when changing circumstances, such as increased traffic levels, different aircraft performance etc. indicate that existing procedures may not be appropriate.

The depth and detail of the assessment must be appropriate to the area of consideration.

4.4.7 Who should be involved

Risk assessment of ATS procedures is best conducted by a group including:

- those responsible for procedure design;
- staff with current knowledge and experience of the procedural area under assessment i.e., system users - ATS and pilots to assess the procedures from an operational perspective;
- engineering specialist - to provide expert opinion on equipment performance;
- safety/risk specialist - to guide the application of the methodology; and
- human factors specialist.

For a major assessment, a ‘facilitator’ may conduct the assessment session. The facilitator’s task is to:

- keep the discussion focused on the subject system function(s);
- assist in stimulating a thorough and systematic search for hazards; and

- guide the meeting through the different steps of the risk assessment process.

Importantly, a 'recorder' should be assigned to record the process undertaken and the outcomes.

4.4.8 Recording of process and results

Results of the risk assessment must be recorded along with:

- the process employed;
- the rationale on which judgments are based; and
- the names and the background of those exercising the judgments.

If hazards are identified a hazard log must be created which records these hazards and the results of subsequent steps in the process to manage the risk associated with these hazards.

4.4.9 Safety Requirements

During the design process, a procedure may be altered as a result of inclusion of identified Safety Requirements. Safety Requirements are those essential actions, procedures, performance requirements or standards that must be met to ensure the safety of the procedure.

The record should indicate whether each Safety Requirement is met or not met. Those not met should have an indication of how and when they may be met in future.

4.4.10 Procedure

Risk assessment of ATS procedures involves the following steps.

Step 1	Identify whether the change involves a change in control procedure, change in equipment, or both.
Step 2	Breakdown the procedures into manageable components. For example, control procedures might be divided into: • transfer of control procedures • coordination procedures • radar procedures • holding procedures • speed control procedures • runway procedures, etc. Equipment user procedures might be divided into: • set-up procedures • operations under normal and emergency conditions • operations under equipment failure or partial failure conditions, etc.
Step 3	Identify potential hazards which affect the ability to maintain safe separation. This is best achieved by the group asking "What can go wrong?" and "What if...?" in relation to the identified divisions in Step 2. Flight threads can also be useful in breaking down the change and examining the effects on different phases of flight. The HAZid methodology may also be used to identify hazards. Note however, that if the HAZid methodology is used in this step then steps 4 and 5 should also be undertaken in accordance with HAZid The group should adopt a balanced perspective, avoiding extreme views, and consider the impact of the procedure on all levels of controller ability and experience.
Step 4	The group identifies the circumstances or incident sequence under which a hazard might occur together with the likelihood of occurrence. Refer guidance on likelihood and consequence tables. Given these circumstances, some identified hazards may be discounted as unrealistic. Reasons for discounting must be recorded.
Step 5	The group makes an assessment of the hazard severity. Refer guidance on likelihood and consequence tables.
Step 6	The group examines the hazard and incident circumstances and identifies essential and desirable measures which, when implemented, will mitigate or eliminate the hazard. These essential mitigation or elimination measures are listed as Safety Requirements and given a unique reference number to aid traceability.

4.5 HAZid

4.5.1 Introduction

Risk assessment and risk management of ATS procedures with HAZid involves working through the following processes:

- hazard identification;

- hazard analysis, including analysis of likelihood of occurrence;
- consequence identification and analysis;
- assessment against risk criteria; and
- risk management.

4.5.2 HAZid Method

HAZid (Hazard Identification) is based on a development of the Hazard and Operability (HAZOP) procedure. The procedure uses keywords or prompt words to systematically generate possible deviations from the norm for ATS and flying tasks. The procedure then examines the effect of each deviation on air traffic related safety.

HAZid is a relatively thorough "top-down" technique because it breaks down activities associated with implementation of ATS procedures into smaller components and identifies their potential failure modes and their effect on ATS safety. Specifically, the HAZid technique is used to identify:

- the hazards;
- the hazardous scenarios;
- the initiating events;
- possible hazard causes;
- recovery factors; and
- recovery factor failures.

Each of these is defined as follows and an example of each is shown an

Attachment 3 to this Appendix

4.5.2.1 ATS related hazards

A hazard is defined as a source of potential harm or a situation with a potential to cause loss. There are certain basic air traffic services related hazards:

- mid-air collisions;
- collisions on the ground;
- wake vortex encounters;
- turbulence events; and

- collision with the ground.

4.5.2.2 Hazardous scenarios

Hazardous scenarios describe the specific hazard under consideration. For example, when considering the mid-air collision hazard at an airport, hazardous scenarios might be:

- mid-air collision between a departing and an arriving aircraft;
- mid-air collision between aircraft on parallel approach, etc.

4.5.2.3 Initiating events

The initiating events describe the generic reasons for the hazardous scenario occurring. This may be a deviation from a flight path. For example, various initiating events for the hazardous scenarios of mid-air collision between a departing aircraft and an arriving aircraft include an aircraft busting a level restriction or an aircraft blundering off a SID or STAR.

4.5.2.4 Hazard causes

The hazard causes describe how the initiating event started. Initiating events may be caused by external influences, human error, equipment failure or procedure design mistakes that can start a chain of events which could lead to a hazard. For an aircraft blundering off a SID the cause could be an equipment failure such as a control system failure or human error such as a pilot selecting the wrong SID in the FMS.

4.5.2.5 Recovery factors

The recovery factors describe the systems available to prevent or reduce the likelihood of initiating events becoming hazardous scenarios. For a mid-air collision the recovery factors include the provision of ATC, the use of TCAS, pilot see and avoid and the flight path geometry.

4.5.2.6 Recovery factor failures

Recovery factors might fail to prevent a mid-air collision from occurring. These recovery factor failures are detailed. Recovery factor failures for TCAS could include a transponder not being fitted to one of the aircraft, or the pilot not reacting to the alerts.

4.5.3 HAZid Procedure

Step 1 External influences on a fixed flight path

HAZid begins by considering a single aircraft on a fixed flightpath. External influences to the planned flightpath are examined first. These external influence sources include:

- meteorological
- topographical
- environmental
- man-made

A checklist for each of these external influences is shown at **Attachment 1** to this Appendix. Those external influences which have an effect on the flightpath are identified and recorded

Step 2 Possible deviations from planned flight path

Once external influences to safe flight are identified and recorded, the HAZid technique moves on to consider possible deviations from the planned flightpath and how these may be caused by internal operational events. These deviations may become initiating events for hazardous scenarios. Typical sources of internal operational events include:

- ATC separation
- navigation aids
- airport design - runway
- airspace design
- aircraft design and maintenance
- aircraft operation

Hazardous scenario initiating events

A systematic search is conducted for initiating events that could lead to an operational hazardous scenario. The following elements of the active/latent failures framework developed by Prof. James Reason are used to identify causes for the initiating event

Operational Hazardous Scenario Initiating Events Causes	
Active Failures	**Latent Failures**
Human Error • Pilot • ATC Equipment failure • Aircraft • ATC Workload Procedure Design Operational failures	Management and organisational Regulatory and standards

Workload itself usually does not present a different initiating event on its own. Rather, workload affects the likelihood of human error; too high or too low a workload could lead to a higher rate of human errors of all types. These errors are already identified in other active failures.

Keywords or prompt words are used to systematically identify possible deviations from planned flight paths. **Attachment 2** to this Appendix contains a prompt list and example of keywords. The potential flightpath deviations are noted.

Possible deviations are examined through a “bottom-up” consideration of:

1. procedures in use
2. human tasks
3. equipment functionality, and
4. geometric factors.

Procedures in use

The procedures in use relate to the design of airspace, and airports, ATC procedures, and flight procedures. These procedures can lead to hazardous scenarios without additional system failures. That is, hazardous scenarios can exist without requiring deviations from normal flight paths. For example, the vertical separation buffer for the base of CTA can be 500 ft. However, wake turbulence separation is applied when an aircraft is operating up to 1,000 ft below.

Human Tasks

Human tasks may fail through various types of human error. Different techniques are available such as Procedure Design Analysis, Hierarchical Task Analysis, Integrated Task Analysis. Essentially the goals, plans and tasks to achieve the goals are recorded and displayed on an outline of the flight paths so that the relative position of each action and pilot-controller communication can be shown. Human error identification techniques are then applied to the analysis.

This is a specialist area of analysis and advice should be sought from appropriate Human Factors specialists. A simple model recognises the differences in the "normal" error rates between knowledge-based, rule based and skill-based decisions as follows:

If decision is..	it is generally described as a..	with an error rate of..
Knowledge-based	mistake	1 in 10
Rule-based	mistake	1 in 100
Skill-based	slip or lapse	1 in 1000

From Rasmussan (1983), "Skill, Rule, Knowledge. Signals, Signs, Symbols and Other Distractions in Human Performance Models" IEEE Transactions on Systems, Man and Cybonetics Vol Sec/13.

Equipment functionality

A Failure Modes and Effects analysis is normally used to analyse the influences of equipment failures upon the air traffic services system. The method is applied at the functional level to all ATS equipment, aircraft communication equipment, navigation, surveillance, flight control and power plant equipment.

Geometric factors

There are other factors which are not related to human error or equipment failure but which are still necessary for the hazard to occur. This is usually a description of the geometry of encounter. Geometry of encounter is split into two variables:

- the likelihood of lateral encounter
- the likelihood of vertical encounter at the defined lateral point.

The lateral encounter point is the plan view of where the flight paths cross. The likelihood of lateral encounter varies with the angle between the lateral encounter points and the flow of traffic along the flight path. Guidelines for determining the lateral and vertical geometry of encounter are at **Attachment 5** to this Appendix.

Air traffic procedures and any deviation from the required navigation tracking determine the size and time of the overlap between aircraft involved in an encounter.

Step 3 Identification of Hazardous Scenarios

The next stage is the introduction of all other aircraft within the air traffic control system into the planned flightpath and the possible deviation region. Hazardous scenarios arise where the flightpath of other traffic overlap the possible deviation region.

Hazard Analysis

Introduction

The hazard analysis process normally involves:

- development of fault schedules;
- construction of fault trees; and
- quantification of the likelihood of human error, equipment failure and operational factors.

Fault schedule

Attachment 3 to this Appendix is an example of a fault schedule that records the result of a hazard identification process.

Fault trees

Information contained in the fault schedule may be used to construct a Fault Tree.

The level of analysis for the fault tree will depend on the situation. However, as a general guide, a simple pessimistic model should be used initially to determine the likelihood of human error, equipment failure, and operational factors and thus the operational risk exposure. This risk exposure is then compared with the risk criteria target level of safety. If the pessimistic model produces a result which is lower than the target

criteria, then further resource allocation is not required as it would not alter the risk management decision. Effort can then be spent on allocating resources for risk optimisation. Risk optimisation is discussed later under Risk Management. **Attachment 4** to this Appendix is an example of a pessimistic fault tree.

Regardless of the level of analysis undertaken for the Fault Tree, there should be an independent audit to check the construction logic.

Consequence Analysis
Measure of consequence

Consequence is the amount of loss suffered when a hazard occurs. The amount of loss for ATS procedures related risk assessments is normally measured as the number of fatalities because this is normally the most drastic possible outcome.

Mid-air collisions and collisions with the ground

Although, on average about 50 percent of people survive a mid-air collision, a simple analysis assumes that all people on board an aircraft will die as the result of a mid-air collision and most collisions with the ground.

Collisions on the ground

Further analysis may be necessary for collisions on the ground. This involves consideration of the number of people on board and the crash survivability of specific categories of aircraft involved. However, the scope for risk optimisation of crash survivability that can be undertaken by Airservices is limited. Therefore, in the majority of cases, the initial assumption that all people on board the aircraft will die is the appropriate and pessimistic assumption for first-cut analysis.

4.5.4 Risk Criteria

4.5.4.1 Overview

Risk is be calculated as the product of the likelihood of hazardous events and the consequences of the event happening. Given the initial assumption that all people on board the aircraft will die, the target level of safety should relate to the number of mid-air collisions in a certain time frame, or the likely number of fatalities in a certain time frame.

4.5.4.2 Risk Management

Management decisions

Management must decide if:

- the risk is so great that it must be refused altogether;
- the risk is, or has been made, so small as to be insignificant (However, any actions which reduce risk and require little effort or resources must be implemented); or
- the risk falls between these two states and has been reduced to the lowest level practicable, bearing in mind the benefits flowing from its acceptance and taking into account the costs of any further reduction. This is known as ALARP, "As low as reasonably practicable".

Risk management principles Risk management has four guiding principles:

- risk limitation
- risk optimisation
- risk justification
- risk monitoring

Risk limitation

Risk limitation requires that the operational risk exposure is below the target level of safety set as policy. Should initial comparison determine that the risk is greater than the target level of safety, the risk must be reduced.

Risk optimization

Risk optimisation means considering how the likelihood or frequency of each event in the fault schedule or fault tree could be reduced, and implementing all reasonably practicable reductions. This includes:

- examining the possible causes of the initiating events to determine how the likelihood of these causes eventuating might be reduced;
- introducing additional recovery factors; or
- examining recovery factors failures to determine how the likelihood of these failures might be reduced.

Management then assesses the cost and practicality of each possible mitigation and decides whether or not to implement the mitigators based on the results of this assessment. All steps must be recorded.

Note: Essential mitigators to be implemented, once agreed, are recorded as Safety Requirements in the Safety Case.

Risk justification

The risk must be justified in terms of the population exposed to the risk and the benefits derived from exposure.

Risk monitoring

The risk must be monitored to ensure that the risk level is maintained. Implicit in the monitoring is the need to identify the events of interest, parameters, the reporting system, the analysis requirements and the change mechanism.

Attachment 1 - External Influences – Typical Sources

Meteorological			
Property	**Example**	**Property**	**Example**
Light	night dawn - sunrise dusk - sunset full daylight	Electromagnetic	lightning, thunderstorms sunspot St Elmo's fire solar winds
Wind	wind direction /speed wind gusts frontal movements boundary layer effects microbursts downdrafts/updrafts geographic waves windshear, cyclone	Water	drizzle rain hail snow ice fog
Temperature, Pressure and Density	High - reduced rate of climb Low - increased rate of climb	Visibility	Rain Sleet Drizzle Snow Fog Hail
Topographical			
Oceanic	icebergs tidal waves sea level	Terrain	mountains/hills valleys
Environmental			
Organic	birds animals	Inorganic	volcanic ash, bushfires smoke, dust storms thunderstorms, lightening, interference background lighting electromagnetic pulse
Man-made			
Free Moving (not under ATC control)	Other aircraft activities Gliders, Airships, Ultralights, Helicopters Aircraft, Parachutists Balloons, Unmanned airborne vehicles	Mobile obstacles	Other aircraft activities Airside vehicles Unmanned tugs Baggage carts Containers
Ground controlled	Laser lights Kites, Fireworks Tethered balloons Radio controlled aircraft Rockets, Firearms		

Attachment 2 - Deviation Prompt lists and keywords

ATC EQUIPMENT	surveillance air-ground-air communications ground-ground communications data communications navigation aids information systems	complete loss partial loss corruption degradation incorrect information
ATC OPERATIONS	planning radar control flight plan information ATC-ATC coordination ATC-pilot communications handovers	Action • not done • less than required • more than required • repeated • sooner than required • later than required • partly done • misordered or • other action done
AIRCRAFT EQUIPMENT	surveillance and TCAS transponder communications navigation systems flight management systems flight systems	complete loss partial loss corruption degradation incorrect information
AIRCRAFT OPERATIONS	height change course change speed change pilot-ATC communications system configuration evasive action cockpit workload	Action • not done • less than required • more than required • repeated • sooner than required • later than required • partly done • misordered or other action done

Example keywords, property words and deviations for HAZid study

Property key words	Flight level or altitude	Rate of descent	Heading	Airspeed or groundspeed
NOT DONE	flight level or altitude change not done	rate of descent change not done	heading change not done	speed change not done
LESS THAN	at lower flight level or altitude than required/requested	rate of descent lower than required/expected	track course change less than expected	slower than required/requested/expected
MORE THAN	at higher flight level or altitude than required/requested	rate of descent higher than required/expected	track course change more than expected	faster than required/requested/expected
AS WELL AS	change more than one parameter at the same time			
OTHER THAN	wrong aircraft changes flight level or altitude	wrong aircraft changes rate of descent	wrong aircraft changes heading	wrong aircraft changes speed
SOONER THAN	flight level or altitude change earlier than expected	flight level/altitude is lower/higher than expected	heading change earlier than expected	speed changes earlier than expected
LATER THAN	flight level or altitude change later than expected	flight level/altitude is higher/lower than expected	heading change later than expected	speed changes later than expected
MISORDERED	flight level or altitude, rate of descent, heading and speed changes misordered			

Attachment 3 – HAZid Example

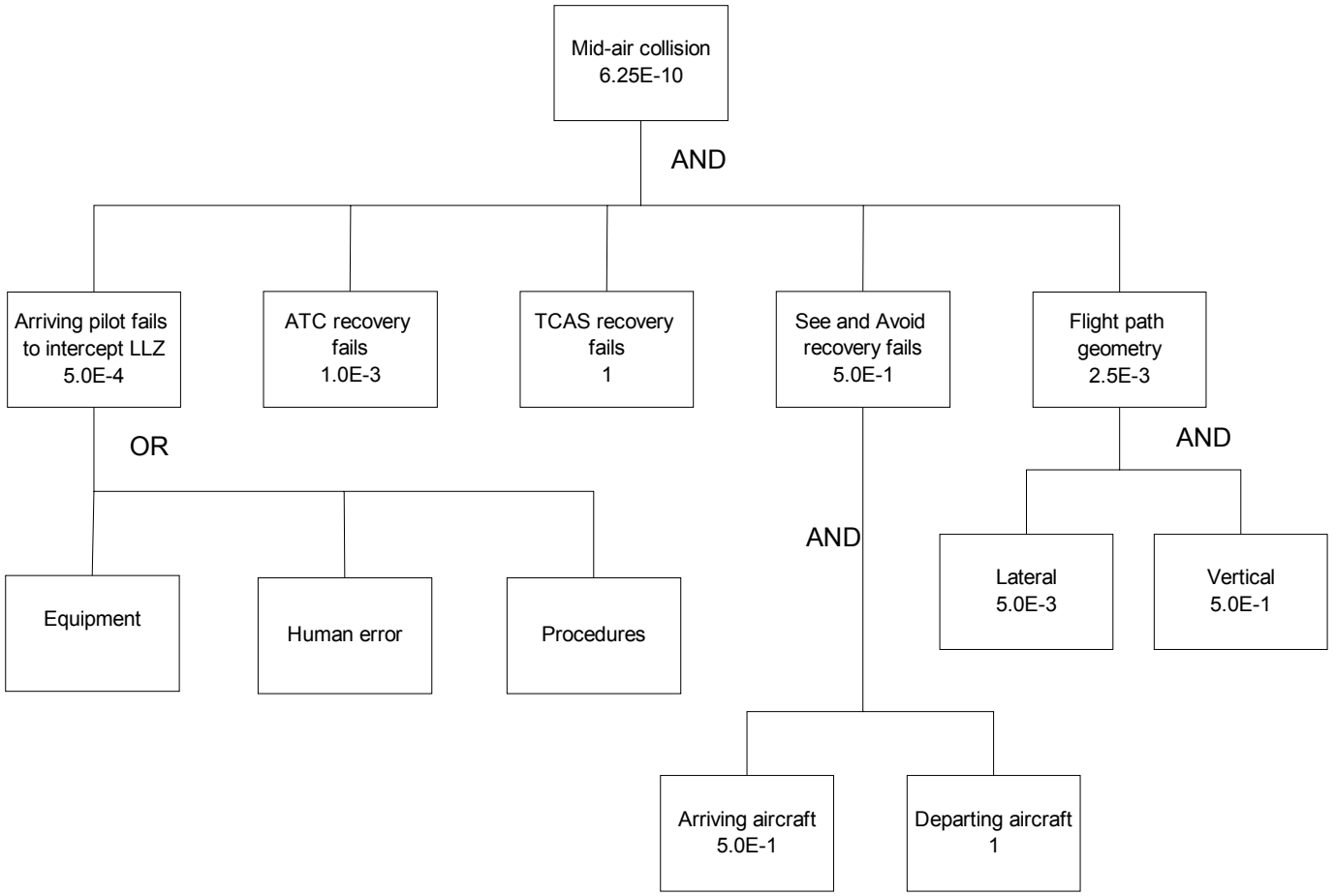
Note. – This addresses only the hazard identification process, not the subsequent steps in the safety assessment process.

Hazard Scenario H1: Mid-air collision between departing and arriving aircraft when the arriving aircraft fails to intercept the LLZ		
Initiating Event: The arriving aircraft fails to intercept the LLZ and continues to head in an easterly direction into the path of the departing aircraft		
Possible Cause of the Initiating Event:	**Recovery Factors which prevent or reduce the likelihood of initiating events becoming hazardous scenarios:**	**Recovery Factors Failure:**
Airborne equipment ILS LLZ receiver fail Flight Director fails ILS Display fails Autopilot fails **Ground Equipment** ILS LLZ transmitter fails **Human Error** Pilot selects wrong DAP plate Pilot selects wrong LLZ frequency Pilot fails to notice intercept is not successful ATC gives wrong runway Callsign confusion by either ATC or pilot ATC gives heading for establishing not compatible with aircraft avionics or manual intercept requirements	**Existing Recovery Factors** Air Traffic Control Director, ADC monitor aircraft's track Airborne Collision Avoidance Systems See and avoid Flight path geometry **Possible Additional Recovery Factors** May include other Air Traffic Control procedures/actions not yet developed. Once agreed for implementation, these are specified as Safety Requirements	**Air Traffic Control** 1. The controllers do not notice that the arriving aircraft is off track 2. The controllers do not have time to resolve the conflict even if they did notice it 3. The controllers plan a faulty strategy for recovery 4. The controllers formulate a good plan but mis-communicate between themselves in the coordination of the plan 5. The controllers make a slip in the verbal instructions to the pilot 6. The pilots make a slip or lapse associated with the controller's instruction to them 7. The pilots may not understand the instruction given to them by the controllers 8. The avoiding action turn places the aircraft beyond its flight envelope and it crashes

Hazard Scenario H1: Mid-air collision between departing and arriving aircraft when the arriving aircraft fails to intercept the LLZ		
Initiating Event: The arriving aircraft fails to intercept the LLZ and continues to head in an easterly direction into the path of the departing aircraft		
Possible Cause of the Initiating Event:	**Recovery Factors which prevent or reduce the likelihood of initiating events becoming hazardous scenarios:**	**Recovery Factors Failure:**
Procedures Wrong LLZ frequency published Publication of incorrect information in paper or electronic formats Errors in procedures design		**TCAS** 1. TCAS not fitted to either or both aircraft 2. TCAS not working on either or both aircraft 3. Transponder on other aircraft not on 4. Other aircraft does not have a transponder 5. Algorithms on either of both aircraft fail to detect other aircraft 6. Pilot does not receive or recognise alarm (RA or TA) 7. Pilot does not respond safely **See and avoid failure** 1. Crew not scanning 2. Visibility not sufficient to detect other aircraft in time 3. Conspicuity not sufficient to detect other aircraft in time 4. Cockpit cut off angles prevent flightcrew scan from detecting other aircraft

Hazard Scenario H1: Mid-air collision between departing and arriving aircraft when the arriving aircraft fails to intercept the LLZ		
Initiating Event: The arriving aircraft fails to intercept the LLZ and continues to head in an easterly direction into the path of the departing aircraft		
Possible Cause of the Initiating Event:	**Recovery Factors which prevent or reduce the likelihood of initiating events becoming hazardous scenarios:**	**Recovery Factors Failure:**
		5. Aircraft detected but not assessed as a threat 6. Avoiding action puts aircraft outside flight envelope or not effective at avoiding collision See and avoid for the departing aircraft is not considered viable due to the aircraft's view angle from the nose up attitude.
		Flight path geometry 1. No vertical separation 2. No lateral separation

Attachment 4 – Fault Tree



Note: This is an example Fault Tree Analysis (FTA). Justification must be provided for the qualitative values used within the FTA

Attachment 5 - Determining Geometry of Encounter
Lateral geometry of encounter

The lateral geometry of encounter is the likelihood that that an aircraft will be in the lateral area of conflict at the same time as an aircraft on a cross track.

The size and time of overlap are used to determine the lateral geometry of encounter. The size of the overlap depends upon the size of the aircraft and the relative flight path directions. The time of overlap depends upon the speed of the aircraft. The following calculation can be used to determine the likelihood of lateral encounter for aircraft crossing at angles between 30 and 90 degrees.

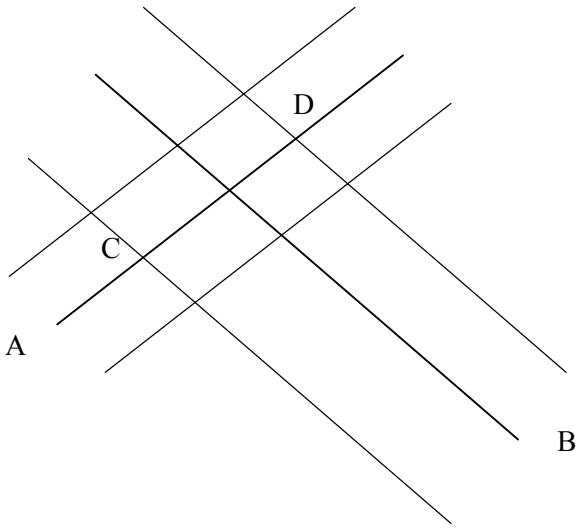
Inputs for size of overlap:

- Aircraft width
- Aircraft length
- Overlap angle

Inputs for time of overlap:

- Airspeed
- Time interval between aircraft

For example, consider the following lateral overlap scenario where aircraft A crosses track B:



Example aircraft width:	30 metres (737 size)
Example aircraft length:	30 metres (737 size)

If aircraft A crosses track B at 90 degrees there is lateral conflict from when the nose of aircraft A reached the line for the port wingtip of aircraft on track B (point C) until the tail of aircraft A passed the line for the starboard wingtip of aircraft on track B (point D). This gives an overlap distance of 60 metres. However, when the tracks cross at less then 90degrees, the conflict distance will increase. For ease of calculation, when tracks cross at angles less than 90 degrees to 30 degrees, an overlap angle of 90 degrees and a factor of 3 should be used, giving an overlap distance of 90 metres. Complete lateral overlap should initially be assumed when assessing tracks which cross at less than 30 degrees. In this case, the likelihood of encounter is 1.

An example where the aircraft cross at an angle less than 90 degrees but greater than 30 degrees follows.

Overlap distance assumed is 90 metres for B737 size.

Airspeed aircraft A:	180 knots = 90metres/second

At a speed of 90 metres/second aircraft A will be in the area of conflict for 1 second.

Time interval between aircraft on track B:	movement rate of 18 aircraft per hour gives 18 per 3600 seconds. This equates to 200 seconds between aircraft.

Therefore, the 1 second exposure time for aircraft A to be in the area of conflict is combined with the 200 second interval between aircraft on the cross track to give a value of 1 in 200. The likelihood that aircraft A will be in the area of conflict at the same time as an aircraft on the cross track is 1 in 200 or 5E-3.

Vertical geometry of encounter

The vertical geometry of encounter is the likelihood of vertical encounter at the defined lateral point. A check of the air traffic procedures and required climb/descent requirements and profiles at the defined lateral point should be undertaken to establish whether the aircraft are allocated level flight at the same altitude or climbing or descending through the defined lateral point.

Should the aircraft be allocated level flight at the same level errors within the altimeter systems would give an overlap factor of at least 2. Therefore, the likelihood of vertical encounter would be 1 in 2 or 5E-1.

5. Templates

Preliminary Hazard Analysis

Service/System	Potential Failure	Existing Mitigation	Effect on ATS	Effect on Aircraft /Flight Crew

FMEA Template

Ref No.		**Failure Mode:**	
ATS Effects	**Safeguards**	**Potential Additional Actions**	**Comments/Responsibility**
Flight Crew Effects	**Safeguards**	**Potential Additional Actions**	**Comments/Responsibility**

HAZid Template

Hazard Scenario H1:		
Initiating Event:		
Possible Cause of the Initiating Event:	**Recovery Factors which prevent or reduce the likelihood of initiating events becoming hazardous scenarios:**	**Recovery Factors Failure:**

APPENDIX D TO CHAPTER 6

SAFETY ASSESSMENT OF A VISUAL NIGHT APPROACH PROCEDURE AT ÍSAFJÖRÐUR, ICELAND

EXECUTIVE SUMMARY

This document describes the results of the safety assessment conducted for the ICAA in connection with a Visual Night Approach Procedure at Ísafjörður, Iceland.

Objective

The safety assessment constitutes an essential part of the basis for the Go/No Go decision for ICAA to implement the Visual Night Approach Procedure at Ísafjörður.

The safety assessment is based on the Safety Assessment Methodology developed by the EUROCONTROL Safety & Quality Management and Standardisation Unit (SQS). The methodology is laid down in the "EATMP Air Navigation System Safety Assessment Methodology" - SAF.ET1.ST03.1000-MAN-01-00 [ref. 3] and focuses on conduction of the first of three steps: the Functional Hazard Assessment (FHA).

The overall objective of an FHA is to determine how safe the procedure shall be by specifying the *safety objectives* of the system related to the identified hazards. That is, specifying the minimum requirements to be achieved by the procedure.

Results

Two FHA sessions were conducted.

During these sessions a total of 37 valid hazards have been identified and analysed. For each of these hazards, safety objectives have been established and it has been verified whether the hazard achieved its safety objective. The hazards have been grouped into three categories as follows:

1. Safety critical hazards

   Hazards falling into this category are hazards that do not achieve the safety objective according to the Risk Classification Scheme. Thus, the risk is considered to be NOT TOLERABLE.

2. Borderline hazards

   Hazards falling into this category are hazards that are in the borderline between NOT TOLERABLE and TOLERABLE. In this safety assessment hazards identified in this category are considered not to achieve the safety objective according to the Risk Classification Scheme.

3. Not safety critical hazards

   If hazards are achieving their safety objective they do not constitute a safety issue and it is assumed that the risk is considered to be TOLERABLE.

Eight (8) hazards achieved their safety objectives, 21 hazards were risk assessed as safety critical / NOT TOLERABLE and eight (8) hazards were risk assessed to be in the borderline to be safety critical.

Most safety critical hazards have been identified in connection with the wind conditions, the approach procedure, missed approaches, lights, birds and the localiser.

Wind conditions

Ísafjörður airport is manned with an AFIS operator. One of the responsibilities of the AFIS operator is to provide Flight Information Service to the pilots of arriving and departing aircraft. The AFIS operator shall inform the pilots of the latest wind information, i.e. wind direction and wind speed. This information will be provided by the AFIS operator from three Wind Direction Indicators (WDI) placed alongside the runway along with information from two weather stations located in the surrounding area. One of these weather stations is located on top of the mountain Þverfjall, providing the AFIS operator with the mean average wind with a 10 minutes interval, whereof the second weather station is located at Arnarnes, providing the AFIS operator with wind information according to ICAO specifications, i.e. the actual wind plus the maximum and minimum wind speed.

By the pilots at the second session it was stated that the wind information was considered insufficient. Two declarations support this statement. Firstly, the WDI placed along the runway indicates the wind at surface level, thus no derivation can be made of the wind at 800 ft, which is the altitude of the aircraft when entering Skutulsfjörður. Secondly, the indications from the wind measuring stations at Arnarnes and Þverfjall do not provide wind information that is useable for the pilots. This is mainly because of the weather station's position in an area where the wind measurements are not representative – or convertible – to the conditions to be expected within Skutulsfjörður.

To determine the wind conditions within Skutulsfjörður, during daylight operations, it is a commonly known practise to do so by visual means, in order to predict the expected wind conditions, including potential turbulence, downdraft etc. Already when flying on the LLZ, the pilots try to assess the expected wind conditions by assessing the surface of the sea. The waves and behaviour of the sea provides the pilots with valuable information, especially when approaching the missed approach point, to decide whether to continue the approach or execute a missed approach. Once inside Skutulsfjörður, the pilots continue assessing, not only the surface of the sea, but also cloud movements, drifting snow and smoke from chimneys. This assists the pilots in planning the final approach turn.

Obviously, it will not be possible for the pilots during night operations to use the same visual indications to predict the weather inside Skutulsfjörður and prepare the approach accordingly. With reference to the above, it has been identified that the wind information provided by the AFIS operator does not provide an adequate picture of the wind conditions to be expected, thus, the pilots will have no picture of the expected wind. The workload in the cockpit will increase, causing a canalised attention on wrong parameters, thus making prediction of the wind conditions one of the most safety critical hazards.

To conclude, it will be extremely difficult for the pilots to predict the wind conditions within Skutulsfjörður, during night operation. This increases the risk seen in comparison with daylight operation, where the risk is significantly lower.

Approach procedure

When flying into Ísafjörður at daylight it was recognised that the workload is significantly higher than flying into other airports in Iceland. The pilots participating at the second FHA session identified that the proposed approach procedure would enforce an extremely high workload on the pilots, thus leaving a low margin for errors. The approach procedure itself has been identified as a safety critical hazard. The approach is based on a speed of 120 knots, 25° bank angle and a descent slope of 4.75° (equals 8.3 %). The latter will require a rate of descent of approximately 1000 ft/min.

Three critical parameters exist, which will require the pilot's full attention throughout the approach turn, while at the same time the pilots shall use the visual guidance means to manoeuvre. The critical parameters are the same as above - the speed, bank angle and descent rate. Speed control is a very important parameter when executing the approach. A slight tail wind will cause an increase of the ground speed, thus an increased bank angle is necessary to complete the turn, increasing the risk of overshooting. It was recognized that the approach turn will set of the Ground Proximity Warning System (GPWS) in the cockpit, which may further increase the physical stress level of the pilots. The GPWS issues an audio warning in the cockpit. It must be noted that most aircraft types allow the pilot to shut off the GPWS. However, this introduces a number of other hazards, not part of this assessment.

Moreover, it was considered a risk that the approach turn ends just overhead the runway threshold leaving the pilots with no final approach at all. It was suggested to make a displaced threshold of approximately 200-300 meters from the runway threshold.

Compared with daylight operation, aircraft flying into Ísafjörður at night will face a higher risk, primarily due to the extremely high workload, but also because of less manoeuvring area as the pilots fly closer to the mountains during daylight operations.

Missed approach

It was recognised that the possibility of executing a safe missed approach is limited, depending on where the aircraft is flying the approach path. Should it be necessary to execute a missed approach on downwind, the pilots do have more manoeuvring space, thus the pilots will be able to make a 180° turn and fly out of Skutulsfjörður. However, if the pilots decide to execute a missed approach on base turn, the situation is more critical. The aircraft is already banking 25° or higher, depending on the speed, and is pitching down 4,75°. If the aircraft at this stage shall execute a missed approach, the bank angle will increase while at the same time full power shall be applied, to bring the aircraft into a stable climb. Furthermore, the pilots will have to visually provide separation from terrain. This will raise the already very high workload in the cockpit to a level where the pilots may not be able to perform their tasks effectively.

A number of reasons may cause that the pilots choose to perform a missed approach. The aircraft may have gotten too far outside the track, and an abruption collision avoidance manoeuvre is necessary or that a failure warning is shown in the cockpit. In case of the latter, the risk of canalised attention exists, where the pilots may tend to focus more on the failure warning, than on performing the missed approach.

It was identified that the pilots tend to fly closer to the mountain during daylight, providing more manoeuvring space, indeed also if a missed approach is necessary. It was also identified that the pilots use a landmark close to the town of Ísafjörður to navigate towards. The landmark brings the aircraft to the middle of Skutulsfjörður, allowing easy exit. It shall be noted that in connection with allowing take-off at night, a strobe light indicating the exit of the valley was installed at Hnifsdalur.

Compared with daylight operation, the risk of a collision with terrain in connection with a missed approach is significantly higher during night operation.

Lights

The approach itself is based on a number of electrical installations, all to be installed. These include obstruction lights, 18 flashing sequenced lights, PAPI lights, floodlights, high intensity runway lights and others. In the assessment it was identified that the lights are either connected to the Local Electric Power Distribution System or the Airport Power Distribution System, however with the majority of the equipment connected to the Airport Power Distribution System. The back-up time was estimated to approximately 4-5 seconds, however, the lights need an additional 2-3 seconds to reach high intensity. Note that the obstruction lights in the mountains have an instant 15-minute battery back-up.

Anything over 2-3 seconds can be considered safety critical. When the aircraft is performing the final approach turn, the pilots are relying on the flood light to indicate the mountain ridge, the PAPI light to provide vertical separation from the mountain ridge and the flashing sequenced lights guiding towards the runway threshold. All these systems are powered by the Airport Power Distribution System. In case of an outage, the pilots will have no guidance means to execute a safe missed approach. It is necessary for the ICAA to look into this issue.

This risk does not exist during daylight operations, thus no comparison of risk can be made.

Birds

It was identified that the probability of a bird strike is high especially on final approach, which is caused by two reasons. Skutulsfjörður stretches below the final approach track, which increases the possibility of bird trekking. The second reason is that a bird nesting area exists close to the runway. Bird trekking occurs from the nesting area and out to the sea, crossing the runway. Even though this safety assessment is only related to the proposed night procedure, it can be said that the bird nesting area is a hazard for daylight operations, however with a higher risk

during night approach as the pilots have no visual means of identifying the birds, thus it is suggested to remove the bird nesting area.

The risk of a bird strike may not be judged higher during night operations compared to daylight operations, however, the consequences, in case of a bird strike, can be considered higher during night operations.

Localizer

Another safety critical hazard is related to the protection of the NAV AIDS, especially the Localizer (LLZ). In the past it has occurred that people has camped close to the LLZ resulting in offset of the LLZ in worst cases. Snow has also resulted in offset of the LLZ before. It will be necessary to protect the LLZ, allowing no access to interfere with the beam. The consequences are much higher during night than compared to daylight, even though the hazard also exists during daylight when flying IMC. During daylight, the pilots may be able to see terrain allowing visually to keep clear of terrain. The pilots will also be able to observe that the LLZ if offset and report it to proper instance. During night operations neither of this is possible, hence, the risk of a collision with terrain has increased.

The risk of a collision with terrain, due to an offset localiser, can be considered higher during night operations compared to day operations.

Conclusion

The target level of safety for the visual night approach procedure has not been achieved.

INTRODUCTION

This document presents a Safety Assessment of a Visual Night Approach Procedure at Ísafjörður, Iceland.

Background

Presently, landings are not permitted during night at Ísafjörður Airport according to the AIP [ref. 01]. Ambulance and emergency flights are, however, exempted from this rule. Ísafjörður Airport does not fulfil the ICAO recommendation of airports and their vicinity according to ICAO Annex 14 [ref 02]. During current conditions risk during landing is too high.

Landing at runway 26 at night is not possible due to obstruction. The mountain in the fjord, Kubburinn is the biggest problem for the approach. In 1997 night take off from runway 08 was permitted and lighting systems and weather station were installed.

To investigate an extension of night operations at Ísafjörður Airport an investigation team of the Icelandic Civil Aviation Administration has been set up. The team has determined as its goal that the risks of night operations must have the same or less risk level as are accepted during day operations. The team has tried to meet this goal by introducing systems that give guidance during the approach, by stringent weather limitations and by setting pilot experience restrictions.

This report covers a safety assessment, which includes hazard identification of the guidance system, including improvements of the light systems, Instrument Flight Rules (IFR) and Visual Meteorological Conditions (VMC) that have been determined as requirements by the investigation team. Details about the systems are given in section 5.

Document Structure

The document is structured as follows:

- Section 3 provides a description of the process of the safety assessment including the objective and a description of the primary parts of the EUROCONTROL Air Navigation System Safety Assessment Methodology that constitute the theory behind the safety assessment.
- Section 4 gives details about the FHA sessions, which was conducted to identify potential hazards.
- Section 5 describes the proposed approach procedure at Ísafjörður Airport in detail and provides a description of the differences between night and day operations at Ísafjörður Airport.
- Section 6 describes and discusses the results of the FHA sessions, i.e. the identification of hazards and outlines all identified safety critical hazards and hazards in the borderline to be safety critical. Further, the section includes an analysis of the obtained results.
- Section 7 constitutes the summary and conclusion.

PROCESS

Objective

The objective of the safety assessment is to examine and identify potential hazards of the proposed improved systems of Ísafjörður Airport to accommodate visual night approaches.

Methodology

The safety assessment has been performed in accordance with the EUROCONTROL EATMP Air Navigation System Safety Assessment Methodology (SAM) [ref 3].

The SAM describes a generic process for the safety assessment of Air Navigation Systems. It requires using the Functional Hazard Assessment (FHA) technique. This technique is fully described in the EUROCONTROL document SAF.ET1.ST03.1000-MAN-00-00 [ref 3].

The Functional Hazard Assessment is a technique to identify and risk assess hazards that can occur in connection with the implementation of a system, or in this case, the approach procedure. In the next sections a brief walkthrough of the FHA methodology is given, providing the reader with a better understanding of the process and purpose of the FHA.

Firstly, the initial steps are described (Section 0). Secondly, details about the applied severity classification scheme and the applied probabilities are outlined (Sections 0 & 0) and finally, the safety objectives and the risk classification scheme are described (Section 0)

The FHA process

The FHA is usually conducted at the beginning of the development or modification of a system.

The overall objective of the FHA is to determine how safe the visual night approach procedure need to be by specifying the safety objectives of the prodecure. That is, specifying the minimum requirements to be achieved by the system. Thus, in this context, safety objectives specify the maximum tolerable probability of occurrence of a hazard of a given severity.

In order to specify the safety objectives, it is necessary to identify all potential failures and hazards in the procedure. This identification is carried out in structured brainstorm sessions attended by operational experts. In this respect, operational experts cover the various groups of people, who have designed/developed the system as well as groups of people who shall operate in the future environment.

Through this structured brainstorming session, facilitated by a moderator, the participants are encouraged to come forward with all concerns and thoughts related to the system. The moderator shall ensure that the session maintains a structured approach and keeps the discussions relevant without suppressing new and unexpected views/ideas.

Once all possible hazards have been identified, each of them is being assessed to determine the consequences on operation and safety.

Figure 1 below illustrates the process as described above:

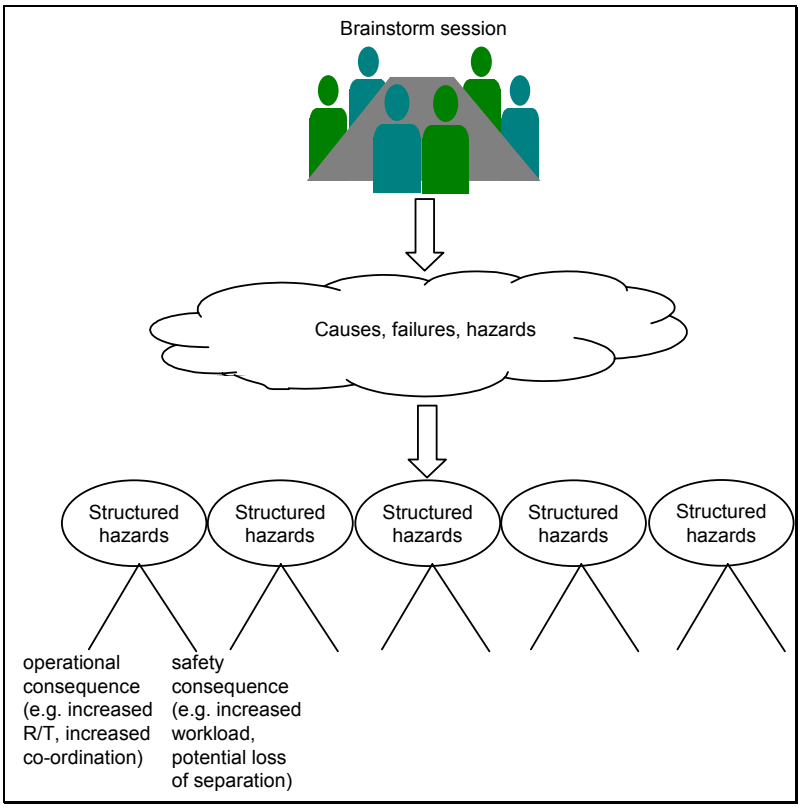


Figure 1: The FHA Process

After assessment of operational and safety consequences the identified hazards are assessed with regard to severity and probability as described below.

Severity Classification

Based on the identified consequences, each hazard is assigned a severity class. The severity class gives an indication of the impact on safe provision of ATS in case the hazard occurs.

The severity classifications used to classify hazards identified in connection with the visual night approach procedure at Ísafjörður FHA is based on the EUROCONTROL Safety Regulatory Requirement (ESARR) 4: Risk Assessment and Mitigation in ATM [ref 4]. However, the severity classification scheme of ESARR 4 was considered to be too general and does not clearly give indications to choose severity classification. In order to accommodate a more clearly classification scheme the structure and contents of the risk classification scheme of SAM [ref 3] was adopted and incorporated into the scheme of ESARR 4 [ref 4], i.e. the scheme is a combination of the two schemes. The applied scheme is shown in Table 1 below.

Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
Effects on Operations	**Complete Loss of Safety Margins**	**Large Reduction in Safety Margins**	**Major Reduction in Safety Margins**	**Slight Reduction in Safety Margins**	**No Safety Effect**
SEVERITY INDICATORS SET1: EFFECTS ON OPERATION					
EFFECT ON THE OPERATION	Result in Accident ***or*** Result in complete loss of separation from terrain or obstacle	Abrupt collision or terrain avoidance manoeuvres are required to avoid a catastrophic accident ***or*** When an avoidance action would be appropriate	Without ATC/Cockpit Crew fully controlling the situation, hence jeopardising the ability to recover from the situation (*without the use of collision or terrain avoidance manoeuvres)*	No direct impact on safety but indirect impact on safety by increasing the workload of the ATC/cockpit crew ***or*** Slight degrading the functional capability of the enabling CNS system.	No effect on the safe operation
ATCO and/or Flight Crew Working Conditions	Workload, stress or working conditions are such that they cannot perform their tasks at all	Workload, stress or working conditions are such that they are unable to perform their tasks effectively	Workload, stress or working conditions such that their ability is significantly impaired	Workload, stress or working conditions are such that their abilities are slightly impaired	No effect
Effect on Air Navigation Service within the area of responsibility	Total inability to provide or maintain safe service	Serious inability to safe provide or maintain service	Partial inability to provide or maintain safe service	Ability to provide or maintain safe but degraded service	No safety effect on service

ATCO and/or Flight Crew Ability to Cope with Adverse Operational and Environmental Conditions	Unable to cope with adverse operational and environmental conditions	Large reduction of the ability to cope with adverse operational and environmental conditions	Significant reduction of the ability to cope with adverse operational and environmental conditions	Slight reduction of the ability to cope with adverse operational and environmental conditions	No effect
SEVERITY INDICATORS SET 2: EXPOSURE					
Exposure time	The presence of the hazard is almost permanent. Reduction of safety margins persists even after recovering from the immediate problem.	Hazard may persist for a substantial period of time	Hazard may persist for a moderate period of time.	Hazard presence is such that no significant consequences are expected.	Too brief to have any safety-related effect
Likelihood to experience adverse operational and environmental conditions	Frequent to permanent presence of the considered adverse operational and environmental conditions	Relatively high likelihood to experience the considered adverse operational and environmental conditions	Slight likelihood to experience the considered adverse operational and environmental conditions	Low likelihood to experience the considered adverse operational and environmental conditions	Rare presence of the considered adverse operational and environmental conditions
SEVERITY INDICATORS SET 3: RECOVERY					
Annunciation, Detection and Diagnosis	Misleading indication. Hard to detect or diagnose. Diagnosis very likely to be incorrect	Ambiguous indication. Not easily detected. Incorrect diagnosis likely	May require some interpretation. Detectable. Incorrect diagnosis possible	Clear annunciation. Easily detected, reliable diagnosis	Clear annunciation. Easily detected and very reliable diagnosis

Contingency measures (other systems or procedures) available	No existing contingency measures available. Operators unprepared, limited ability to intervene.	Limited contingency measures, providing only partial replacement functionality. Operators not familiar with procedures or may need to devise a new procedure at the time.	Contingency measures available, providing most of required functionality. Fall back equipment usually reliable. Operator intervention required, but a practised procedure within the scope of normal training	Reliable, automatic, comprehensive contingency measures	Highly reliable, automatic, comprehensive contingency measures

Table 1: Severity Classification Scheme

*Note that **large** as used in the headlines above implies a level of risk, which is greater than **major**.*

The severity classification scheme provides a framework for assessing how strongly the safe provision of ATS will be affected by the hazards. The severity classification is a subjective verdict given by the operational participants.

The scheme allows classifying the hazards into 5 categories, category 1-5, with category 1 as the most severe classification with complete loss of safety margins and category 5 as the least severe classification with no safety consequences. It focuses on the extent of the reduction of safety margin if the hazard occurs and whether or not the crew or ATC is fully controlling the situation and able to recover from the situation.

It shall be mentioned that the hazard analysis comprised a systematic assessment of the possible cause and worst case outcome. Hence, the worst credible consequences were chosen.

Probability Classification

Each identified hazard must also be assessed for its probability of occurrence, i.e. an estimate of how often the hazard will occur. Without the probability, it is not possible to decide if the safety objective is fulfilled (cf. section 3.4).

The determination of the probability is subjective. The participants of the FHA sessions based the probability of occurrence of each hazard solely on their own estimation and experience, which, in many cases, were rough guesses since the approach procedure has not yet been implemented and hence not been in operation.

Thus, any probability classification comprises an average ‘best guess’ from a number of operational experts.

The scheme from which the probabilities were classified is shown below:

Probability Classification Descriptions	
Probable	A high number of similar occurrences have been experienced/observed at Ísafjörður OR a high number of similar occurrences have been recorded under similar conditions either nationally or in other states
Remote	Similar occurrences have been experienced/observed a number of times at Ísafjörður OR similar occurrences have been recorded several times under similar conditions either nationally or in other states
Extremely Remote	Similar occurrences have been experienced/observed a very few times at Ísafjörður OR only a few similar occurrences have been recorded under similar conditions either nationally of in other states
Extremely Improbable	No records or observations of similar conditions exist OR the hazard is considered to be impossible

Safety objectives

As mentioned before, the overall objective of the FHA is to identify *safety objectives* for the identified hazards. The safety objective is derived from the severity classification assigned to the hazard. Based on the specific severity classification, the safety objective specifies the maximum tolerable probability of the failure condition occurrence; that is *“how safe the system needs to be”*.

The figure below presents the risk classification scheme providing the coherence between the severity classification and the probability classification and the TOLERABLE / NOT TOLERABLE levels can be derived.

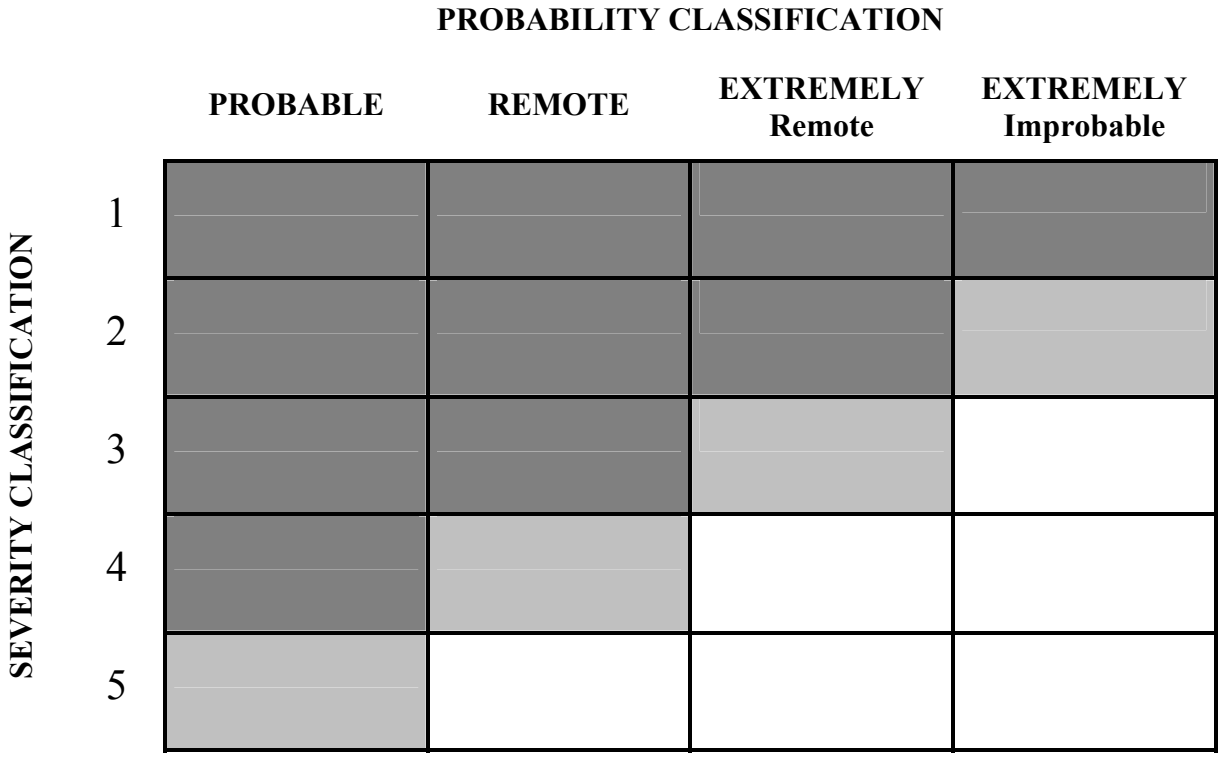


Figure 2: Risk Classification Scheme

The scheme shall be interpreted as follows:

If the severity class is determined as 3 (by the operational experts through the brainstorm session), the safety objective would be: "the probability of '*a hazard'* occurring shall not be greater than extremely remote".

Table 2 shows the safety objectives for all possible severity classes:

Severity Class	Safety Objective
1	the probability of the hazard occurring shall be 0 (zero)
2	the probability of the hazard occurring shall not be greater than extremely improbable
3	the probability of the hazard occurring shall not be greater than extremely remote
4	the probability of the hazard occurring shall not be greater than remote
5	the probability of the hazard occurring shall not be greater than probable

Table 2: Safety Objectives

However, as all classifications of safety critical hazards are based on subjective opinions a borderline area is introduced. It is most likely that participants do not agree to the assignments of severity and probability which is the reason why it is important to consider the hazards classified in the borderline in order to be absolutely certain that no hazards are accepted as TOLERABLE but should have been NOT TOLERABLE. Hazards classified on the

borderline (the light grey zone in the scheme below) will generally be considered to be NOT TOLERABLE, but will be referred to as *hazards in the borderline to be safety critical* (borderline hazards).

Figure 3: Risk Classification Scheme

In the analysis in the following sections other definitions are also used in the determination of a hazard to be NOT TOLERABLE or TOLERABLE or in the borderline. The term *safety critical hazards* refers to hazards that are NOT TOLERABLE and as such refers to hazards that do not meet their safety objectives. The term *borderline hazards* also refers to hazards in the NOT TOLERABLE area although considered separately in the analysis and the term *not safety critical hazards* refers to hazards considered to be TOLERABLE and as such refers to hazards that do not meet their safety objectives.

THE FHA SESSIONs - PROCESS AND PREPARATION

The objective of the FHA sessions was to identify all potential hazards in connection with a visual night approach at Ísafjörður and to classify each hazard with regard to severity and probability in accordance with the FHA methodology.

The hazards were identified in two Functional Hazard Assessment (FHA) sessions. Originally only one FHA session was planned. However, to ensure a high quality and accuracy of the safety assessment it was agreed between ICAA and Integra Consult to perform a second FHA session after the conduction of the first FHA session.

The first FHA session was conducted on 26 and 27 April 2001. The second FHA was conducted on 31 May 2001. Both sessions took place in ICAA's head office in Reykjavik.

This section introduces the reader to the general process practiced prior to and during the FHA sessions. Results from the various sessions are presented in Section 6 as well as in Annex D.

Participants

The best way to identify all hazards in connection with a visual night approach at Ísafjörður was to invite procedural developers of the Ísafjörður visual night approach procedure and operational experts experienced in operating into Ísafjörður.

In the first FHA session the procedure developers, one ICAA pilot and an AFIS operator from Ísafjörður participated. In addition other members of the investigation team were invited to give their input to the sessions.

In the second FHA session five pilots from Icelandair, Islandsflug and member of the pilots safety board participated. During the first session it was experienced that more viewpoints from operational experts were required. It was mentioned that the pilots safety board was having reservation concerning the safety of the proposed approach procedure. It was therefore agreed between ICAA and Integra Consult to conduct a second session and invite participants from Icelandair and Islandsflug and the pilot union's safety group. It is very important, when introducing a new operational procedure, to have the end-user's acceptance. In this case the end users are the pilots who shall execute the approach into Ísafjörður.

The selection of participants was very important as their knowledge and experience was required to fulfil the overall objective. The final result of the FHA sessions has been very dependent on the involvement of the attendees and the selected participants all had a relation to the area in focus for the particular FHA session. The ICAA selected the participants. A list of participants of the first and the second FHA are enclosed as Annex C.

Apart from the operational experts and procedure developers, representatives from ICAA were present at the sessions. Their role was to assist the operational experts in any technical issues.

Prior to the FHA sessions

The FHA sessions were prepared in a co-operation between Integra Consult and ICAA.

The participants of the first FHA session did not receive any information about the FHA methodology prior to the session. They were introduced to the methodology at the beginning of the session.

Such an introduction was, however, given to the participants prior to the second FHA and proved to be beneficial for the success of the session. Each participant received a briefing paper containing an introduction to the FHA methodology, the process of the session and a description of how to classify severity and probability.

FHA sessions

Introduction

Each of the FHA sessions was commenced with a briefing of how the session was to be carried out and the expectations of the participants during the session.

Approach to FHA sessions

To identify all potential hazards a structured brainstorm approach was used. The advantage was to obtain a free-flowing diversity of thoughts whilst ensuring that all aspects were covered.

All participants were requested to express their opinions and concerns to ensure that all possible areas within the procedure were covered.

The brainstorm session was facilitated by a moderator. His main tasks were to:

- keep the discussions centred on the question "WHAT IF?"; i.e. on considering the consequences of/impacts on of the different hazards of the assessed functions ;
- maintain a structured approach and keep the discussions relevant, without suppressing new and unexpected views/ideas ;
- allow all participants an equal opportunity to contribute ;
- encourage relevant contributions and ensure that all participants had an opportunity to put forward their views ;
- ensure comprehensive and balanced consideration of each function.

The approach to the hazard identification was to structurally use the approach charts of Ísafjörður (firstly the instrument approach chart Annex E and secondly the landing chart Annex F). The moderator requested the participants to consider hazards in connection with firstly the approach into Ísafjörður, then downwind over the city, then baseleg and finally the final approach.

All results of the assessment were recorded in a special database specifically tailored to Functional Hazard Assessments by Integra staff. This was done on-line during the brainstorm – and projected to a white screen for plenary approval.

Once the hazards were identified, the study team discussed each hazard and determined whether they were credible; i.e. whether there is a possible cause or failure mode and whether there is a measurable probability of occurrence.

For the identified hazards considered credible, the operational experts determined the precise wording of the hazard.

When the exact hazard description was defined, each hazard was analysed in accordance with the following:

- *Operational Consequences* The operational consequences identify the effects that the hazard will have on the operation and emphasise the impact / changes the hazard will introduce compared to "normal operation". An example is: increased R/T or increased co-ordination.
- *Safety Consequences* The safety consequences were derived from the operational consequences by deciding the impact on the safe provision of ATS. An example is: increased risk of collision with ground.
- *Risk Assessment* Based on the identified safety consequences, the hazard was risk assessed. A severity classification as well as a probability classification were assigned to the hazard. The severity classification scheme as detailed in Section 0 and probability scheme detailed in Section 0 were used at the risk assessment.

Second FHA session

The objective of the second FHA session was to verify the results and the risk assessment of the first FHA session, and to make sure that all potential hazards were covered and properly analysed. Furthermore, the objective of the second session was to identify further hazards that were not identified during the first session.

The second session was not moderated as strict as the first session, allowing more thoroughly discussions to take place.

At the session, a total of 5 additional hazards were identified and all previously identified hazards were discussed and verified.

Analysis

After the conduction of the FHA sessions, the process has been concluded with performance of the following activities:

- the recorded information has been structured ;
- safety objectives for the hazards have been derived ;
- assessment of whether the risks are TOLERABLE or NOT TOLERABLE has been performed.

Before the results of the FHAs are recorded and documented in section 6 a description of the visual night approach procedure and the visual daylight procedure at Ísafjörður are given. This is to clearly document all technical issues and assumptions of which the safety assessment, i.e. the FHA session are based on.

OVERVIEW

To illustrate and document the proposed approach procedure and the environment under which the safety assessment has been undertaken, a detailed illustration of the proposed visual night approach procedure will be given in the following. It has been necessary to carry out the safety assessment under some "basic" assumptions that are also documented in the following.

The safety assessment is based solely on the proposed procedure, cf. section 5.5 below and the assumptions as listed in section 5.2.

Target Level of Safety

It is recognised that Ísafjörður airport does not fulfil the ICAO recommendation as set down in ICAO Annex 14 of airports and their vicinity. This means that risk during landings and take off is higher than at airports fulfilling all ICAO Annex 14 requirements. Nevertheless, a target level of safety has been identified by the Icelandic Civil Aviation Administration that:

the risk of operating into Ísafjörður during night shall be equal or lower than flying into Ísafjörður at daylight.

To achieve this target level of safety, it is appreciated that strict weather limitation shall be introduced as well as a definition of pilot experience and aircraft performance. This is part of the assumptions, cf. section 5.2.

The conclusion of this safety assessment will state whether the proposed visual night approach procedure achieves this target level of safety.

Overall Assumptions

In the following a number of overall assumptions on which the safety assessment is based are listed.

a) The implementation of the visual night approach procedure will be the same as the proposed procedure, detailed in section 5.5.

It is assumed that the procedure being installed is identical to the proposed procedure made available to Integra Consult in the beginning of this project. The procedure is detailed in section 4.5.

b) Pilots operating into Ísafjörður adhere to the Icelandic AIP

It is also assumed that the pilots operating into Ísafjörður on a visual night approach, will follow the requirements as laid down in the AIP. This is especially related to the weather minima that are described in section 5.3.

c) ICAA will revise Unit Directives for Ísafjörður AFIS operators.

ICAA shall revise and update the unit directives for the AFIS operators at Ísafjörður airport. This includes activities to be carried out before an aircraft approaches during night. Further, it shall state that only one aircraft shall be allowed in the fjord at a time.

d) ICAA will carry out test flights on installed equipment.

It is assumed that the ICAA will carry out test flights to check the installed electrical equipment. This implies testing the intensity of the lights. No scheduled traffic shall be allowed into Ísafjörður before the equipment is tested and approved by the operating airlines into Ísafjörður.

e) ICAA will develop operational regulations for pilots and aircraft operating into Ísafjörður at night.

It is assumed that strict operational requirements for pilot qualifications shall be developed to ensure that a certain level of skills of the pilots exists. Furthermore, requirements to aircraft performance shall be introduced making sure that only aircraft that are able to carry out the proposed approach procedure will be allowed into Ísafjörður during night operations.

It shall also be noted that this safety assessment is performed taking into consideration the aircraft types that are supposed to operate into Ísafjörður at night. These are the Fokker 50 (FK50) and the ATR42 (AT42).

Furthermore it should be mentioned, that the approach path is developed with the assumption of a speed of 120 knots, a 25° bank angle and a pitch of 4.75° (equals 8,3 % slope).

The analysis is not based on any restrictions on wind/speed and strength of turbulence for which no limitations have been identified for performing the study of the analysis.

VMC conditions

According to the AIP, RAC 0-5, [ref 1], VFR flights into Ísafjörður shall be conducted so that the aircraft is flown in conditions of visibility and distance from clouds equal to that prescribed for operating in Airspace class F. This requires a distance from clouds at 1500 m horizontally and 1000 ft vertically. The Flight Visibility is defined to be 5 km when flying below 10000 ft AMSL. However, it shall be necessary for the pilots to comply with AIP RAC 0-7, [ref 1], chapter 8, Rules Regarding VFR Flight During Night. This rule states that flights, in the vicinity of an aerodrome, shall have unobscured flight visibility from the aircraft to the aerodrome and operating within 15 NM from an illuminated aerodrome. According to note no. 1, the flight visibility shall never be less than 8 km during VFR flight at night, thus it overrules the previously mentioned Flight Visibility of 5 km.

It is assumed, c.f. assumption b) listed above, that the pilots adhere to these VMC conditions. It is possible for a pilot to try to land below minima, as the AFIS operator at Ísafjörður has no authority to reject the pilot landing clearance. However, violations of the AIP requirements constitutes hazards that are not dealt with in this assessment.

Weather Stations

The Tower at Ísafjörður airport receives wind information from three different and independent weather information sources:

- Þverfjall – This is a dial up information source, which is located on mountain Þverfjall. It provides the AFIS operator with a 10-minute average wind factor.
- Arnarnes – This is a wind information source located at Arnarnes. This source provides the wind information according to ICAO specifications, i.e. the actual wind plus the maximum and minimum wind speed, visibility, cloud ceiling and temperature.
- Three Wind Direction Indicators placed alongside the runway at Ísafjörður airport.

Based on these sources the AFIS operator provides the arriving and departing aircraft with the wind information.

Description of proposed Visual Night Approach Procedure

The introduction of the procedure will require a number of electrical installations within Skutulsfjörður and around Ísafjörður airport. These are described in the following.

The proposed visual night approach into Ísafjörður can be split into two parts: firstly the IFR to be flown when passing IOG LOC and secondly the visual part of the approach which is to be initiated once passing the Missed Approach Point, 7.5 DME IOG.

This safety assessment is based on the IFR approach as shown in Annex E. The VFR part of the approach is based on the proposed visual night approach as shown in Annex F.

IFR approach

The IFR approach to Ísafjörður is based on a LLZ from the IOG LOC. This localizer is DME equipped. An NDB, OG, is co-located with the LOC. Once passing the LOC the aircraft is recommended to follow the back course LLZ at course 332° until passing the missed approach point, which is at 7.5DME IOG and QDM 261° from IS NDB. The IS NDB is located at Arnarnes. At 4.0DME on the IOG LLZ it is recommended that the aircraft passes 1600', descending.

When passing the missed approach point, the pilots shall be able to be visual with the Skutulsfjörður, i.e. be able to see the strobe light located next to Arnarnes, indicating the entry to the fjord. A strobe light is also placed opposite Arnarnes at Hnifsdalur. This strobe light was established in connection with the permission to perform take off at night, and is directed to the airport, thus it is not visible for inbound traffic (and the missed approach point).

When the pilots are VMC no later than the missed approach point, and are confident that they are visual with Skutulsfjörður and the strobe lights, the aircraft is to turn left into Skutulsfjörður and follow the proposed procedure and will be flying VMC from this point. If WX conditions are sufficient for VMC flight the pilot can go VMC anytime.

VMC approach

Skutulsfjörður is surrounded by mountains, which constitutes a high risk for any approach path into Ísafjörður airport. When an approach is to be carried out during night, it is necessary that the mountains are marked with obstruction lights.

The implementation of the approach procedure requires installation of a number of different lights and equipment.

In the mountain Eyrarhlið five steady red obstructions lights are to be installed to identify the Eyrarhlið Mountain. These will be powered from the local electric distributor. Local UPS (battery back-up) shall be installed providing back-up for at least 15 minutes to fulfil the requirement of power back-up. The power back-up will take over immediately in case of outage. These lights will be placed at approximately 800 ft above sea level.

On top of the Ski Lodge and high up in the mountain Kubburinn, two flashing red obstruction lights shall be installed. The objective of these is to indicate the two biggest obstructions in the final approach turn. This light will be controlled by the AFIS operator and feed from the airport power distribution system.

On the side of mountain Kubburinn, the side that faces the approach, a floodlight shall be installed. The lights will be in approximately 10 meters high poles and will be directed towards the mountain, giving an indirect light towards the pilot. The objective is to light the mountain ridge that lies below the final approach turn. The floodlight shall be powered from the airport power distribution system.

PAPI lights will be installed on the right side of the runway. These lights will be placed on the roof of a building. The objective of the PAPIs is to inform the pilot if the approach angle is correct, also in respect to passing the above mentioned mountain ridge. Based on calculations the approach angle is set to 4.75°. The PAPI lights have 5 brightness steps and are controlled by the AFIS operator. The lights are connected to the airport power distribution system. Due to the importance of this system, the control system will be dual.

The runway lights at Ísafjörður will be 200W high intensity lights with dual control loops. This system shall be powered from the airport power distribution system. This is an upgrade of the system seen in comparison with the current 45W low intensity lights with a single control loop.

When night take off was permitted, three steady red obstruction lights were installed at Kirkjubólshlíð.

From the runway end and through the approach turn, 18 sequence flashing lights will be installed: a total of 6 sets of such flashing lights, each consisting of 3 flashing lights. The objective of these lights is to identify the approach path for the pilots. The lights shall be sequenced to run towards the runway end, with a flash rate of twice a second. The system will be controlled by the AFIS operator and will be powered by the airport distribution system.

Upon entering Skutulsfjörður the aircraft is to be at 800 ft. The approach path “guidance” begins once the pilots have passed the city. The objective of the sequenced lights is to assist the pilots in performing the approach turn from downwind until final approach. The approach path requires the aircraft to pass a mountain ridge on mountain Kubburinn. The aircraft will pass the mountain ridge with 300 ft separation or less and 300 ft above the mountain ridge, and the suggested altitude at this stage is 600 ft. At this stage the pilot will follow the PAPI lights that provide 4,75° (equals 8,3 %) slope guidance towards the runway threshold. As mentioned above, the PAPI lights will be placed on the right side of the runway.

The intention of the visual night approach is to allow scheduled passenger aircraft, i.e. ATR and Fokker 50 to perform the approach, hence the speed reference for the approach turn is set to 120 knots and is based at a bank angle of 25°. The descent path of 4.75° will require approximately 1000ft/min rate of descent on final approach. The approach turn ends over the runway threshold.

Daylight operation

At the second FHA session, in which pilots from Icelandair and Islandsflug participated, it was identified that a night approach will result in several operational changes seen in comparison with daylight operation into Ísafjörður.

Those differences were indicated to be very important for the safety analysis. A description of how an approach into Ísafjörður is carried out during daylight follows.

Note, the aim of this section is merely to give the reader an understanding of the differences between the night and day operation, as some of these statements will be referred to in the analysis. In this section some hazards will be "revealed", however no analysis will take place in this section.

Description

The approach into Ísafjörður is special, some may even call it spectacular, and the pilots executing the approach appreciate all assistance given. The location of the airport is incredible in itself, the wind phenomena, creating windshear, downdraft etc. is common in Skutulsfjörður. It is common that the pilots observe the water to identify the wind phenomena.

During daylight operation, already when flying on the LLZ, the pilots observe the surface of the water to give indication of what kind of weather they can expect when entering Skutulsfjörður. If the expected weather is assessed by the pilots as being unacceptable, they will execute a missed approach, not later than at the missed approach point. At the FHA sessions it was emphasised that the pilots constantly assess the surface of the sea to determine if it is necessary to execute a missed approach. It was identified that this will not be possible during night operation, thus the pilots will loose a valuable decision tool whether to continue or abort the approach. Furthermore, by the pilots it was identified that the weather information given by the AFIS operator is not useable to the pilots for several reasons. The wind coming from the three Wind Direction Indicators placed alongside the runway are not illustrative, as the wind reference at the runway is not comparable with the wind at 800 ft, due to the mountains. Furthermore, the AFIS operator receives wind information from two weather stations located in the mountains, c.f. section 5.4 above. It was indicated by the pilots that this information was not assisting in determining whether to continue the approach and plan to execute a safe approach accordingly or to execute a missed approach.

During daylight, the pilots also assess the sea surface inside Skutulsfjörður to determine if windshear or downdrafts are to be expected. The pilots do not just assess the sea surface, but also drifting snow and smoke from the chimneys to have an indication of what to expect during the approach.

It was stated that the proposed visual night approach introduces other differences than when flying into Ísafjörður during daylight. As described earlier, the approach path to be flown is indicated by sequenced flashing lights, assisting the pilots to keep clear of the mountains. This approach turn is based on a 25° bank angle at 120 knots. At day operations the pilots fly closer to the mountains to achieve more manoeuvring space inside Skutulsfjörður. By flying closer to the mountain, the pilots are able to follow the electricity poles on the mountain.

Another issue to take into account is a bird nesting area which exists adjacent to the runway, which creates a hazard. However, during daylight operation the pilots may be visual with the bird, hence making an avoidance manoeuvre.

To sum up, it can be concluded that flying into Ísafjörður even during daylight increases the workload in the cockpit significantly, seen in comparison with executing a visual approach at other Icelandic airports.

Wind conditions

The location of Ísafjörður within Skutulsfjörður surrounded by mountains creates unstable wind conditions. Within Skutulsfjörður turbulence may occur and the same applies to windshear. Downdraft is a potential hazard that can occur close to the runway.

It has not been possible for Integra Consult to investigate all implications that can occur under certain wind conditions. If the wind is from the north, special conditions can be expected and others can be expected if the wind is coming from the south. The hazard analysis ***does not take the wind into consideration.*** The reason is that it has not been possible to use the received information to prepare a thorough analysis. However, it can be said that the wind will not reduce the severity of any hazards identified. If the aircraft experience a hazard under wind conditions where turbulence can be expected, it will obviously firstly increase the severity and secondly increase the probability of a potential collision into ground/terrain and obstacles.

It will be necessary for the ICAA to perform a thorough analysis of the wind conditions to explain the physical conditions that can be expected under the approach. This will enable the ICAA to develop specific wind restrictions of when it will be allowed to perform the visual night approach.

Determination of Severity Classification

As mentioned in Section 0, the severity classification is based upon the identified consequences. Each identified hazard will introduce an increase in the workload in the cockpit.

It has been necessary to highlight the following issue, in order for the reader to better understand the term “increase of workload”, which is associated with all hazards analysed in the following.

Based on the statements from the pilots operating into Ísafjörður airport during daylight, c.f. section 5.6, the workload in the cockpit is significantly higher then when performing a visual approach to other Icelandic airports. If it is identified that a hazard will result in a dramatically increase of workload, it shall be added to the already increased workload of flying into Ísafjörður.

Another term frequently used in the assessment, is that the probability of a collision with ground, mountains and/or obstacles has increased. If a specific hazard occurs, the increased workload in the cockpit and other physical and mental actions occurring to the pilots, affected by the occurrence of the hazard, the risk for the aircraft to collide with the ground or obstacles has increased.

The severity of the hazard will then depend on the scale of reduction in safety margins. The objective of the severity classification scheme is to support the determination of the scale of reduction in safety margins.

Determination of the severity category is, as with everything else in this FHA, a subjective worst case judgement taken by the operational experts attending the FHA sessions.

RESULTS AND ANALYSIS

All hazards are recorded in the hazard log enclosed as Annex D. In the hazard log, a remark has been given to the hazards that were identified in the second FHA. In the following however, no distinction between hazards identified in the first and in the second FHA will be made.

During the two FHA sessions, a total of 74 hazards were identified. However, not all of these hazards will be analysed and covered in the safety assessment of the visual night approach to Ísafjörður and as such count in the total number of valid hazards.

During the analysis it was discovered that some hazards were already covered under a previously analysed hazard. These hazards will be referred to as 'repetivie hazards'. For traceability purposes and to clearly demonstrate that all potential hazards have been covered, they are kept in the hazard log.

Some hazards that were identified at the FHA sessions have later been classified as hazards not related to the visual night approach to Ísafjörður. The hazards have been kept in the hazard log for traceability purposes with a remark.

Some of the identified hazards were covered by the assumptions described in section 5.2 and have not been counted as hazards in connection with the visual night approach. These are also kept in the hazard log and indicated with a remark.

The table below illustrates the distribution of hazards that will not be analysed as hazards in connection with the visual night approach.

	Hazards not related to the safety assessment	Hazards covered by assumption	Repetitive hazards
Number of hazards	2	7	28
Hazard id	7.13, 8.2	4.4, 4.5, 5.11, 8.3, 8.4, 8.5, 10.10	Not specified

Table 3: Hazard Distribution for non related hazards

The identified hazards have been structured into 10 functions (groups):

1. Weather
2. Birds
3. Runway
4. ATC
5. Lights
6. NAV/AIDS
7. Wind/turbulence
8. Pilot
9. Aircraft Performance
10. Approach Path.

The order of the functions is random. As it can be seen in the table, each hazard is assigned an id: x.y. The first digit refers to the function to which the hazard is related. The second digit is the consecutive number.

Reasons why the hazards have been grouped into each of the groups of hazards not covered in the total number of identified hazards are given in the following subsections.

Hazards not related to this Safety Assessment

7.13 "Turbulence when executing missed approach after passing missed approach point"

This hazard is not specifically related to the approach into Ísafjörður and thus not related to this safety assessment. It is an existing procedure already in use.

"Misconception when flying resulting in that wing crashes into the sea when performing turn into the fjord"

8.2 The hazard does not relate to the approach itself. Misconception is also possible at daylight.

Hazards covered by assumptions

4.4 "The runway is not cleared of obstacles"

It is assumed that ICAA will develop unit directives ensuring proper procedures to be carried out before each arrival, cf. assumption c).

4.5 "More than one aircraft in the fjord at a time"

It is assumed that ICAA will issue procedure allowing only one aircraft in the fjord at a time, cf. assumption c).

5.11 "Intensity of the runway lights"

It is assumed that the runway lights are shifted from low intensity to high intensity lights, cf. assumption d).

8.3 "Pilot continues approach in conditions close to weather minima"

It is assumed that pilots adhere to the VMC conditions and follow the requirements as laid down in the AIP, cf. assumption b).

8.4 "Pilot is not familiar with the surroundings"

It is assumed that ICAA will make qualification requirements for operating into Ísafjörður at night to ensure a certain level of skills, cf. assumption e).

8.5 "Misunderstanding of lights – if aircraft is flown by one pilot aircraft"

It is assumed that ICAA will make regulatory requirements to ensure that only two man cockpit crews operate into Ísafjörður, cf. assumption e).

10.10 "Ship going into the harbour – obstruction for go-arounds"

It is assumed that ICAA issues restrictions on ship traffic during landing of aircraft, cf. assumption e).

Repetitive Hazards

The 28 'repetitive hazards' will not be further explained in this subsection.

Valid Hazards

A total of 37 valid hazards were identified.

Of these 37 hazards, 5 were identified at the second FHA session. As mentioned above, the second FHA session were not facilitated as strict as prescribed in the Safety Assessment Methodology [ref 03], hence the risk assigned to the hazard, i.e. the severity classification and probability classification have been assigned by Integra based on statements given by the pilots at the second session.

Two hazards have not been assigned a probability classification, as it was impossible for the participants at the first session to judge this. The two hazards, 10.2 and 10.3, are both related to being off track on the approach path.

As explained in the methodology section, the safety objective indicates the maximum tolerable probability that a specific hazard occurs. If the estimated probability is higher than specified in the safety objective, the hazard has not achieved the safety objective.

When comparing the 37 hazards with the safety objectives the following can be derived:

	Safety Critical Hazards (NOT TOLERABLE)	Borderline Hazards (NOT TOLERABLE)	Non Safety Critical Hazards (TOLERABLE)
Number of hazards	21	8	8

Table 4: Hazard Distribution for valid hazards

Note that only hazards that are risk assessed as NOT TOLERABLE according to the safety objective scheme (cf. Section 0), are classified as *safety critical*.

In the following, all safety critical hazards and borderline hazards will be described in detail grouped into the 10 functions.

Safety Critical Hazards

Some of the identified hazards described in the following may also be hazards occurring during day operations, however, they have been included in the analysis as the severity increases during night operations.

Weather

One safety critical hazard was identified related to weather. The hazard is analysed below where the rationale for not achieving the safety objective is given.

Hazard 1.1 – Rapid change in visibility due to rain/snow showers

The operational consequence of this hazard is that the visibility for the pilots will be reduced. It was identified that the visibility when passing the missed approach point can be e.g. 8 km. However the visibility may be able to decrease rapidly when the aircraft approaches the turn. This will increase the workload in the cockpit, as the pilots shall now take a decision whether to continue the approach or execute a missed approach. It is noted that the AIP, RAC 0-6 states that the flight visibility for performing night VFR flights shall be 8 km or higher. This is common if the wind is coming from north east at 35-40 knots. Depending on how much the visibility reduces and how far within Skutulsfjörður the aircraft has got to, it may not be possible to execute a safe missed approach. In reduced visibility the pilots may not be able to see the obstruction lights installed in the mountains.

The hazard was classified as severity classification 3 mainly because it may not be possible to execute a missed safe approach and because of the extent of increased workload. The probability was estimated to Remote, hence the safety objective has not been achieved, cf. risk classification scheme Figure 3.

In order to reduce this hazard it was recognised that it could be necessary to restrict visual night operation into Ísafjörður airport during precipitation. This also emphasizes the risk, especially for those pilots attempting to carry out the approach below set minima.

Birds

Two safety critical hazards were identified relating to birds.

Hazard 2.1 – Birdstrike over the city

If a bird strikes the aircraft when the aircraft is flying downwind over the city the operational consequences will be that the aircraft will, in worst cases, get out of control. This depends, however, on which part of the aircraft the bird strikes. If it strikes on a critical part of the aircraft it will result in an increased workload in the cockpit due to the possibility of the structural damage to the aircraft this may cause. A birdstrike over the city increases risk of a collision with the ground over the city.

The hazard was classified as severity classification 2. If a bird strikes the aircraft the safety margin is reduced marginally and a strike will result in a large reduction of the pilot's ability to maintain control of the aircraft, i.e. to cope with adverse operational conditions. The probability was estimated to Extremely Remote. A birdstrike over the city has occurred once, hence the safety objective has not been achieved, cf. risk classification scheme Figure 3.

No immediate mitigation means exist to reduce the hazard.

Hazard 2.6 – Birdstrike on final approach due to bird nesting area close to the runway and bird trekking across the final approach track

It was identified that there is a risk of a bird strike on final approach. There are two reasons for this. Firstly, Skutulsfjörður continues below the final approach track, which can lead to bird trekking. Secondly as a nesting area is located adjacent to the runway on the wrong side of the runway bird trekking can occur across the runway and the final approach track as birds must cross the runway when they go for food.

During final approach is probably the most vulnerable time of an aircraft to encounter a birdstrike. Due to the possibility of a structural damage to the aircraft, the workload may increase dramatically. Depending on the severity of the structural damage to the aircraft, the aircraft may get out of control, thus increasing the risk of a collision with ground.

The hazard was not risk assessed at the first session. Based on comments and statements from both sessions, Integra has severity assessed the hazard to 2 due to the large reduction in safety margins and level of workload. The probability was judged to probable, due to the location of the bird nesting area. It is also considered that some birds (terns and seagulls) will react when they hear the aircraft noise and will start flying towards the sea, which requires the birds to cross the runway.

By removing the birdnesting area adjacent to the runway, the probability of occurrence will be highly reduced. However, no immediate mitigation means exist for reducing the probability of a birdstrike that can occur, due to the location of Skutulsfjörður.

Runway

Hazard 3.1 – Incident on runway due to Lack of Safety Areas

Runway safety areas on both sides of the runway are missing at Ísafjörður airport. If an incident occurs, the consequences will be more severe when no safety area exist. The possibilities for damages to aircraft, passengers and crewmembers increase significantly.

This hazard was assessed to a severity classification 2, which indicates a large reduction in safety margins. The probability was estimated to Probable, thus making it a safety critical hazard.

It is recognised that it is difficult to do something about this hazard. It is possible to increase the safety area to the right side of the runway. It is, however, difficult to make a safety area on the left side of the runway, as this is directly connected to the Skutulsfjörður. It is not possible to increase the safety area, as this will interfere with the entrance to Ísafjörður harbour.

Air Traffic Control

Two hazards are identified as safety critical relating to the Air Traffic Control.

Hazard 4.1 – Lack of Flight Information due to inattentive AFIS operator

The Tower of Ísafjörður is operated by an AFIS operator. As only few flights will approach Ísafjörður at night it is more likely that the AFIS operator will be inattentive when an aircraft is approaching Ísafjörður than to other more busy airports. If the AFIS operator is inattentive it constitutes a safety critical hazard, i.e. if the pilot is not provided with flight information such as:

- changes in weather
- runway friction (e.g. wet, damp, or with indicated braking actions)
- obstructions on the runway.

The aircraft may encounter unexpected turbulence/windshear/downdraft. Lack of such information will encounter an increased workload in cockpit especially if such information is expected.

If the pilot is not informed about the runway friction or obstacles on runway it may result in structural damage to the aircraft. This information is extremely important and lack of such information is extremely hazardous.

The hazard was severity classified as category 2, which indicates a large reduction in safety margins. The workload and working conditions will be such that the pilots are unable to perform their tasks effectively and the ability to cope with adverse operational and environmental conditions is largely reduced. The Probability was estimated to be extremely remote, only a few similar incidents have been recorded in other states.

As the hazard is related to human error no immediate mitigation means exist to reduce the hazard.

Hazard 4.2 – Loss of radio communication between AFIS operator and arriving aircraft

Loss of radio communication between AFIS operator and arriving aircraft is more hazardous during night time. The operational and safety consequences are the same as in connection with hazard 4.1 described above. It will result in the same lack of information for the pilot hence it will increase the workload in the cockpit and it may result in structural damage to the aircraft.

The hazard was severity classified as category 2, which indicates a large reduction in safety margins. The workload and working conditions will be such that the pilots are unable to perform their tasks effectively and the ability to cope with adverse operational and environmental conditions is largely reduced. The Probability was estimated to be extremely remote. It has occurred in Ísafjörður, but it is not a common incident.

Lights

Three hazards are identified as safety critical, c.f. the risk classification scheme, Figure 3.

Hazard 5.1 – The pilots fail to see the strobe light indicating Ísafjörður.

When flying on the LLZ, a strobe light located next to IS NDB indicates the entrance to the Skutulsfjörður. It was identified that the pilots may fail to see the strobe lights indicating Skutulsfjörður. If the pilots are not visual with the strobe lights when passing the missed approach point, they shall execute a missed approach, thus no specific hazard exists.

It was identified that it is easy to mistake lights, e.g. from a car holding still. It may occur that the pilots will begin to fly after the wrong light. Once the pilots identify their mistake, they will focus their mental energy on determining their position and not on flying the aircraft, thus the workload increases.

At the first FHA session, the hazard was severity assessed to class 4, with the probability of extremely improbable, which classifies the hazard as not safety critical. However, at the second FHA this hazard was characterised as a safety critical hazard, with a higher probability than estimated at the first session. If it happens at night, even if the probability is extremely improbable, the severity will increase significantly due to the possibility of a collision with ground/obstacles.

Currently one strobe light indicates the entrance to Skutulsfjörður and is located adjacent to IS NDB. The strobe light located in Hnifsdalur was installed in connection with introduction of take off during night. This light is directed towards Ísafjörður airport and is not visible when flying the LLZ. The strobe light at Arnarnes, located next to IS NDB, is the only strobe light visible when flying on the LLZ. It can be suggested to make both strobe lights

visible when flying the LLZ, perhaps with different colours, reducing the probability of mistaken other lights for being the strobe light. If both strobe lights become visible from outside the fjord it is necessary to interconnect the two lights meaning if one strobe light goes u/s the other one will automatically be turned off as well to ensure that they will not be mistaken from the other.

Hazard 5.7 – Airport Power Distribution System outage

The light installations required for the proposed visual night approach are all connected to one of the following two power distribution systems: The Airport Power Distribution System or the Local Electric Power Distribution System. This hazard is related to a situation where the Airport Power Distribution System goes down. The following lights are connected to the Airport Power Distribution System and will be affected by the outage:

- Two red flashing lights at Kubburinn and on the ski lodge;
- The 18 sequenced flashing lights identifying the approach path from downwind to the runway threshold,
- PAPI lights;
- Flood light on the side of Kubburinn, indicating the mountain ridge;
- Runway lights at Ísafjörður airport.

When comparing the systems being affected, it shows that all these lights are essential for the pilots to complete the safe turn, thus an outage occurring when an aircraft is downwind can be hazardous. The worst consequences will occur when an aircraft has passed the town of Ísafjörður and is positioning the aircraft according to the flashing sequenced lights. In case of a failure of the Airport Power Distribution System at this stage, the only means of orientation is the obstruction lights, powered by the Local Electrical Power Distribution System, c.f. hazard 5.12. The workload will increase dramatically. The pilot's mental energy may focus on orientating the position, thus leaving no energy to control the aircraft. It will be very difficult for the pilots to execute a safe missed approach, as they do not have any visual indication of the mountains surrounding Skutulsfjörður. The safety consequences, as identified at the FHA session, are disorientation and an increased risk for collision with ground/mountains or obstacles.

The hazard was severity classified as category 2, which indicates a large reduction in safety margins. The workload and working conditions will be such that the pilots are unable to perform their tasks effectively. The Probability was estimated to remote, as it does happen a couple of times per year. Last year it occurred between 2 and 3 times. This frequency of outages depends on the weather conditions. Icing on the lines creates more failures. The safety objective is not fulfilled.

It is necessary to look into the time lap between occurrence of the failure and until back-up is working. At the moment, all lights are back-up powered with an average switchover time of 4-5 seconds. Even during this time, the lights may have cooled off, requiring additional seconds to reach full intensity again. It is Integra's belief that a back-up time of more than 2-3 seconds can be extremely hazardous and may increase the risk of a collision with ground/mountains or obstacles.

Hazard 5.12 – Local Electrical Power Distribution System outage

Lights not powered by the Airport Power Distribution System are powered by the Local Electrical Power Distribution System. Lights effected by a potential outage are:

- All lights in the town of Ísafjörður;
- Five obstructions lights high in the mountain Eyrarhlið.
- Strobe lights indicating entrance to Skutulsfjörður.

It shall be mentioned that Ísafjörður hospital does have an instant back-up diesel generator, allowing electrical power to the hospital immediately, in case of an outage.

An outage of Local Electrical Power Distribution System is highest when the aircraft has passed the missed approach point and is heading towards the town of Ísafjörður. The pilot's will, after passing the town of Ísafjörður, position the aircraft according to the flashing sequenced lights. If the town lights goes out while the aircraft is heading towards the town for positioning, the pilots will have no visual aids. The 5 obstruction lights in Eyrarhlið are back-up powered by battery allowing an instant switchover for at least 15 minutes. The same applies to the strobe lights indicating the entrance to Skutulsfjörður. This light is also equipped with an instant 15-minute back-up battery.

The workload will increase and the pilots may experience spatial disorientation. It will become difficult for the pilots to execute a safe missed approach.

The hazard was assessed to a severity classification 2. This is when assuming the aircraft is heading towards the town of Ísafjörður for positioning, or in a situation where the pilots decide to execute a missed approach after passing the town of Ísafjörður. The probability is set to remote, hence the safety objective is not fulfilled.

As for the previous hazard, it is necessary to look into the back-up time.

Navigation Aids

Two hazards were identified as safety critical within this group.

Hazard 6.2 – Lack of accuracy of the approach aids (OG, IOG, IS, RE).

The hazard is related to a situation where the approach aids are inaccurate. The most critical one is the localizer. As described above, the approach can be divided into two parts, the instrument approach from passing IOG until passing the missed approach point and the visual part of the approach. If the back course of the localizer is inaccurate, the aircraft may get off track and in worst case get close to the mountains on the North Side. The cockpit crew workload will increase once they realise the situation and has to execute a missed approach without any navigational aids, as the localizer cannot be used. The mental energy will be used to orientate the pilots, trying to get clear of the ground/mountains. The risk of a collision with the ground/mountains will increase and there is a possibility of structural damage to the aircraft.

If the localiser is not working, the AFIS operator will get an indication. However, if the back course of the localiser is offset due to outside effects e.g. snowbanks, no indication is available.

The hazard was classified as severity classification 2, because of the large reduction in safety margins it can result. The probability of the hazard is estimated to Extremely Remote, however it has occurred that the localiser has been offset to the limit due to snowbanks around the equipment. The safety objective is not fulfilled.

It may be necessary to install indications in the Tower, enabling the AFIS operator to inform the pilots if the localiser is offset, thus restricting the possibility of the IFR part of the approach.

Hazard 6.3 – Lack of protection of Nav Aids.

This hazard is somewhat related to the previous hazard, 6.2. There is no protection around the navigation aids, hence it is easy for somebody, intentionally or unintentionally, to interfere with the navigation aids. The cockpit crew's workload will increase once the crew realises the interference. No far field monitoring exits at the moment. It has occurred that people camp close to the localiser site. Currently, no observation has been done to investigate if they interfere with the localiser. However, taken into consideration that the pilots, when performing a night approach, will trust the accuracy of the localiser 100% (compared to approx. 50% at daylight), the hazard is necessary to take into account. The hazard will increase the probability of a collision with ground / surrounding mountains, hence may result in structural damage to the aircraft

The severity classification is set to 2, based on the large reduction in safety margins, with an estimated probability of Extremely Remote.

It is suggested to carry out an investigation, firstly to establish the frequency of occurrences and secondly on the effects it has. It may be necessary to make access to the localiser impossible, by establishing physical blocking of the areas.

Wind/Turbulence

Two hazards have been identified as safety critical within this group and will be analysed in the following:

Hazard 7.2 – Wrong wind indication from the wind measuring system located on Þverfjall

A wind measuring system is installed on Þverfjall as mentioned above. It is a dial-up system from the Tower. The information given to the AFIS operator is the mean average wind, measured with 10 minutes intervals. The hazard exists in connection with the fact that this system gives wrong indications to the AFIS operator. Flying into Ísafjörður is very dependent on the predicted weather (winds, turbulence, windshear and downdraft). The pilots, who operates regularly into Ísafjörður, has a number of thumb-rules, with respect to what to expect when the wind is from certain directions. If the pilots get wrong information, they will prepare the approach on a wrong basis and may be surprised by severe weather conditions.

The main reason for the system to give wrong information is related to icing. If ice covers the system, it will not give correct information. It takes a long time before the failure is identified. Only then, the weather data coming from the system will no longer be transmitted to the pilots.

The severity classification is set to 2 as unexpected turbulence, windshear and/or downdrafts can cause a collision with ground/mountains and/or obstacles. The workload will increase dramatically in the cockpit, being able to control the aircraft. The probability is set to remote, as records show that the hazard has occurred before.

Hazard 7.14 – Wind information received from the TWR is limited.

This hazard was identified at the second FHA session.

As mentioned, the AFIS operator receives the wind information from two weather stations, located at Arnarnes and Þverfjall respectively. The information received from Þverfjall weather station is based on the mean average wind measured on top of the mountains with a 10 minutes interval. Receiving this information requires a dial-up process for the AFIS operator. The weather station at Arnarnes provides the actual wind including minimum and maximum wind speed. This information is passed along to the pilots. Furthermore, the pilots receive information from three Wind Direction Indicators, all placed along the runway at Ísafjörður airport. Because of the geographic location of Ísafjörður special wind conditions can be encountered. The pilots at the second FHA identified that the wind information received did not reproduce a true picture of what to expect during the approach, and the pilots are dependent on using visual means to assess the expected winds and turbulence, windshear and downdrafts.

As described above in detail, section 5.5 (Daylight operation) the pilots assess the surface of the sea, already when established on the LLZ to see which kind of weather conditions can be expected, allowing to plan ahead. Furthermore, once inside Skutulsfjörður, the pilots continue assessing the surface of the sea, cloud movements, drifting snow and smoke coming from chimneys. As this visual assessment cannot be performed during night operations and as it was identified that the wind information received from the AFIS operator does not give the pilots clear indication on what conditions to be expected, it constitutes a hazard. The workload will increase for the pilots, which increases the probability of a collision with ground/terrain and results in difficulties to keep control of the aircraft, due to encountered unexpected turbulence, downdrafts and/or windshears.

As this hazard was identified at the second FHA session, it was not risk assessed at the session. Based on statements and comments from the session, Integra has risk assessed it to a severity classification 2 with the probability of Probable, as the hazard will exist for every visual approach into Ísafjörður.

If the Visual Night Approach Procedure will be installed as proposed, it is necessary for ICAA to install wind measuring equipment allowing the AFIS operator to provide the pilots with valuable and reliable information during the approach. It will be necessary for the ICAA to carry out investigations to identify the most optimal location for the installation of such equipment. Furthermore, a wind rose shall be developed, detailing under which wind conditions it is allowed to make a visual approach into Ísafjörður during night.

Pilot

One safety critical hazard was identified within the group. It can be discussed whether the hazard is specifically related to the implementation and execution of the visual night approach procedure. It has been judged to be necessary to analyse the hazard in this section, because the severity classification is higher than during the daylight, thus it is classified as a safety critical hazard.

Hazard 8.7 – Pilot sets wrong QNH on altimeter.

The hazard is related to a situation where the pilots set a wrong QNH on the altimeter during the approach. When flying on the LLZ, no visual reference exists for the pilots to identify the incorrect QNH. If the PAPI is not reliable, the aircraft may be too low and make a control flight into terrain (into the ridge). A safety net will be the aircraft's Ground Proximity Warning System (GPWS). However, it was identified that the proposed visual night approach procedure will activate the GPWS during a 'normal' visual night approach, because of the approach path. The workload will increase dramatically once the pilots realise the incorrect QNH and the probability of a collision with ground has increased.

The severity classification was set to 2 due to the large reduction in safety margins and the increased workload. The probability was set to remote, based on experience. It does happen a number of times that the pilots set incorrect QNH during approach, thus the safety objective has not been achieved.

As human errors cause this hazard, it is difficult to identify mitigation means to reduce the risk and to predict the probability. One mitigation mean is to reemphasis the importance of cross checking and rechecking the QNH setting when passing the transition level and perhaps before entering Skutulsfjörður.

Aircraft Performance

One safety critical hazard was related to this group

Hazard 9.3 – Loss of control due to FK50/ATR not capable of performing approach.

No tests or calculations have been performed to investigate whether the Fokker 50 and ATR-42 are capable of performing the approach, given the specification in section 5.4 of this document. This constitutes a hazard. As outlined in the assumptions for this assessment, the safety assessment is based on the assumption that either Fokker 50 or ATR-42 shall perform night operations into Ísafjörður.

It is necessary to perform calculations and simulator trials to investigate if the approach procedure will push the aircraft outside of the flight envelope, thus resulting in a potential loss of control or structural damage. Based upon this the hazard has been categorised as severity classification 2 with a probability of Probable, as no tests have been performed yet.

It will be necessary to investigate in detail whether those aircraft types will be able to perform the approach, still leaving sufficient allowance for recovering from potential wind shear and/or downdrafts on baseleg/final approach. This is to be done on a FAA level D approved full Flight Simulator.

Approach path

Five (5) hazards are identified related to the proposed approach path. One of these hazards was identified in the second FHA session. That is hazard 10.16. As mentioned in the beginning of the analysis section, it was not possible to assign a probability to two hazards. These two hazards are both analysed in the following as safety critical hazards.

To get a clear picture of this group of hazards, which can be characterised as the most important safety critical hazards, the order in which the hazards are analysed is not numeric. It is necessary to mention hazard 10.4 initially, allowing thoroughly discussions to the subsequent hazards.

Hazard 10.4 – The approach requires the aircraft to bank all the way to the runway threshold. In addition the aircraft will have to use a steep descent angle (4,75°). The final turn ends over the runway threshold and requires a steep angle of descent.

A detailed description of the proposed approach path has been given in section 5.5. This hazard is elaborating on this description.

To illustrate the importance of this hazard, it is necessary to draw parallels to the daylight operations, which is also discussed earlier (in section 5.6).

It is recognised that flying into Ísafjörður airport, even at daylight, is a difficult task for the pilots, mainly because of the geographical location of the airport, surrounded by mountains, but also because of the unexpected weather conditions. The workload is significantly higher when flying into Ísafjörður than into any other airports at daylight.

However, during daylight operations, the pilots have some visual means to assess, among others, the surface of the sea to identify expected winds, allowing the pilots to plan the approach accordingly. Also, the pilots fly closer to the mountains giving more manoeuvring space.

Flying into Ísafjörður at night, the pilots will not have the visual indications to estimate the expected winds and will also have to follow the approach path, which is lighted by electrical installations, as detailed before. The hazard exists in the suggested approach path. The path is developed with the assumptions of 120 knots, a 25° bank angle and a pitch of 4,75° (equals a slope of 8.3 %). It was identified at the second session that it will be difficult for a FK50 or an AT42 to comply with these assumptions. The workload of executing this approach will be so high that it leaves no space for coping with additional encounters. Even in executing the approach itself, *with no weather conditions taken into consideration*. It was identified that the aircraft Ground Proximity Warning System (GPWS) may engage during the final approach turn, distracting the pilots, thus further increase the workload. The GPWS will give an audio warning in the cockpit – "SINK RATE". Furthermore the bank angle warning may engage too, usually when banking more than 15°. The approach turn also requires a steep descent angle, at 4.75°, equals approximately a descent rate of 1000 ft/min. The aircraft will be pushed to the limits of the flight envelopes, hence allowing limited power to recover from potential windshear or downdraft. A potential birdstrike shall also be taken into consideration at this stage. Skutulsfjörður continues below the final approach track increasing the probability of a birdstrike on final approach. The aircraft must have sufficient power to recover from such an encounter, either to perform a missed approach or to continue landing at Ísafjörður.

Taking all this into consideration at one time, it will be necessary for the pilots to focus on maintaining the aircraft within these limits. However when making the base turn it is crucial for the pilots to be visual with the PAPI lights, to keep clear of the mountain ridge, but also the runway itself. Depending on the wind, the pilots will have to concentrate on the ground speed, as the turn is based on 120 knots. In case of a 10 knots easterly wind, the aircraft will be flying with 130 knots (10 knots tailwind), requiring an even higher bank angle.

It was identified that the workload will be extremely high when performing the approach, and the risk for collision with ground and/or obstacles, causing structural damage to the aircraft, has increased. The severity classification is 2, with the rationale of large reduction in safety margins and the level of workload. The probability for an accident because of the proposed procedure was estimated to Remote, thus it is a safety critical hazard, c.f. risk classification scheme Figure 3.

It has to be mentioned, that the above considerations are considered for an approach being performed with a Fokker 50 or an ATR 42. As mentioned earlier in this assessment (hazard 9.2), it will be necessary to investigate in detail if those aircraft types will be able to perform the approach, still leaving sufficient allowance for recovering from potential windshear and/or downdrafts on baseleg/final approach.

<u>Hazard 10.2 – Aircraft off track on downwind.</u>

If the aircraft is off track on downwind it may constitute a hazard. Basically an aircraft can be off track by flying inside the path or outside the path, hence the later the flying the closer to the mountain.

If the aircraft is off track by flying outside the path, the five obstruction lights will still be available indicating the mountain Eyrarhlið, allowing the aircraft to keep clear of this mountain. Should the pilots continue to the approach, instead of executing a missed approach, the workload will increase as the pilots will focus on aligning the aircraft on the approach path. Should the pilots execute a missed approach, the hazard will have no safety consequences as there is enough manoeuvring space to make a safe 180° turn to get out of Skutulsfjörður.

If the aircraft is off track by flying inside the path, and not executing a missed approach, the mental energy of the pilots will be focussed towards aligning the aircraft on the path. This can result in a necessary increase of bank angle once initiating the baseleg turn, to enable the aircraft of staying within the approach path, thus the probability of overshooting is increased.

The severity classification was set to 4, because of a slight reduction in safety margins. The assumptions have been taken into consideration at this stage, i.e. that ICAA will issue minimum pilot qualifications for pilots operating into Ísafjörður at night. The severity classification will increase, if an inexperienced pilot is to fly the visual night approach (with respect to operating into Ísafjörður airport). The minimum qualifications should contain experience

flying into Ísafjörður during daylight a number of times (to be defined by the ICAA) and perhaps have successfully flown the approach in a full flight simulator.

Hazard 10.3 – Aircraft off track on baseleg.

Similar to being off track on downwind an aircraft can be off track on base leg, inside and outside the proposed path.

Should the aircraft be off track inside the approach path, it will be necessary to increase the bank angle further, to align with the path. The probability for a go around is higher, as the aircraft may not be aligned with the runway. Furthermore the probability of missing the PAPI lights is higher, thus the pilots will have no guidance to pass the mountain ridge.

Speed control is an important factor in connection with this hazard. In case of an easterly wind, the aircraft will have a tailwind, thus the ground speed will increase. This may get the aircraft off track outside the proposed path; hence the workload will increase for the pilots to align with the path. It is necessary to increase the bank angle to align with the proposed path and to keep clear of the mountain ridge.

In both cases, the probability of a collision with ground has increased, thus the severity classification is set to 2. Currently there is no experience in flying the approach; hence no probability can be assigned. The hazard, however, were characterised as safety critical at the sessions.

It will be necessary for the ICAA to issue a wind rose or a quick reference table, clearly describing when it is allowed to make a visual night approach into Ísafjörður. This will not mitigate the hazard, but it will reduce the probability of occurrence.

Hazard 10.6 – PAPI lights not indicating correct angle.

As mentioned the approach path takes the flight over a mountain ridge, which is illuminated by a floodlight. To assist the pilots passing the mountain ridge, PAPI lights are to be installed at the right side of the runway at Ísafjörður, set to match the descent profile of 4,75° or 8,3%. If the PAPI lights indicate an incorrect angle, the probability of a collision with ground or obstacles has increased, causing structural damage to the aircraft. The severity classification was set to 2 because of the large reduction in safety margins.

The suggested location of the PAPI lights is on a roof, on top of a hangar. Other possibilities have been investigated, but the hangar has been considered to be the best solution. However, it has been discovered that the roof is not very stable, as it is made of aluminium, and the wind may make it shake, thus resulting in a moving indication. Because of this, the probability for the PAPI lights to indicate an incorrect angle was estimated to Probable.

It is necessary to identify a more stable ground of which the PAPI must be installed to make the hazard less safety critical.

Hazard 10.15 – Difficult for the pilots to see the flashing sequence lights – “Line of sight” from 800 ft

It was identified at the second FHA session that it might be difficult for the pilots, especially those operating FK50 to be able to see the sequenced flashing lights. The reason is the “line of sight” when flying in 800 ft. The nose of the FK50 is long, reducing the visibility from the cockpit. Furthermore, taking into consideration that the pilots are sitting approximately 30-40cm from the windscreen, the pilots will not be able to see the lights just below them. This will result in an increased workload in connection with using the mental energy on trying to follow the flight path as close as possible and will leave less room for the crew to deal with unexpected matters.

Integra has set the severity classification to 3, based on the statements and comments from the session. The probability is set to probable.

No immediate mitigation means exist to reduce the probability of this hazard.

Hazard 10.16 – Flight Path – reduced manoeuvring area inside the fjord.

Seen in comparison with the daylight operation it is identified that the manoeuvring possibilities inside Skutulsfjörður is reduced. It will be difficult for the pilots to manoeuvre inside Skutulsfjörður, as they are not visual with the mountains surrounding the fjord. This hazard is especially connected to a situation where it is required to make a missed approach. The missed approach in the fjord usually requires to make a 180° turn and to fly out of Skutulsfjörður. The reduced manoeuvring possibilities increase the risk of a collision with ground/mountains or obstacles, thus the severity classifying is set to 2. The probability is by Integra estimated to be extremely remote, thus it is a safety critical hazard.

No immediate mitigation means exists to reduce the risk of this hazard.

Hazard 10.21 – Lack of possibilities to execute a safe missed approach.

It was identified that the pilots will have difficulties in executing a safe missed approach on parts of the approach path. It gets more critical the further on the approach path, i.e. the closer to the runway. Different reasons may require the pilots to execute a missed approach. It can relate to other identified hazards, i.e. the aircraft is off track, the lights goes out or the pilots get a malfunction indication in the cockpit and wish to abort the approach to fly outside Skutulsfjörður. If it becomes necessary to make a missed approach on the base turn, the aircraft is already banking 25° or more with a descent slope of 4.75°, thus leaving it difficult to execute a safe missed approach. The workload in the cockpit will increase to an even higher level, still taking into consideration the already high workload the pilots face, thus the risk of a collision with ground or obstacles has increased.

The severity of the hazard has been set to a severity classification 2, due to the large reduction in safety margins and the level of workload. The probability has been set to extremely remote, as it does occur a couple of times a year that an aircraft has to execute a missed approach at Ísafjörður.

The lack of possibilities to execute a safe missed approach constitutes a major safety hazard in this approach procedure. No mitigation means can be recognised, which can be implemented into the proposed procedure. It was identified that, during daylight operation, the pilots have a landmark at the city they navigate towards, when executing a missed approach. No aid exists in the night procedure, leaving the pilots with no mean of navigation out of Skutulsfjörður. It shall be noted that the strobe light located on Kubburinn is directed towards the airport. It shall be investigated if this light can be seen if, for instance, the pilots execute a missed approach just when turning towards base.

Borderline hazards

The following hazards have been characterised as borderline hazards. The reason why these are analysed is that determination of the severity classification and probability are subjective. It may occur that a hazard has been set too low in its classification. To prevent this Integra has decided to analyse those hazards that were close to be classified as safety critical. The analysis will not be as exhaustive as the safety critical hazards, however recommendations for mitigation means are still identified, wherever possible.

Weather

No borderline hazard were identified in this group.

Birds

No borderline hazards were identified in this group.

Runway

No borderline hazards were identified in this group.

ATC

No borderline hazards were identified in this group.

Lights

In connection with lights these hazards were identified as hazards on the border to be TOLERABLE.

Hazard 5.5 – Obstruction lights on Eyrarhlið u/s or covered by snow.

In situations where the obstruction lights at Eyrarhlið are either unserviceable or covered by snow, the pilot's workload will increase, as they shall be more attentive to follow the flashing sequence lights. The risk to collide with Eyrarhlið has increased.

The lights are to be placed on high poles. It has happened once that the three obstruction lights at Kirkjubólshlíð has been unserviceable, due to technical failure.

The severity has been set to 3, because of the major reduction in safety margins and an estimated probability of extremely remote.

ICAA has to look into the back-up functions and maintenance of the lights. This will reduce the probability even more, thus making it an acceptable hazard.

Hazard 5.8 – Control lines from the TWR to the lights are not working.

The hazard is related to a situation where the AFIS operator is unable to turn on the lights. As it is assumed that ICAA will issue Unit Directives that the AFIS operator shall turn on the lights 10-15 minutes before the arriving aircraft passes IOG (current procedure within the ICAA). In case the lights will not be turned on, the aircraft will execute a missed approach and will not enter Skutulsfjörður, thus the hazard will have no consequences.

If these instructions are issued and followed, the hazard will be eliminated.

Hazard 5.10 – Lack of visual reference due to mountain ridge lighted by floodlight.

The hazard exists because of the high intensity of lights that the pilots will be exposed to on baseleg. The pilots will be exposed to the flashing sequenced lights, the high intensity floodlight, PAPI lights and the high intensity runway lights when initiating the baseleg turn. Once the aircraft has passed the mountain ridge and is turning towards final approach, the only lights to which the pilots will be exposed are the runway lights. Even though they are high intensity the amount of lights to which the pilots are exposed have reduced significantly and the pilot's vision will have to be 'adjusted' to the new settings. Mentally, it is easier for human eyes to get used to more light, than when being exposed to a high intensity going to a low intensity. This transition may prove to be hazardous, depending on the time required. The vision 'adjusting' happens at the most crucial part of the approach, when the aircraft is banking 25°, pitching 4.75° and is close to the runway threshold. This may lead to frustration for the pilots, who are using all the energy of orientation instead of controlling the aircraft. The risk of missing the runway and hitting the ground are increased.

This hazard was identified at the second FHA session and was not, as mentioned before, risk assessed at the session. Integra has, based on the statements and attitude of the pilots from the second session; risk assessed this hazard as being a severity classification 4 with a probability of remote. The rationale for setting the severity classification to 4 is because it is assumed that the ICAA will carry out a number of test flights into Ísafjörður airport after installation of the system. At this stage the pilots will be able to judge if the light intensity is too strong, allowing the engineers to reduce it.

Navigation Aids

No borderline hazards were identified in this group.

Wind/Turbulence

One hazard was identified as borderline hazard in this group.

Hazard 7.15 – Breaking mountain waves (inside the fjord).

At one occasion, a pilot departing Ísafjörður encountered Breaking Mountain Waves. This resulted in a severe increase of workload in the cockpit. With the increased workload the probability of a collision with ground or obstacles is increased.

The hazard was identified at the second FHA session, thus it is not risk assessed. Integra has, based on statements from the session, and has risk assessed the hazard with a severity classification of 2, with an estimated probability of extremely improbable.

Pilot

One hazard was identified as borderline hazard in this group.

Hazard 8.1 – Pilot in the right hand seat has to take over control.

The majority of the approach procedure will have to be performed by the pilot sitting in the left hand seat (1st pilot). The reason is that it is a left hand turn, thus the 1st pilot will have the best view. It may happen that the pilot in the right hand seat (2nd pilot) will have to take over. This will cause a change of flight deck procedures and may result in an extremely high workload for the 2nd pilot. The 2nd pilot may not be fully aware of the position, thus he/she will focus the mental energy on establishing orientation of the aircraft. This will increase the risk of a collision with the ground or obstacles.

It was severity assessed to classification 2, because of the large reduction in safety margins with an estimated probability of extremely improbable.

Aircraft Performance

One borderline hazard was identified in the assessment related to performance of the aircraft.

Hazard 9.1 – Aircraft experience left engine failure.

A hazard occurs if the left engine of the aircraft fails during the approach. The most critical part will be during the base turn. The aircraft will, however, still be at 600 ft, allowing some space to loose altitude. The risk of a collision with ground/terrain is increased.

It is necessary to complete this scenario in a full flight simulator to investigate the recovery performance. Until then, this hazard will not be elaborated further.

It shall be mentioned, that the severity classification is 2, based on the large reduction in safety margins with the probability of extremely improbable.

Approach path

One borderline hazard was identified in the assessment related to lack of speed control on approach.

Hazard 10.9 – Lack of speed control on approach.

An increased workload is required in connection with the physical conditions as downdraft, updraft and turbulence. At final approach low power is required due to high pitching. Easterly winds can increase the severity of the hazard. If the wind is Easterly, the ground speed will be too high and it will be impossible for the pilots to reduce the speed, thus the aircraft may go off track on the base turn (c.f. hazard 10. 3). This will require a steeper bank angle and result in a longer landing or possibly a go around. If the aircraft lands, the probability of overrunning the runway and causing structural damage to the aircraft is increased.

If the speed is too low, the aircraft might not be able to recover from encountering of turbulence etc. The risk of stalling is increased. If the pilots attempt to land, the aircraft may land short of the runway, causing damage to the aircraft.

The severity is estimated to 3, due to the increase of workload. The severity will, however increase if encountering turbulence, downdraft or updrafts. The probability was estimated to extremely remote, which is based on the number of missed approaches a year. It was identified that missed approaches, due to speed, occurs a few times a year.

Not Safety Critical Hazards

A total of eight (8) hazards out of the 37 valid hazards meet the safety objective and are classified as TOLERABLE in connection with a visual night approach, i.e. they are risk assessed as fully acceptable. These hazards will not be described in detail. The following are considered to be not safety critical hazards:

3.1	3.3	5.1	5.4	5.6	6.1	9.2	10.11

SUMMARISED RESULTS

The following consists of the analysis leading up to the conclusion of the report. The analysis will take into account the most safety critical hazards. Integra has chosen to highlight the following functions of which the most safety critical hazards exist:

- Wind conditions
- Approach Procedure
- Missed approach
- Lights
- Birds
- Localiser.

Wind conditions

Ísafjörður airport is manned with an AFIS operator. One of the responsibilities of the AFIS operator is to provide Flight Information Service to the pilots of arriving and departing aircraft. The AFIS operator shall inform the pilots of the latest wind information, i.e. wind direction and wind speed. This information will be provided by the AFIS operator from three Wind Direction Indicators (WDI) placed alongside the runway along with information from two weather stations located in the surrounding area. One of these weather stations is located on top of the mountain Þverfjall, providing the AFIS operator with the mean average wind with a 10 minutes interval, whereof the second weather stations is located at Arnarnes, providing the AFIS operator with wind information according to ICAO specifications, i.e. the actual wind plus the maximum and minimum wind speed.

By the pilots at the second session it was stated that the wind information was considered insufficient. Two declarations support this statement. Firstly, the WDI placed along the runway indicates the wind at surface level, thus no derivation can be made of the wind at 800 ft, which is the altitude of the aircraft when entering Skutulsfjörður. Secondly, the indications from the wind measuring stations at Arnarnes and Þverfjall do not provide wind information that is useable for the pilots. This is mainly because of the weather station's position in an area where the wind measurements are not representative – or convertible – to the conditions to be expected within Skutulsfjörður.

To determine the wind conditions within Skutulsfjörður, during daylight operations, it is a commonly known practise to do so by visual means, in order to predict the expected wind conditions, including potential turbulence, downdraft etc. Already when flying on the LLZ, the pilots try to assess the expected wind conditions by assessing the surface of the sea. The waves and behaviour of the sea provides the pilots with valuable information, especially when approaching the missed approach point, to decide whether to continue the approach or execute a missed approach. Once inside Skutulsfjörður, the pilots continue assessing, not only the surface of the sea, but also cloud movements, drifting snow and smoke from chimneys. This assists the pilots in planning the final approach turn.

Obviously, it will not be possible for the pilots during night operations to use the same visual indications to predict the weather inside Skutulsfjörður and prepare the approach accordingly. With reference to the above, it has been identified that the wind information provided by the AFIS operator does not provide an adequate picture of the wind conditions to be expected, thus, the pilots will have no picture of the expected wind. The workload in the cockpit will increase, causing a canalised attention on wrong parameters, thus making prediction of the wind conditions one of the most safety critical hazards.

To conclude, it will be extremely difficult for the pilots to predict the wind conditions within Skutulsfjörður, during night operation. This increases the risk seen in comparison with daylight operation, where the risk is significantly lower.

Approach procedure

When flying into Ísafjörður at daylight it was recognised that the workload is significantly higher than flying into other airports in Iceland. The pilots participating at the second FHA session identified that the proposed approach procedure would enforce an extremely high workload on the pilots, thus leaving a low margin for errors. The approach procedure itself has been identified as a safety critical hazard. The approach is based on a speed of 120 knots, 25° bank angle and a descent slope of 4.75° (equals 8.3 %). The latter will require a rate of descent of approximately 1000 ft/min.

Three critical parameters exist, which will require the pilot's full attention throughout the approach turn, while at the same time the pilots shall use the visual guidance means to manoeuvre. The critical parameters are the same as above - the speed, bank angle and descent rate. Speed control is a very important parameter when executing the approach. A slight tail wind will cause an increase of the ground speed, thus an increased bank angle is necessary to complete the turn, increasing the risk of overshooting. It was recognized that the approach turn will set of the Ground Proximity Warning System (GPWS) in the cockpit, which may further increase the physical stress level of the pilots. The GPWS issues an audio warning in the cockpit. It must be noted that most aircraft types allow the pilot to shut off the GPWS. However, this introduces a number of other hazards, not part of this assessment.

Moreover, it was considered a risk that the approach turn ends just overhead the runway threshold leaving the pilots with no final approach at all. It was suggested to make a displaced threshold of approximately 200-300 meters from the runway threshold.

Compared with daylight operation, aircraft flying into Ísafjörður at night will face a higher risk, primarily due to the extremely high workload, but also because of less manoeuvring area as the pilots fly closer to the mountains during daylight operations.

Missed approach

It was recognised that the possibility of executing a safe missed approach is limited, depending on where the aircraft is flying the approach path. Should it be necessary to execute a missed approach on downwind, the pilots do have more manoeuvring space, thus the pilots will be able to make a 180° turn and fly out of Skutulsfjörður. However, if the pilots decide to execute a missed approach on base turn, the situation is more critical. The aircraft is already banking 25° or higher, depending on the speed, and is pitching down 4,75°. If the aircraft at this stage shall execute a missed approach, the bank angle will increase while at the same time full power shall be applied, to bring the aircraft into a stable climb. Furthermore, the pilots will have to visually provide separation from terrain. This will raise the already very high workload in the cockpit to a level where the pilots may not be able to perform their tasks effectively.

A number of reasons may cause that the pilots choose to perform a missed approach. The aircraft may have gotten too far outside the track, and an abruption collision avoidance manoeuvre is necessary or that a failure warning is shown in the cockpit. In case of the latter, the risk of canalised attention exists, where the pilots may tend to focus more on the failure warning, than on performing the missed approach.

It was identified that the pilots tend to fly closer to the mountain during daylight, providing more manoeuvring space, indeed also if a missed approach is necessary. It was also identified that the pilots use a landmark close to the town of Ísafjörður to navigate towards. The landmark brings the aircraft to the middle of Skutulsfjörður, allowing easy exit. It shall be noted that in connection with allowing take-off at night, a strobe light indicating the exit of the valley was installed at Hnifsdalur.

Compared with daylight operation, the risk of a collision with terrain in connection with a missed approach is significantly higher during night operation.

Lights

The approach itself is based on a number of electrical installations, all to be installed. These include obstruction lights, 18 flashing sequenced lights, PAPI lights, floodlights, high intensity runway lights and others. In the assessment it was identified that the lights are either connected to the Local Electric Power Distribution System or the Airport Power Distribution System, however with the majority of the equipment connected to the Airport Power

Distribution System. The back-up time was estimated to approximately 4-5 seconds, however, the lights need an additional 2-3 seconds to reach high intensity. Note that the obstruction lights in the mountains have an instant 15-minute battery back-up. Anything over 2-3 seconds can be considered safety critical. When the aircraft is performing the final approach turn, the pilots are relying on the flood light to indicate the mountain ridge, the PAPI light to provide vertical separation from the mountain ridge and the flashing sequenced lights guiding towards the runway threshold. All these systems are powered by the Airport Power Distribution System. In case of an outage, the pilots will have no guidance means to execute a safe missed approach. It is necessary for the ICAA to look into this issue.

This risk does not exist during daylight operations, thus no comparison of risk can be made.

Birds

It was identified that the probability of a bird strike is high especially on final approach, which is caused by two reasons. Skutulsfjörður stretches below the final approach track, which increases the possibility of bird trekking. The second reason is that a bird nesting area exists close to the runway. Bird trekking occurs from the nesting area and out to the sea, crossing the runway. Even though this safety assessment is only related to the proposed night procedure, it can be said that the bird nesting area is a hazard for daylight operations, however with a higher risk during night approach as the pilots have no visual means of identifying the birds, thus it is suggested to remove the bird nesting area.

The risk of a bird strike may not be judged higher during night operations compared to daylight operations, however, the consequences, in case of a bird strike, can be considered higher during night operations.

Localizer

Another safety critical hazard is related to the protection of the NAV AIDS, especially the Localizer (LLZ). In the past it has occurred that people has camped close to the LLZ resulting in offset of the LLZ in worst cases. Snow has also resulted in offset of the LLZ before. It will be necessary to protect the LLZ, allowing no access to interfere with the beam. The consequences are much higher during night than compared to daylight, even though the hazard also exists during daylight when flying IMC. During daylight, the pilots may be able to see terrain allowing visually to keep clear of terrain. The pilots will also be able to observe that the LLZ if offset and report it to proper instance. During night operations neither of this is possible, hence, the risk of a collision with terrain has increased.

The risk of a collision with terrain, due to an offset localiser, can be considered higher during night operations compared to day operations.

CONCLUSION

This safety assessment has been performed in connection with the implementation of a visual night approach at Ísafjörður.

The safety assessment followed the EUROCONTROL Safety Assessment Methodology. Two Functional Hazard Assessment (FHA) sessions were conducted, in which a total of 74 hazards were identified. Some of these hazards were repetitive hazards or hazards covered by the assumptions. By deducting those hazards, a total of 37 hazards were identified of which 21 hazards have been analysed to be safety critical and an additional 8 hazards have been analysed to be on the borderline to be safety critical.

Prior to the performance of the safety assessment the ICAA identified an overall safety target:

The risk of operating into Ísafjörður during night shall be equal or lower than flying into Ísafjörður at daylight.

Based on the fact that 21 safety critical hazards and 8 borderline hazards have been identified it has been considered that the **target level of safety has not been achieved**, i.e. the risk of flying into Ísafjörður during night is significantly higher than flying into Ísafjörður during daylight, with the given assumptions.

ANNEX A:
LIST OF ABBREVIATIONS

List of Abbreviations

AFIS	Aerodrome Flight Information Service
AIC	Aeronautical Information Circular
AIP	Aeronautical Information Publication
ATC	Air traffic Control
ATS	Air Traffic Services
ATM	Air Traffic Management
CAA	Civil Aviatio Authority
ESARR	EUROCONTROL Safety Regulatory Requirement
FHA	Functional Hazard Assessment
GPWS	Ground Proximity Warning System
ICAA	Icelandic Civil Aviation Authority
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
LOG	Localiser
LLZ	Backcource Localiser
NDB	Non-Directional Beacon
PAPI	Precision Approach Path Indicator
RAC	Rules of the Air and Air Traffic Services
SAMI	Safety Assessment Methodology
TWR	Tower
UPS	Uninterruptible Power Supply
VMC	Visual Meteorological Conditions
WDI	Wind Direction Indicators

ANNEX B:
REFERENCES

#	Document	Edition	Author
1	AIP Iceland,	-	Directorate of Civil Aviation
2	ICAO Annex 14 “Aerodromes”	Third edition	ICAO
3	EATMP Air Navigation System Safety Assessment Methodology, *SAF.ET1.ST03.1000-MAN-01-00*	1.0	EUROCONTROL
4	Risk Assessment and Mitigation in ATM	0.2	ESARR 4

ANNEX C:
LIST OF PARTICIPANTS

(Not included)

ANNEX D:

HAZARD LOG,

Note.- Only an extract of the hazard log has been reproduced in the manual. The complete log contained details for all the identified hazards described in the text.

Weather

#	Hazard	Operational Consequences	Safety Consequences	Pre-Mitigation Severity/Probability	Mitigation	Post-Mitigation Severity/Probability	Remark
1	Rapid change in visibility due to rain/snow showers.	The visibility will be reduced.	If the VIS is 8 km when starting the approach into the fjord, the VIS should not be able to decrease so rapidly. However, if the wind is from the NE at 35-40 kts it may happen. Even if the wind is 20-25 kts, it may not be possible to execute a safety missed approach. It may also increase the workload in the cockpit.	3 Remote			Good visibility when departing for BIIS – some pilots will land – Even with VIS less than 7 km. It may be an idea to introduce a restriction, restricting aircraft visual night approach during precipitation.

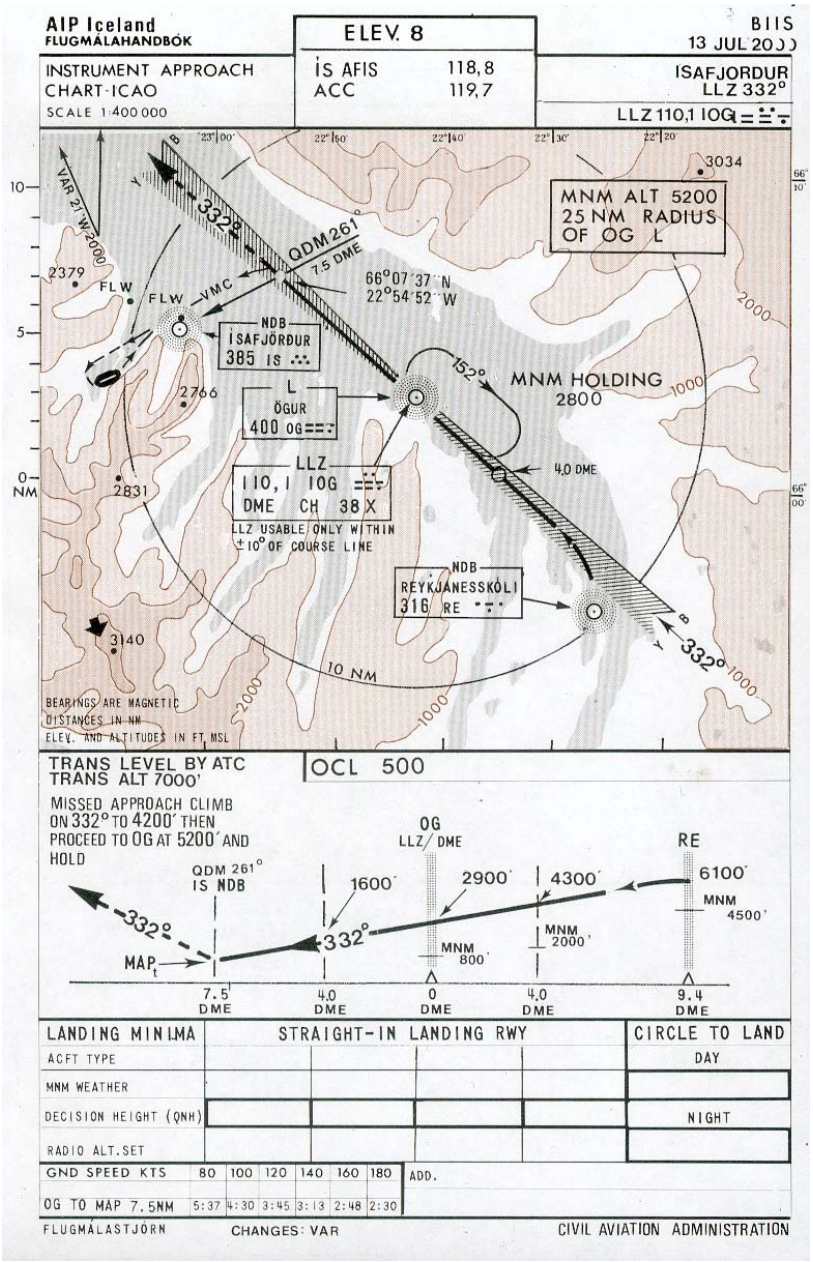
#	**Hazard**	**Operational Consequences**	**Safety Consequences**	**Pre-Mitigation Severity/Probability**	**Mitigation**	**Post-Mitigation Severity/Probability**	**Remark**
2	Rapid changes in visibility.						Repetitive hazard.
3	Lack of accuracy of determination of cloud ceiling	Ceilometer placed outside the fjord. Fairly easy for the AFIS operator to determine the ceiling. The pilots may not be able to carry out a visual approach and will have to execute missed approach.	If missed approach, the workload will increase.	4 Extremely Remote			Especially during rain.

Birds

#	**Hazard**	**Operational Consequences**	**Safety Consequences**	**Pre-Mitigation Severity/Probability**	**Mitigation**	**Post-Mitigation Severity/Probability**	**Remark**
1	Birdstrike over the city.	Due to the possibility of structural damage to the aircraft, the workload may increase dramatically. Depending on the severity of the structural damage to the aircraft, the aircraft may get out of control.	Increase risk of a collision with the ground.	2 Extremely Remote			
2	Birdstrike on final approach.	Similar as birdnesting next to the airport.					Repetitive hazard.
3	Birdstrike during go arounds.						Repetitive hazard.
4	Seagull flies over the harbour.						Repetitive hazard.

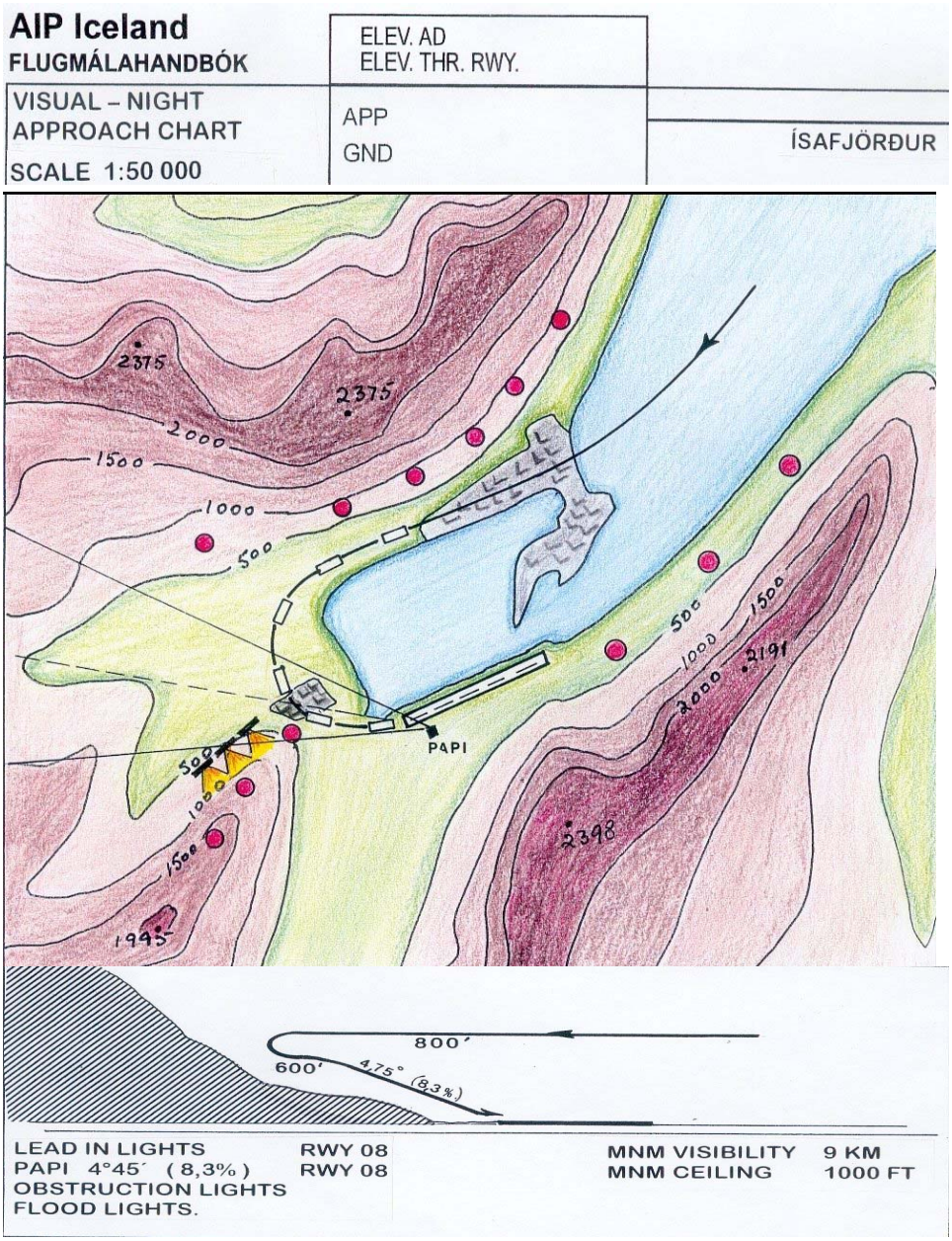
#	Hazard	Operational Consequences	Safety Consequences	Pre-Mitigation Severity/Probability	Mitigation	Post-Mitigation Severity/Probability	Remark
5	Bird nesting around the airport.	Birdstrike. No effort has been done from the CAA to eliminate the nesting of the birds on the airport area.	Possibility for structural damage. Increased workload.	2 Probable			
6	Birdstrike on Final Approach due to bird nesting area close to the runway and birdtrekking across the final approach track.	Due to the possibility of structural damage to the aircraft, the workload may increase dramatically. Depending on the severity of the structural damage to the aircraft, the aircraft may get out of control.	Increase risk of collision with the ground.	2 Probable			
7	Birds can be encountered at final approach.	Birds can be encountered at final approach, as the lake continues below the flight path.					Repetitive hazard.

ANNEX E:
INSTRUMENT APPROACH CHART,



ANNEX F:
PROPOSED LANDING CHART,
AT ÍSAFJÖRÐUR, ICELAND

Note.- Not to be used for navigation. This approach was not approved.



CHAPTER 7 - SAFETY AUDITING

7.1 SAFETY AUDIT PROGRAMME

7.1.1 Safety auditing is the third core safety management activity. It provides management with information concerning the safety of current operations, and areas where some form of corrective action may be required. It is one of the proactive safety management activities, providing a means of identifying potential problems before they have an impact on safety.

7.1.2 Safety audits can be conducted by both the safety regulatory authority, and the ATS service provider. While the procedures used in the conduct of these two types of audits are similar, the scope is quite different.

7.1.3 In auditing an ATS service provider, the safety regulatory authority would take a broad view of the safety management procedures of the organization as a whole. The key issues in such an audit would be:

a) Does the organization comply with the national safety regulatory requirements?

b) Is the organization's safety management system based on sound principles and procedures?

c) Does the organization have adequate staff, and are the staff adequately trained, to ensure that the safety management system functions as intended?

d) Are safety issues managed effectively, and is the organization meeting its safety performance targets?

7.1.4 The audit programme of an ATS service provider is an internal management tool. It involves periodically undertaking a detailed review of the safety performance, procedures and practices of each unit or section with safety responsibilities.

7.1.5 The need for internal safety audits as part of the safety management system, and the benefits to ATS service providers from establishing their own auditing system, were introduced in Chapter 4. Profit (1995) describes the role of such internal safety auditing as being to ensure that:

a) risks are identified and the potential for causing or contributing to an accident/incident are recognized;

b) the Safety Management System structure is sound in terms of appropriate levels of staff, compliance with approved procedures and instructions, and a satisfactory level of competency and training to operate equipment and facilities and maintain their levels of performance;

c) adequate arrangements exist to handle foreseeable emergencies;

d) equipment performance is adequate for the safety levels of the service provided; and

e) effective arrangements exist for promoting safety, monitoring safety performance and processing safety issues.

7.1.6 A safety audit which address all these issues must look at more than just compliance with regulations and procedures. The audit team should make its own assessment of whether the procedures in use are appropriate, and whether there are any work practices which could have as yet unforeseen safety consequences.

7.1.7 For an audit to be successful, the co-operation of the personnel of the unit or section concerned is essential. The safety audit programme should be based on the following principles:

a) It must never appear to be a "witch hunt". The objective is to gain knowledge. Any suggestions of blame or punishment will be counter-productive.

b) The auditee should make all relevant documentation available to the auditors, and make arrangements for staff to be available for interview as required.

c) Facts should be examined in an objective manner.

d) A written audit report describing the findings and recommendations should be presented to the unit or section within a specified period.

e) The staff of the unit or section, as well as the management, should be provided with feedback concerning the findings of the audit.

f) Positive feedback should be provided, by highlighting in the report the good points observed during the audit;

g) While deficiencies must be identified, negative criticism should be avoided insofar as possible.

7.1.7.1 Following the audit, a monitoring mechanism may need to be implemented to verify the effectiveness of any necessary corrective actions.

7.1.8 The scope of a safety audit may vary from an overview of all activities of the unit or section to a specific activity. An initial audit would normally cover all activities. Follow-up audits may concentrate only on aspects of the operations where the need for corrective action was identified. Audits of specific aspects of a unit or section's activities could also be conducted as the result of safety performance monitoring indicating possible problems in those areas.

7.1.9 The criteria against which the audit will be conducted should be specified in advance. These criteria should include those items listed in Section 2.5 of the PANS-ATM which are relevant to the unit or section being audited. The criteria should address relevant parts of:

a) national safety regulatory requirements;

b) the organization's safety policy;

c) the organization's safety management manual; and

d) the organization's operational documentation, including the unit's local instructions.

7.1.10 The organization should develop an organization-wide safety audit plan. This safety audit plan should be revised annually, and should that provide for all units or sections to be audited at regular intervals. Typically, this would be every 2-3 years.

7.1.11 Audits required for follow-up of previous safety audits where corrective action was proposed, or because an undesirable trend in safety performance was identified through the safety performance monitoring system, cannot always be scheduled in advance. The overall audit programme for a year should make allowance for the possibility of such unscheduled audits.

7.1.12 In addition to an organization-wide audit plan, a detailed audit plan should be prepared for each individual audit. Figure 7-1 illustrates the audit process diagrammatically. The processes involved in each step are discussed in more detail in the following parts of this chapter.

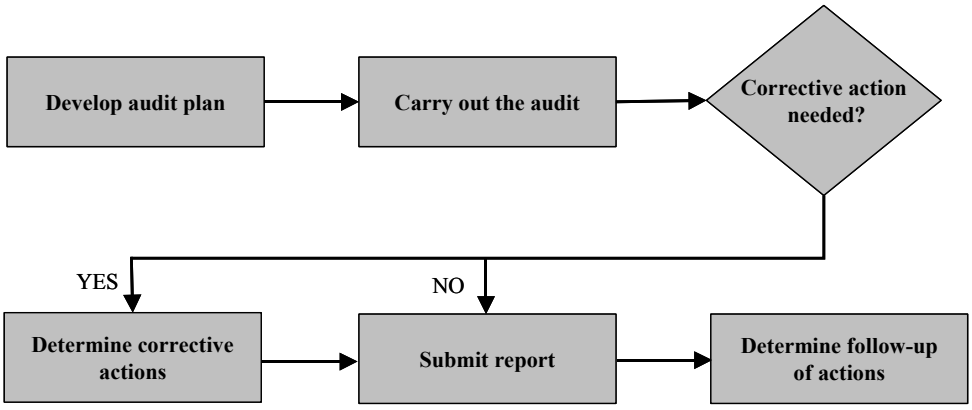


Figure 7-1. The safety audit process

7.2 THE SAFETY AUDIT TEAM

7.2.1 Safety audits may be undertaken by a single individual or a team, depending on the scale of the audit. The staff selected to conduct an audit should have practical experience in disciplines relevant to the area to be audited, a good knowledge of the relevant regulatory requirements, a good knowledge of the organization's safety management system, and have been trained in auditing procedures and techniques. An audit team comprises:

a) An audit team leader;

b) One or more auditors (optional);

7.2.2 The audit team members should, as far as is possible, be independent of the area being audited. It is also preferable that the audit team is not composed exclusively of management level staff. This can help ensure that the audit will not be viewed as threatening. Staff with current operational experience may also be better at identifying possible problems, in some circumstances.

The role of the audit team leader

7.2.3 An audit team leader should be appointed if more than one auditor is involved. The audit team leader is responsible for the overall conduct of the audit. This responsibility includes:

a) selecting and managing the audit team;

b) planning and preparing for the audit;

c) quality control of the audit team's work;

d) preparation and submission of the audit report; and

e) chairing discussions with the management team of the unit or section being audited.

7.2.3.1 During the audit, the team leader will also undertake some of the general tasks listed in 7.2.4.

The role of auditors

7.2.4 The tasks to be undertaken by each audit team member will be assigned by the team leader. These tasks may include conducting interviews with staff of the unit or section being audited, reviewing documentation, observing operations, and writing material for the audit report.

7.3 PLANNING AND PREPARATION

7.3.1 A formal notification of intention to perform the audit should be forwarded to the unit or section to be audited in adequate time for any necessary preparations for the audit to be made. This notification should specify:

a) the unit or section to be audited;

b) the authority under which the audit is conducted;

c) the proposed schedule;

d) the overall purpose of the audit and the scope of the topics to be discussed;

e) the number and type of staff who may be required for interview, and the documentation which will need to be available to the audit team; and

f) the audit team members.

Pre-audit planning activity

7.3.2 One of the first actions in planning an audit will be to verify the feasibility of the proposed schedule and identify the information which will need to be available before commencement of the audit It will also be necessary to specify the criteria against which the audit will be conducted and develop a detailed audit plan together with checklists to be used during the audit.

7.3.2.1 The checklists consist of a comprehensive series of questions grouped under topic headings, which are used to ensure that all relevant topics are covered.

The audit plan

7.3.3 An outline of a typical audit plan is shown in Table 7-1.

Outline of Contents of an Audit Plan

INTRODUCTION

This section should introduce the audit plan and the background for the audit.

PURPOSE

The purpose, objectives, scope and the criteria against which the audit will be conducted should be specified.

UNIT TO BE AUDITED

This section should clearly specify which area to be audited.

PLANNED ACTIVITIES

This section should identify and describe the activities to be performed, the areas of interest and how the different subjects will be addressed.

It should also specify the documents which should be available for the audit team and if the audit will involve interviews, the areas to be addressed during the interview should be listed.

SCHEDULE

This section should include a detailed schedule for each of the activities planned.

AUDIT TEAM

This section should introduce the audit team members.

Table 7-1. Example of a typical structure for an Audit Plan

7.4 CONDUCT OF THE AUDIT

Opening meeting

7.4.1 At the opening meeting, the audit team leader should briefly present the background to the audit, its purpose, and any specific issues that will be addressed by the audit team. The practical arrangements, including the availability of staff for interview, should be discussed and agreed with the manager of the unit or section being audited.

Audit procedures

7.4.2 The techniques for gathering the information on which the audit team's assessment will be made include:

a) review of documentation;

b) interviews with staff; and

c) observations by the audit team.

7.4.3 The audit team should work systematically through the items on the relevant checklist. Observations should be noted on standardized observations sheets. An example of an observation sheet is provided in Appendix A. to this chapter.

7.4.4 If a particular area of concern is identified during the audit, this should be the subject of a more thorough investigation. However, the auditor must keep in mind the need to complete the rest of the audit as planned, and must avoid spending an excessive time exploring a single issue and so risk missing other problems.

Audit interviews

7.4.5 The principal way in which auditors obtain information about the functioning of the safety management systems is by asking questions. This provides additional information to that available in written material, and gives the staff involved an opportunity to explain the system and work practices. Face-to-face discussions also permit the auditors to make an assessment of the level of understanding of the safety management system, and the degree of commitment of the staff of the unit or section to safety management.

7.4.6 The persons to be interviewed should be drawn from a range of management, supervisory and operational positions.

7.4.7 The purpose of audit interviews is to elicit information, not to enter into discussions. All auditors should observe the following guidelines relating to the conduct of audit interviews:

a) Listen attentively and let the speaker know you are listening.

b) Remain neutral. Do not disagree, criticise or interrupt.

c) If there is any doubt about the meaning of what the auditor has been told, restate the main point "Are you telling me that...?". Get agreement on the summary of what have been said.

d) Ask 'W' questions - what, why, where, when, who and how - these are the key words that will bring forward facts and information.

e) Ask questions that make people to go deeper into the matter. Ask 'suppose', 'what-if' and 'show-me' questions. Ask for explanations and examples.

Audit observations

7.4.8 Once the audit activities are completed, the audit team should review all audit observations against the relevant regulations and procedures, to confirm the correctness of observations noted as non-conformities, deficiencies or safety shortcomings.

7.4.9 An assessment of the seriousness should be made in respect of all items noted as non-conformities, deficiencies or safety shortcomings.

7.4.10 It should also be remembered that the audit should not focus solely on negative findings. An important objective of the safety audit is also to highlight good practice within the area being audited.

Closing meeting

7.4.11 A closing meeting should be held with the management of the unit or section at the conclusion of the audit activities to brief them on the audit observations and any resulting recommendations.

7.4.12 Prior to this meeting, the audit team should:

a) Agree on the audit conclusions.

b) Prepare recommendations, such as proposing appropriate corrective action, if required.

c) Discuss whether there is a need for follow-up action.

7.4.13 At the closing meeting, the audit team leader should present the observations made during the audit and give the representatives of the unit or section being audited the opportunity to correct any misunderstandings. Dates for issue of the interim audit report and receiving comments on it should be mutually agreed.

7.5 CORRECTIVE ACTION PLAN

7.5.1 At the completion of an audit, the management of the unit or section has the responsibility for developing a corrective action plan setting out the action(s) needed to resolve identified deficiencies or safety shortcomings within the agreed time period. An example of a corrective action form can be found in Appendix B to this chapter.

7.5.2 When completed, the corrective action plan should be forwarded to the audit team leader. The final audit report will include this corrective action plan and details of any follow-up audit action proposed. The manager of the area being audited is responsible for ensuring timely implementation of the appropriate corrective actions.

7.6 AUDIT REPORTS

7.6.1 The audit report should be an objective presentation of the results of the safety audit. As soon as possible after completion of the audit, an interim audit report should be forwarded to the manager

of the unit or section for review and comments. Any comments received should be taken into consideration in the preparation of the final report, which constitutes the official report of the audit.

7.6.2 The key principles to be observed in the development of the audit report are:

a) consistency of observations and recommendation in the closing meeting, interim audit report and audit final report;

b) conclusions substantiated with references;

c) observations and recommendations stated clearly and concisely;

d) avoidance of generalities and vague observations;

e) objective presentation of the observations;

f) use of widely accepted aviation terminology, avoiding acronyms and jargon;

g) avoidance of criticism of individuals or positions.

7.6.3 An outline of a typical audit report is provided in Table 7-2.

CONTENTS OF AN AUDIT REPORT

INTRODUCTION

This section should identify the audit, of which this report is the formal documentation and introduce the different chapters included in the report.

LIST OF REFERENCED DOCUMENTS

This section should outline all documents, which have been used during the audit.

BACKGROUND

This section should describe the reason for the audit. This could just be a regular audit, or there could be a specific reason for the auditing authority performing the audit (e.g. safety risk identified, safety incident observed).

PURPOSE

This section should state the objective and scope of the audit as described in the audit plan.

Any event during the audit, which has led to problems fulfilling the objective, should be described. The consequences hereof should be concluded.

STAFFING

This section should list the personnel included in the audit.

OBSERVATIONS

This section should in general terms describe the observations of the audit team. This should cover both good points and points of concern.

The details concerning the observations should be attached as observation sheets, including also the agreed corrective actions

GENERAL CONCLUSION

This section should present the general conclusions of the audit. This should not only focus on problems, but also highlight good points.

ATTACHMENTS

All observations sheets and associated corrective actions sheets should be attached to the audit report.

Table 7-2: Examples of contents of an audit report

7.7 AUDIT FOLLOW-UP

7.7.1 The primary purpose of audit follow-up is to verify the effective implementation of the corrective action plan. Follow-up action may be effected through monitoring the status of implementation of accepted corrective action plans or follow-up audit visits.

7.7.2 Where a follow-up visit has been made, a further report of this visit should be prepared. This should clearly indicate the current status of the implementation of the agreed corrective actions. If any non-compliance, deficiency or safety shortcoming remains unresolved, the audit team leader should highlight this in the follow-up report. A copy of this should be forwarded to the senior management of the organization.

APPENDIX A TO CHAPTER 7

OBSERVATION SHEET	
Organisation audited:	No.:
Area audited:	Date of issue:
Document References:	
Observation: (Abstract) (Description)	
Seriousness (minor/major):	Prepared by (Auditor):
Clearance Target Date:	
Acknowledgement signature (Auditee):	Acknowledgement date (Auditee):

APPENDIX B TO CHAPTER 7

CORRECTIVE ACTION	
Corrective Action Sheet no:	Connected to Observation Sheet no:

Short Term Corrective Action

Identify immediate action needs (statement):	
Identified by (signature):	Completion/Verified due (date):
Action performed by (signature):	Action performed (date):
Action verified (signature):	Action verified (date):

Long Term Corrective Action

Establish root cause (statement):
Identify preventive action needs (statement):

Identified by (signature):	Completion/Verified due (date):
Action performed by (signature):	Action performed (date):
Action verified (signature):	Action verified (date):

Auditor's Notes

Corrective action verified by (Auditor):	Title (Auditor):
Corrective action verified by (signature):	Corrective action verified (date):
Records/Comments (Auditor):	

CHAPTER 8 - SAFETY MANAGEMENT TRAINING

8.1 THE SAFETY TRAINING PROGRAMME

8.1.1 Training is an important factor in generating and preserving a safety culture. It will be necessary to provide specific safety management training for staff at all levels who occupy positions with safety responsibilities.

8.1.2 Implementing an effective safety management training programme requires that the organization:

a) identify the training needs for all personnel involved in activities affecting safety;

b) identify sources of training to meet the above needs; and

c) produce a training plan, implement a schedule and monitor the results.

8.1.3 The training programme should ensure that the safety policy and principles of the Organization are understood and adhered to by all staff, and that all staff are aware of the safety responsibilities of their position.

8.1.4 The development of specific safety training courses, and the incorporation of safety content into other courses, should be the joint responsibility of the safety manager and the training manager.

8.2 TRAINING NEEDS

8.2.1 Different levels of training will be needed for safety management specialists and other staff. During the initial implementation of the safety management system, specific training in safety will have to be provided for existing staff. Once the safety management system is fully implemented, the safety training needs for other than the safety specialists should be able to be met by incorporating the appropriate safety content into the general training programme for each position.

8.2.2 The safety manager should, in conjunction with the personnel department, review the job descriptions of all staff, and identify those positions which have safety responsibilities. The details of the safety responsibilities should then be added to the job descriptions.

8.2.3 Once the job descriptions have been updated, the safety manager, in conjunction with the training manager, should conduct a training needs analysis, to identify the training that will be required for each position.

Initial safety training for all staff

8.2.4 One of the functions of safety management training is to create an awareness of the objectives of the safety management system of the organization, and the importance of developing a safety culture. All staff should receive a basic introductory course covering:

a) the basic principles of the safety management;

b) the organization’s safety policy and safety management system;

c) the importance of complying with the safety policy and with the required procedures that form part of the safety management system;

d) the roles and responsibilities of staff in relation to safety.

8.2.5 In addition, all staff with safety responsibilities should receive further training appropriate to their positions, in accordance with the requirements determined from the training needs analysis.

Specialist safety training

8.2.6 A number of safety related tasks require the expertise of specially trained personnel. This includes:

a) investigating safety occurrences;

b) monitoring safety performance;

c) performing safety assessments; and

d) performing safety audits.

8.2.7 It is important to ensure that staff performing these functions receive adequate training in the special methods and techniques involved. The training requirements for staff performing these functions should be determined on the basis of the training needs analysis.

8.2.8 Depending upon the depth of training required and the level of existing expertise in safety management within the organization, it may be necessary obtain assistance from external specialists in order to provide this training.

On-going safety training requirements

8.2.9 Once the safety management system is fully implemented, the safety training needs for the majority of staff can be met by the incorporation of the required safety content in the regular training programs. Specific safety training courses will, however, be required for persons occupying, or appointed to, safety specialist positions.

8.2.10 Ab initio training courses will need to include a level of safety training comparable to that provided to all staff during the implementation phase. Appropriate safety content, once again determined on the basis of the training needs analysis, should be incorporated in the training courses for staff moving to new positions, and in all refresher training programmes.

Note.- Guidance on the development of training programmes and the conduct of training needs analyses is contained in the ICAO TRAINAIR Training Development Guideline

CHAPTER 9 - SAFETY REGULATORY FRAMEWORK FOR AIR TRAFFIC SERVICES

9.1 INTRODUCTION

9.1.1 Annex 11, Section 2.26 requires States to implement systematic and appropriate safety management programmes in relation to the provision of air traffic services. It will therefore be necessary for all States to establish regulatory provisions concerning ATS safety management, together with the necessary supporting infrastructure to enable them to discharge their responsibilities in relation to oversight of these provisions.

9.1.2 There are two prerequisites for the introduction of a regulatory system. These are:

a) the provision, in the basic aviation law of the State, for a code of air navigation regulations and the promulgation thereof;

b) the establishment of an appropriate State body, hereinafter referred to as the Civil Aviation Authority (CAA), with the necessary powers to ensure compliance with the regulations.

Note.- Further guidance on basic aviation law and State codes of air navigation regulations can be found in the Manual of Procedures for Operations Inspection, Certification and continued Surveillance, (Doc 8335).

9.1.3 States will, in general, already have their basic aviation law and code of air navigation regulations in place. The first step in establishing the regulatory framework for ATS safety management will therefore be to examine the existing legislation and regulations to identify what changes, if any, will be necessary to provide the CAA with the necessary powers to ensure that the requirements of Annex 11 Section 2.26, and the associated procedures in PANS-ATM Chapter 2, are complied with in the provision of ATS within its area of responsibility.

9.1.3.1 In addition to promulgating the necessary regulations, this will require the establishment of an appropriate body to carry out oversight of the operation of the ATS safety management programme. Within this manual this body will be referred to as the *ATS Safety Regulatory Authority*.

9.1.4 The organizational structure and size of the ATS Safety Regulatory Authority should suit the national environment and the complexity of the existing civil aviation system. The function may be placed within the CAA, or in an autonomous statutory body, independent of the ATS service providers, with the legal powers to perform the regulatory function.

9.1.5 In those States where the CAA also acts as both regulator and ATS service provider, it is important that a clear separation between the ATS provision function and the ATS safety regulatory function be maintained. The safety regulation of the service provider should be conducted as though the service provider was an external entity in order to maintain the independence of the regulatory function.

9.2 FUNCTIONS OF THE ATS SAFETY REGULATORY AUTHORITY

9.2.1 The core functions of the ATS Safety Regulatory Authority are:

a) development and updating of the necessary regulations;

b) setting national safety performance targets; and

c) safety oversight of ATS service providers.

9.2.2 With reference to point a) above, the extent to which new regulations will be necessary can vary considerably from one State to another depending on the scope of existing regulations, and will not be discussed further here.

9.2.3 With reference to point b) above, the safety performance targets set by the ATS Safety Regulatory Authority would be targest for the overall ATS system. They should take into account any national safety performance targets which may have been set by the CAA for the State aviation system as a whole. Setting safety performance targets has already been discussed in Chapter 2.

Safety Oversight

9.2.4 The objective of the safety oversight of ATS service providers is to verify compliance with relevant:

a) ICAO SARPs and procedures;

b) national legislation and regulations; and

c) national and international good practices.

9.2.5 The methods of safety oversight may include safety inspections and/or safety audits of the organizations concerned. Safety oversight should also involve a systematic review of significant safety occurrences.

9.2.6 The safety oversight procedures should be standardized and documented to ensure consistency in their application. Procedures should also be easily understandable, mandatory, and form a complete documented system.

9.3 APPROACHES TO THE DISCHARGE OF REGULATORY RESPONSIBILITIES

9.3.1 In the discharge of the regulatory responsibilities ATS Regulatory Authority may adopt either an active role, involving close supervision of the functioning of all activities of the ATS provider's safety related activities, or a passive role, whereby greater responsibility is delegated to the ATS provider.

9.3.2 A system of active supervision by the regulatory authority could be so rigorous as to amount to complete domination and dictation of the conduct of operations, leading to an undermining of the morale of operations personnel and to lowering of safety standards. Such a system would also require the establishment of a large enforcement organizations.

9.3.3 The State, in the passive role, could leave both the interpretation and the implementation of the regulations to the ATS provider, relying upon the ATS providers' technical competence and encouraging compliance through threat of enforcement action. This might place an unreasonable burden of responsibility on the ATS provider for interpretation of and compliance with the regulations. The State would not be in a position to assess the adherence of the ATS provider to the regulations other than by knowledge acquired by chance or in the course of accident or incident investigation. Such a system would not enable the State to exercise the necessary preventive and corrective function and consequently it could no adequately discharges its responsibility under the Convention.

9.3.4 The foregoing leads to the conclusion that considerable merit exists in a State regulatory system which falls between the active and passive extremes and which should:

d) Represent a well-balanced allocation of responsibility between the State and the ATS provider for the safety of provision of ATS;

e) Be capable of economic justification within the resources of the State;

f) Enable the State to maintain continuing regulation and supervision of the activities of the ATS provider without unduly inhibiting the ATS provider's effective direction and control of the organization; and

g) Result in the cultivation and maintenance of harmonious relationships between the State and the ATS provider.

REFERENCES

ICAO Documents

Annex 11 – *Air Traffic Services*

Annex 13 – *Aircraft Accident and Incident Investigation*

Procedures for Air Navigation Services – Air Traffic Management (Doc 4444)

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

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

Human Factors Guidelines for Safety Audits Manual (Doc 9806)

Human Factors Digest No. 10 – *Human Factors, Management and Organization* (Circular 247)

Other References

Flight Safety Foundation Icarus Committee (1999) The dollars and sense of risk management and airline safety. *Flight Safety Digest* vol.18 No.5

Maurino, D. E. *et al.* (1995) *Beyond aviation human factors – safety in high technology systems.* Aldershot, Ashgate.

Profit, R. (1995) *Systematic safety management in the air traffic services*. London, Euromoney Publications.

Reason, J. (1990) *Human error.* Cambridge, Cambridge University Press.

Reason, J. (1997) *Managing the risks of organizational accidents.* Aldershot, Ashgate.

Robinson, R. M. *et al*. (1998) *Risk and reliability – an introductory text,* 3rd. edition. Melbourne, Risk and Reliability Associates Pty. Ltd.

- END -