Public AUTHORITY for Civil Aviation

Guidance for Development of Aeronautical Telecommunication System Safety Case (CAR-171)

Effective: 5th December 2019

Manual Number: 1.3.19

Issue Date: 05 December 2019

Revision: 01

CONTROLLED COPY

Intentionally Left Blank

List of Effective Pages

Page No.	Rev No.	Date of Issue
1	01	05/12/19
2	01	05/12/19
3	01	05/12/19
4	01	05/12/19
5	01	05/12/19
6	01	05/12/19
7	01	05/12/19
8	01	05/12/19
9	01	05/12/19
10	01	05/12/19
11	01	05/12/19
12	01	05/12/19
13	01	05/12/19
14	01	05/12/19
15	01	05/12/19
16	01	05/12/19
17	01	05/12/19
18	01	05/12/19
19	01	05/12/19
20	01	05/12/19
21	01	05/12/19
22	01	05/12/19
23	01	05/12/19
24	01	05/12/19
25	01	05/12/19
26	01	
27	01	
28	01	
29	01	
30	01	
31	01	
32	01	
33	01	
34	01	
35	01	
39	01	
40	01	

Page No.	Rev No.	Date of Issue
41		
42		
43		
44		
45		
46		
47		
48		
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		
61		
62		
63		
64		
65		
66		
67		
68		
69		
70		
71		
72		
73		
74		
75		
79		
80		

Page No.	Rev No.	Date of Issue
81		
82		
83		
84		
85		
86		
87		
88		
89		
90		
91		
92		
93		
94		
95		
96		
97		
98		
99		
100		
101		
102		
103		
104		
105		
106		
107		
108		
109		
110		
111		
112		
113		
114		
115		
119		
120		

Intentionally Left Blank

Corrigendum of Amendments

No.	Ref	Description
01	01	New Issue

Intentionally Left Blank

Table of Contents

Intentionally Left Blank

Abbreviations and Acronyms

AT/RN	Aeronautical Telecommunication/Radio Navigation
ATS	Air Traffic Services
CAR	Civil Aviation Regulation
FMEA	Failure Modes and Effects Analysis
ICAO	International Civil Aviation Organization
ERP	Emergency Response Plan
PANS	Procedures for Air Navigation Services
SMS	Safety Management System
SRM	Safety Risk Management
SARPS	Standards and Recommended Practices
SPI	Safety performance Indicator
SPT	Safety performance target

Intentionally Left Blank

Definitions

Availability: The probability that a system will be able to perform its intended function when required for use.

AUTHORITY, means Directorate General of Civil Aviation Regulation - Public AUTHORITY for Civil Aviation.

Facility: an item of equipment or interconnected items of equipment at a location that forms part of a service.

Failure: Inability of the service to perform its intended service or Function Fault.

Failure Modes and Effects Analysis: is a safety assessment methodology for identifying system's failure modes with their effects and causes. The aim is to identify potential weaknesses and improve reliability, availability or safety.

Function Fault: Degradation in the performance of a service.

Hazard: A state, or set of conditions of a service, or an object, with the potential to cause an aircraft accident or air safety incident**.**

Hazard Identification: the process of recognizing that a hazard exists and defining its characteristics.

Maintainability: The ability of a service to be retained in, or restored to service.

Operational Requirement: The stated purpose of the service

Reliability: The probability that, during a certain period of time, a service performs its prescribed functions.

Risk: The probability of occurrence, together with the severity of the consequences, of a hazardous event.

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

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

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

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

Service: An aeronautical telecommunication service as defined in CAR 171.

Service Provider: A person approved to operate and maintain an aeronautical telecommunication service**.**

Intentionally Left Blank

FOREWORD

(1) The CAR 171 regulatory standards covering aeronautical telecommunication service providers require service providers to have Safety Management System processes in place to assess the safety implications and safety hazards involved in their operations, and to determine the action necessary to reduce the risks of those hazards to acceptable levels.

(2) This document provides guidelines for aeronautical telecommunication service providers to comply with that requirement.

(3) The following CARs are used as the base material for this manual:
   (a) CAR 171 – Aeronautical Telecommunication Service Provider
   (b) CAR 100 - Safety Management System

(4) The editing practices used in this document are as follows:
   (c) 'Shall' is used to indicate a mandatory requirement and may appear in CARs.
   (d) 'Should' is used to indicate a recommendation
   (e) 'May' is used to indicate discretion by the AUTHORITY the industry or the applicant, as appropriate.
   (f) 'Will' indicates a mandatory requirement and is used to advise of action incumbent on the AUTHORITY

Intentionally Left Blank

Chapter 1 – AERONAUTICAL TELECOMMUNICATION SAFETY MANAGEMENT

1.1. PURPOSE AND SCOPE

This document provides guidelines for aeronautical telecommunication service providers for the development and maintenance of safety cases covering CAR 171 services and which includes the process followed to assess the safety implications and safety hazards involved in their operations, and to determine the action necessary to reduce the risk of those hazards to acceptable levels.

1.2. SAFETY MANAGEMENT SYSTEM

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

One way of presenting such evidence and arguments is by preparing a safety case. A safety case is an explicit documentation of a safety related system, the corresponding safety objectives, and associated safety risk assessment and risk management of the system, at appropriate milestones in the life of the system.

1.3. AUTHORITY REQUIREMENTS FOR A SAFETY MANAGEMENT SYSTEM

1.3.1. To ensure that safety in the provision of aeronautical telecommunications services are maintained, the appropriate service provider shall implement safety management systems (SMS) for the aeronautical telecommunications services under its jurisdiction.

1.3.2. The objectives of aeronautical telecommunication services safety management are to ensure that:

a) the established level of safety applicable to the provision of aeronautical telecommunication services within an airspace or at an aerodrome is met; and
b) Safety-related enhancements are implemented whenever necessary.

1.3.3. An Aeronautical Telecommunication services SMS should include e, inter alia, the following with respect to the provision of air traffic services:

a) monitoring of overall safety levels and detection of any adverse trend;
b) safety reviews of aeronautical telecommunication services units;
c) safety assessments in respect of the planned implementation of airspace reorganizations, the introduction of new equipment systems or facilities, and new or changed ATS procedures; and
d) a mechanism for identifying the need for safety enhancing measures.

1.3.4. **SAFETY REVIEWS**

1.3.4.1. Safety reviews of Aeronautical Telecommunication services units shall be conducted on a regular and systematic basis by personnel qualified through training, experience and expertise and having a full understanding of relevant Standards and Recommended Practices (SARPs), Procedures for Air Navigation Services (PANS), safe operating practices and Human Factors principles.

1.3.4.2. The scope of Aeronautical Telecommunication services unit safety reviews should include

Operational and technical issues to ensure that:

a) the environmental working conditions meet established levels for temperature, humidity, ventilation, noise and ambient lighting, and do not adversely affect controller performance;
b) automation systems generate and display flight plan, control and coordination data in a timely, accurate and easily recognizable manner and in accordance with Human Factors principles;
c) equipment, including input/output devices for automation systems, are designed and positioned in the working position in accordance with ergonomic principles;
d) communications, navigation, surveillance and other safety significant systems and equipment:
    1) are tested for normal operations on a routine basis;
    2) meet the required level of reliability and availability as defined by the appropriate AUTHORITY;
    3) provide for the timely and appropriate detection and warning of system failures and degradations;
    4) include documentation on the consequences of system, subsystem and equipment failures and degradations;
    5) include measures to control the probability of failures and degradations; and
    6) include adequate backup facilities and/or procedures in the event of a system failure or degradation; and
e) detailed records of systems and equipment serviceability are kept and periodically reviewed.

Note. — In the context above, the terms reliability and availability have the following meanings:

1) Reliability. The probability that a device or system will function without failure over a specified time period or amount of usage; and
2) Availability. The ratio of percentage of the time that a system is operating correctly to the total time in that period.

1.3.5. **SAFETY ASSESSMENTS**

1.3.5.1. A safety assessment shall be carried out in respect of proposals for significant airspace reorganizations, for significant changes in the provision of ATS procedures applicable to an airspace or an aerodrome, and for the introduction of new equipment, systems or facilities, such as:

a) Re-sectorization of an airspace;
b) Physical changes to the layout of runways and/or taxiways at an aerodrome; and
c) Implementation of new communications, surveillance or other safety-significant systems and equipment, including those providing new functionality and/or capabilities.

1.3.5.2. Significant changes may affect the effectiveness of existing safety risk controls. In addition, new hazards and related safety risks may be inadvertently introduced into an operation when change occurs. Hazards should be identified and related safety risks assessed and controlled as defined in the service provider's existing hazard identification or SRM procedures.

1.3.6. **THE MANAGEMENT OF CHANGE**

1.3.6.1. The service provider's management of change process should take into account the following considerations:

a) Criticality. How critical is the change? The service provider should consider the impact on their activities, and the impact on other organizations and the aviation system.
b) Availability of subject matter experts. It is important that key members of the aviation community are involved in the change management activities.

c) Availability of safety performance data and information. What data and information is available that can be used to give information on the situation and enable analysis of the change?

1.3.6.2. Small incremental changes often go unnoticed, but the cumulative effect can be considerable. Changes, large and small, might affect the organization's system description, and may lead to the need for its revision. Therefore, the system description should be regularly reviewed to determine its continued validity, given that most service providers experience regular, or even continuous, change.

1.3.6.3. The service provider should define the trigger for the formal change process. Changes that are likely to trigger formal change management include:

a) introduction of new technology or equipment;
b) changes in the operating environment;
c) changes in key personnel;
d) significant changes in staffing levels;
e) physical changes (new facility or base, aerodrome layout changes etc.).

1.3.6.4. The service provider should also consider the impact of the change on personnel. This could affect the way the change is accepted by those affected. Early communication and engagement will normally improve the way the change is perceived and implemented.

1.3.6.5. The consideration of human factors has particular importance in SRM as people can be both a source and a solution of safety risks by:

a) contributing to an accident or incident through variable performance due to human limitations;
b) anticipating and taking appropriate actions to avoid a hazardous situation: and
c) solving problems, making decisions and taking actions to mitigate risks.

1.3.6.6. It is therefore important to involve people with appropriate human factors expertise in the identification, assessment and mitigation of risks.

1.3.6.7. The change management process should include the following activities:

a) **understand and define the change;** this should include a description of the change and why it is being implemented;

b) **understand and define who and what it will affect;** this may be individuals within the organization, other departments or external people or organizations. Equipment, systems and processes may also be impacted. A review of the system description and organizations' interfaces may be needed. This is an opportunity to determine who should be involved in the change. Changes might affect risk controls already in place to mitigate other risks, and therefore change could increase risks in areas that are not immediately obvious;

c) **identify hazards related to the change and carry out a safety risk assessment;** this should identify any hazards directly related to the change. The impact on existing hazards and safety risk controls that may be affected by the change should also be reviewed. This step should use the existing service provider's SRM processes;

d) **develop an action plan;** this should define what is to be done, by whom and by when. There should be a clear plan describing how the change will be implemented and who will be responsible for which actions, and the sequencing and scheduling of each task;

e) **sign off on the change;** this is to confirm that the change is safe to implement. The individual with overall responsibility and AUTHORITY for implementing the change should sign the change plan; and

f) **assurance plan;** this is to determine what follow-up action is needed. Consider how the change will be communicated and whether additional activities (such as audits) are needed during or after the change. Any assumptions made need to be tested.

Figure 1-1 provides an overview of the change management process for a service provider.

1.3.6.8. One appropriate methodology for addressing the above requirement is through the development and maintenance of a safety case, as per chapter 2.

Chapter 2 – REQUIREMENTS FOR A SAFETY CASE

2.1. REQUIREMENTS FOR A SAFETY CASE

2.1.1. The CAR 171 sets the basic standards for a safety case, or another equivalent safety assessment process, to be prepared by service providers, for:

a) all new services;
b) any changes (modifications or upgrades) to existing services the effect of which would be that the service would no longer be in accordance with the certificate issued to the service provider by AUTHORITY under regulation CAR 171;
c) any changes that require prior notification to AUTHORITY because of a requirement to do so in the service provider's safety management system; and
d) Withdrawal of an existing system.

2.2. SAFETY PLANNING

2.2.1. It is expected that safety will be built into any new CAR 171 service from its early inception and the management of safety related activities will be undertaken in a planned manner over the lifecycle of the service.

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

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

2.2.4. The distinct phases of CAR 171 service's life that would be covered by a safety case are normally:

a) **The Operational Requirements Phase**, when the role and broad functionality of the new service is determined. This phase should identify the safety objectives of the service and its applicable safety requirements, (these may be based on ICAO SARPS, AUTHORITY regulatory requirements, and the service provider's internal safety standards);

b) **The Design and Procurement Phase**, when the new or replacement service is designed and developed to meet the specified operational and/or engineering requirements. In this phase, the system configuration and operation is defined, incorporating the safety objectives and requirements within the evolving design. A full hazard and risk assessment is usually undertaken;

c) **The Installation and Pre-Commissioning Phase,** when the service is subject to procedural and/or engineering readiness testing against the design specifications, followed by operational trials, such as simulation. At this phase, the risk assessment is tested and validated by actual trials and testing of the installed system, and specific safety related operational, engineering and/or management

procedures are developed to obviate or control the identified risks; and

d) **The Commissioning and Routine Operations Phase,** when the safety of the service continues to be monitored and improved as any hazards are identified as they arise, and the risks are mitigated during actual operations.

2.2.5. The safety case should describe the historical and current safety status of the Aeronautical Telecommunication system as it develops throughout its entire lifecycle.

2.3. PURPOSE AND SCOPE OF THE SAFETY CASE

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

2.3.2. The purpose and scope of the safety case should be clearly stated in its introductory paragraphs, and should include:

a) A statement of the purpose and role of the service under consideration including the system Operational Requirement and a description of how it operates. The description of the system should include: its location; its configuration including the sub-system elements; the system boundaries; the elements of the system which have been considered within the scope of the document, i.e., whether it covers equipment, procedures, personnel, etc.; and the interfaces with other external systems.

b) A statement of the assumptions upon which the safety case is based. This should include the defined or known levels of safety, or integrity, of each of the interfacing or support systems/services, and those other services externally provided by third parties, such as those provided by telecommunications service providers, electrical power service providers, etc.

2.3.3. The relevant phases of the system, covered by the particular part/s of the safety case should also be defined.

2.4. SAFETY CASE COVERAGE OVER THE LIFECYCLE OF THE SERVICE

2.4.1. As previously discussed, safety cases should be developed in separate parts to define the safety situation of the service over the discrete stages of its lifecycle. A four-part Safety Case has been used to define the safety situation at the Operational Requirements stage, at the completion of the Design and Procurement phase, at Installation and Pre-Commissioning, and for the day-to-day Operational phase.

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

2.4.3. A guide to the coverage of each part of a four-part Safety Case is included in Appendix A "Safety Case Coverage for a Four Part Safety Case".

2.5. SAFETY OBJECTIVES AND SAFETY REQUIREMENTS

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

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

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

2.5.4. The selection of an appropriate way of expressing the safety requirements is important. Traditional measures include the specification of reliability, availability, continuity, maintainability, recoverability, accuracy, etc., which have some interdependence. In the case of CAR 171 services specifying only availability, without also specifying a limit on the rate of occurrence of failures and faults and the recoverability of the system following failure, could be insufficient to adequately define the safety requirements. For instance, a very infrequent occurrence of a fairly long down-time may be less hazardous than more frequent failures with shorter down-times. Quantitative statements of safety requirements should be used where possible, however, in many areas (e.g. where people and procedures are involved) it may not be feasible to define quantitative values. For these areas, qualitative values can be established. Where possible, these should be equated to corresponding quantitative values, within an accepted risk tolerability classification scheme.

Chapter 3 – RISK MANAGEMENT

3.1. METHODOLOGY

3.1.1. Safety Risk Management (SRM) is a key component of safety management and the appropriate methodology for the risk management, i.e., hazard identification, risk assessment, and risk control of CAR 171 services is required. The methodology may vary depending upon the type and safety implications of the proposed Aeronautical Telecommunication system, or system change, and the use of different methods, or combinations thereof, may be appropriate for the different elements and lifecycle phases included in the safety case.

3.1.2. Service providers should ensure they are managing their safety risks. This process is known as safety risk management, which includes hazard identification, safety risk assessment and safety risk mitigation.

3.1.3. The SRM process systematically identifies hazards that exist within the context of the delivery of its services. Hazards may be the result of systems that are deficient in their design, technical function, human interface or interactions with other processes and systems. They may also result from a failure of existing processes or systems to adapt to changes in the service provider's operating environment. Careful analysis of these factors can often identify potential hazards at any point in the operation or activity life cycle. Safety risk assessments and safety risk mitigations will need to be continuously reviewed to ensure they remain effective. Figure 3-1 provides an overview of the hazard identification and safety risk management process for a service provider.

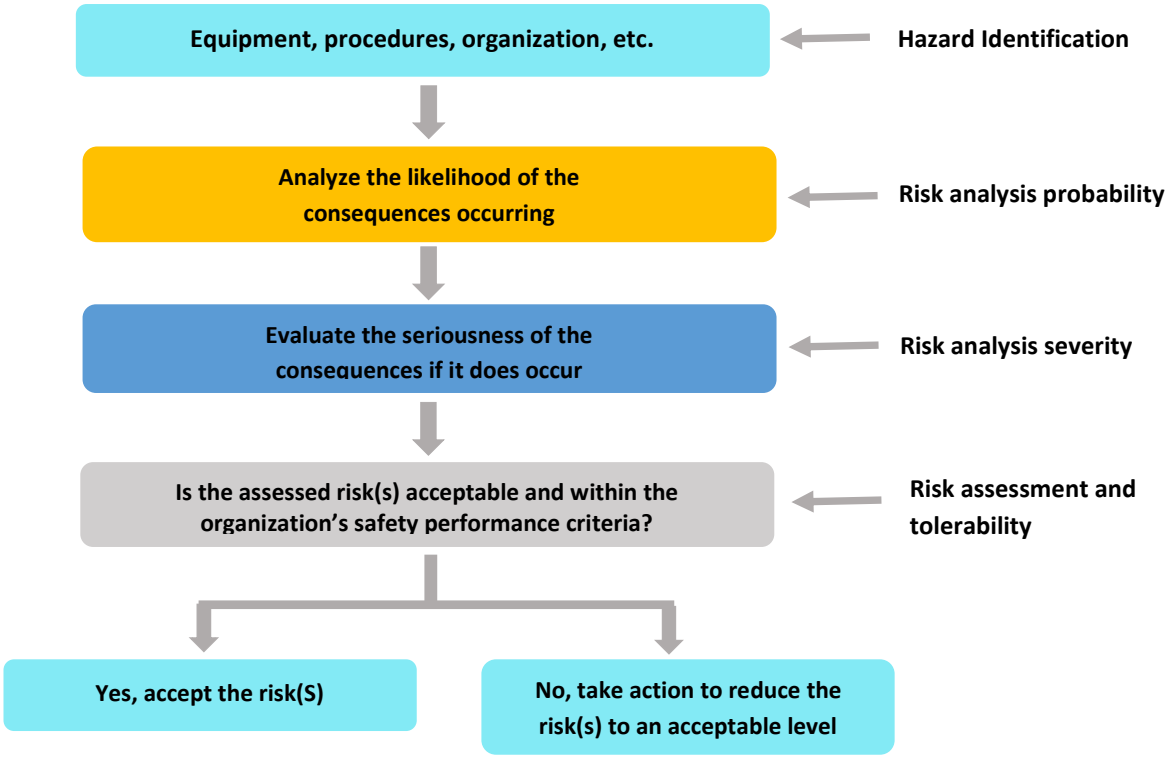

Figure 3-1. Hazard identification and risk management process.

3.2. HAZARD IDENTIFICATION AND RISK ASSESSMENT

3.2.1. Hazard identification is the first step in the SRM process.

The service provider should develop and maintain a formal process to identify hazards that could affect aviation safety in all areas of operation and activities. This includes equipment, facilities and systems. Any aviation safety-related hazard identified and controlled is beneficial for the safety of the operation. It is important to also consider hazards that may exist as a result of the SMS interfaces with external organizations.

3.2.2. Techniques for hazard identification/risk assessment include:

- the use of data or experience with similar systems/changes undertaken by overseas or other respected providers of similar CAR 171 services;
- quantitative modeling based on sufficient data, a validated model of the change, and analyzed assumptions;
- the application and documentation of expert knowledge, experience and objective judgment by specialist staff;
- trial implementation of the proposed change in an “off-line” system, or under surveillance and with sufficient backup facility to revert to the existing system before the change, if risks cannot be mitigated;
- a formal analysis / “Risk Analysis of Technological Systems;
- Reliability, availability and maintainability (RAM) analyses

3.3. SAFETY RISK ASSESSMENT CRITERIA

3.3.1. There are a number of ways in which CAR 171 service could cause, or contribute to, an aviation incident or accident. For example, if facilities that are used for air ground communication fail, or facilities that provide precision navigation functions directly to pilots lose integrity that affects their accuracy.

3.3.2. Lesser impacts on safety might arise where the integrity of a system is degraded or lost, but where there are alternative back-up systems, or contingency arrangements, in place to maintain separation.

3.3.3. In order to ensure that the range of possible safety risks are appropriately classified and controlled, service providers shall develop safety risk assessment model and procedures which will allow a consistent and systematic approach for the assessment of safety risks. Such a safety risk classification scheme provides a structure for deriving the safety requirements for services, as well as the criteria for risk control decisions. Typically, such schemes provide a standard relationship between the probability of occurrence of each risk and the categorized severity of the risk in terms of its potential impact on safety, finally equating that to a risk acceptability criterion. The acceptability rating will help determine what safety risks are acceptable or unacceptable and to prioritize actions.

3.3.4. A safety case document should include the risk assessment criteria (also termed a risk tolerability classification scheme) adopted by the service provider for safety management.

3.4. RISK CONTROL

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

- System Redesign, Modification or Replacement;
- Process or Procedures Redesign;
- Reliability Improvement Schemes;
- Personnel Education or Training; And
- Various Management controls on personnel, procedures and equipment.

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

3.5. PRECEDENCE OF RISK CONTROLS

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

APPENDIX A

SAFETY CASE COVERAGE FOR A FOUR-PART SAFETY CASE

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

Safety Case Part 1 - Operational Requirements Phase

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

Safety Case Part 2 - Design and Procurement Phase

Part 2 of the safety case is essentially to assure that the design of the system supports and provides for the safety requirements. Arguments to support the design rationale and the proposed technology of the system, and to verify and validate that such satisfies the safety requirements should be provided. The human factors aspects of the design, and the safety implications of the design of the procedures, and the ability of personnel to safely operate to the design procedures, should also be considered. Here, a full hazard and risk evaluation of the detailed design, including hardware, software, man/machine interface, human factors, equipment and administrative interfaces and external factors, should be undertaken.

Safety Case Part 3 - Installation and Pre-Commissioning Phase

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

Safety Case Part 4 - Normal Operations Phase

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

Note in respect to all Parts

It is important that all parts of the safety case be retained and maintained as necessary over the life of the service, reflecting the safety situation for any approved modifications or changes to the system.