Australian Government
Civil Aviation Safety Authority

# Advisory Circular

## AC 171-2(0) MARCH 2006

# GUIDELINES FOR THE PREPARATION OF SAFETY CASES COVERING CASR PART 171 SERVICES

**CONTENTS**



## 1. REFERENCES

This Advisory Circular (AC) should be read in conjunction with the Civil Aviation Safety Regulations – CASR Part 171 – Aeronautical Telecommunication Service and Radionavigation Service Providers, and the associated Manual of Standards (MOS) for Part 171. Those documents are available on the CASA website at: www.casa.gov.au.

## 2. PURPOSE OF THIS AC

The CASR Part 171 regulatory standards covering aeronautical telecommunication and radionavigation service providers require for 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. (Ref: CASR Part 171.086 and MOS-Part 171 Chapter 3.) This AC provides guidelines for service providers to comply with that requirement.

## 3. STATUS OF THIS AC

This is the first issue of AC 171-02. It remains current until re-issued, withdrawn or superseded. These guidelines were originally issued by CASA in CAAP Airways-1 dated February 1998.

***Advisory Circulars are intended to provide advice and guidance to illustrate a means, but not necessarily the only means, of complying with the Regulations, or to explain certain regulatory requirements by providing informative, interpretative and explanatory material.***

***Where an AC is referred to in a 'Note' below the regulation, the AC remains as guidance material.***

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

## 4. DEFINITIONS

The following definitions are applicable to this AC. They are not necessarily definitions that apply to CASR Part 171.

***service***: An aeronautical telecommunication service or aeronautical radionavigation service as defined in CASR Part 171.
***service provider:*** A person approved to operate and maintain an aeronautical telecommunication or radionavigation service.
***availability***: The probability that a system will be able to perform its intended function when required for use.
***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***: 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 recognising 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.

## 5. SAFETY MANAGEMENT SYSTEM

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

**5.2** 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.

**5.3** This document provides guidelines for the preparation and maintenance of safety cases covering Part 171 services.

## 6. CASA REQUIREMENTS FOR A SAFETY MANAGEMENT SYSTEM

**6.1** One of the elements of the Civil Aviation Safety Authority's regulatory requirements for safety management systems (SMS) is for service providers to have a process 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. (Ref: CASR 171.086 for SMS requirements, and MOS-Part 171 Chapter 3 section 2 for safety case standards.)

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

## 7. REQUIREMENTS FOR A SAFETY CASE

**7.1** MOS-Part 171 Chapter 3 sets the basic standards for a safety case, or another equivalent safety assessment process, to be prepared by service providers, for:

- all new services;
- 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 CASA under regulation 171.250;
- any changes that require prior notification to CASA because of a requirement to do so in the service provider's safety management system; and
- withdrawal of an existing system.

## 8. SAFETY PLANNING

**8.1** It is expected that safety will be built into any new Part 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.

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

**8.3** For those services that have a lifecycle consisting of several distinct phases, the hazards and associated risks may differ in type and degree in each phase, and their identification and control treatment will be more appropriately undertaken at a particular phase in the lifecycle. Accordingly, safety 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.

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

**8.5** The distinct phases of a Part 171 service's life that would be covered by a safety case are normally:

- **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, CASA regulatory requirements, and the service provider's internal safety standards);
- **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;
- **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 ghosting or mimicking. 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
- **the commissioning and routine operations phase,** when the safety of the service continues to be monitored and improved as any hazards are identified as they arise, and the risks are mitigated during actual operations.

**8.6** The safety case should describe the historical and current safety status of the airways system as it develops throughout its entire lifecycle.

## 9. PURPOSE AND SCOPE OF THE SAFETY CASE

**9.1** 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.

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

- A statement of the purpose and role of the service under consideration including the system Operational Requirement and a description of how it operates. The description of the 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.

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

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

## 10. SAFETY OBJECTIVES AND SAFETY REQUIREMENTS

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

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

**10.3** The 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.

**10.4** 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 Part 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 (refer to the next section).

## 11. RISK MANAGEMENT

### 11.1 Methodology

**11.1.1** An appropriate methodology for the risk management, i.e., hazard identification, risk assessment, and risk control of Part 171 services is required. (Ref MOS-Part 171 Chapter 3 section 2). The methodology may vary depending upon the type and safety implications of the proposed airways 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.

### 11.2 Hazard identification and risk assessment

**11.2.1** 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 Part 171 services;
- quantitative modelling based on sufficient data, a validated model of the change, and analysed assumptions;
- the application and documentation of expert knowledge, experience and objective judgement 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 in accordance with Australian Standard AS/NZS 3931 "Risk Analysis of Technological Systems - Application Guide", or another accepted standard or text on risk analysis/system safety;
- event tree analysis (ETA);
- quantified risk analysis (QRA);
- failure modes and effects analysis (FMEA);
- human factors analysis (HFA);
- hazard and operability studies (HAZOPs); and
- reliability, availability and maintainability (RAM) analyses.

### 11.3 Safety risk assessment criteria

**11.3.1** There are a number of ways in which a Part 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.

**11.3.2** 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.

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

**11.3.4** 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. Examples of existing risk assessment criteria for airways related services are available in the references.

### 11.4 Risk control

**11.4.1** A risk control process to eliminate or mitigate all risks categorised 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.

**11.4.2** 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.

### 11.5 Precedence of risk controls

**11.5.1** In the application of the above, or other, risk control processes, a safety precedence sequence should be adopted and applied. For instance, control of identified hazards should normally be sought first through improved 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.

## 12. SAFETY CASE COVERAGE OVER THE LIFECYCLE OF THE SERVICE

**12.1.1** 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.

**12.1.2** 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.

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

## 13. AUTHORITY FOR ISSUE AND CHANGE OF THE SAFETY CASE

**13.1** Safety Cases should be placed under a documentation control process.

**13.2** The Safety Case should be authorised by a competent authority designated by the service provider. For Part 171 services, an authority or authorities covering System Requirements, System Design, System Operation, and System Maintenance should be appointed, and the issue of the parts of the safety case should be made under the authority of one or more of these designated bodies, as appropriate to the content of each part.

**13.3** A guide to the requirements for authorisation of the four parts of the safety case is included at Appendix B to this AC - "Authorities for the Issue and Change of the Safety Case".

## 14. AUDITS OF SAFETY CASES

### 14.1 Internal monitoring and audit

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

### 14.2 CASA audits

**14.2.1** CASA, under its Surveillance Procedures Manual, may carry out audits of Part 171 services. The relevant documentation pertaining to the safety case may be a focus of such audits.

## 15. FURTHER READING & REFERENCES

The following references provide more detailed guidance on the development of System Safety Cases.


- UK Civil Aviation Authority, ATS Standards Department, **En-Route Regulation Information Package**, June 1994
- **Systematic Safety Management in the Air Traffic Services** by Richard Profit, published by Euromoney Publications PLC 1995 ISBN 1 85564 470 3
- Australian New Zealand Standard AS/NZS 3931:1998 **Risk Analysis of Technological Systems - Application guide** ISBN 0 7262 9905 7
- **IEC 61508-1 Ed 1.0 Functional safety of electrical/electronic/programmable electronic safety related systems**, International Electrotechnical Commission, 3 rue de Varembe, Geneva, Switzerland.
- United States of America MIL-STD- 882D 10 February 2000 **System Safety Program Requirements**
- **Safety-related systems, Guidance for engineers**, Hazards Forum, Issue 1 March 1995 ISBN 0 9525 103 0 8


---

Patrick Murray
Group General Manager
Air Transport Operations Group

INTENTIONALLY LEFT BLANK

**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 CASA to advise 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. Such amendments to the safety case should be authorised by the appropriate approval authority (refer to Appendix B).

## APPENDIX B

## AUTHORITIES FOR THE ISSUE AND CHANGE OF THE SAFETY CASE

The following is a guide to the requirements for authorisation of the four parts of the safety case:

### Part 1 to be approved by the System Requirements Authority (SRA)

The System Requirements Authority (SRA) is the body which has the authority for establishing the system operational requirements and the associated system safety objectives and requirements. Part 1 of a Safety Case should be authorised by the SRA.

### System Design Authority (SDA)

The System Design Authority (SDA) is the body which authorises the design of the airways system and the procedures, facilities, equipments and components of the service, including:

- the system design meeting operational specifications, safety objectives and requirements, and applicable external standards.
- the process, technology, functionality and physical structure of the system.

In the case of engineering based systems, a separate SDA may be nominated for both the engineering and the operational elements of the system. Part 2 of the Safety Case should be authorised by the SDA.

### System Operating Authority (SOA)

The System Operating Authority is the body which authorises the system operation, including:

- operational requirements;
- man-machine interface and human factors;
- acceptance of the system after verification by the necessary trials, engineering, ground and flight tests;
- ensuring that operational personnel and resources have the capability and capacity to operate the system safely;
- authorisation of the procedures for removal and return of the system to operational service;
- standards and training requirements for operational staff.

Parts 3 and 4 of the Safety Case are be authorised by the SOA (and the System Maintenance Authority in respect to the system maintenance aspects, see below).

**System Maintenance Authority (SMA)**

The System Maintenance Authority is the body which authorises the system maintenance aspects of the safety case, including:

- maintenance procedures;
- system maintainability requirements can be met;
- acceptance of the maintenance of the system, after the necessary trials and engineering tests;
- ensuring that maintenance personnel and resources have the capability and capacity to maintain the system to achieve the required levels of operational safety;
- authorisation of the procedures for the removal and return of equipment to operational service;

Parts 3 and 4 of the safety case should be authorised by the SMA (and the System Operating Authority in respect to the operational components, see above).