

# **FLIGHT INSPECTION ORGANISATIONS**

## **SAFETY MANAGEMENT GUIDELINES**



**International Committee for Airspace Standards and Calibration**

**Safety Management Group**

# **FLIGHT INSPECTION ORGANISATIONS**

## **SAFETY MANAGEMENT GUIDELINES**

### **CONTENTS**

#### **PART 1: PRELIMINARY MATERIAL**

1. INTRODUCTION
2. SCOPE
3. STRUCTURE
4. STATUS
5. REFERENCES
6. DEFINITIONS, SYMBOLS, AND ABBREVIATIONS

#### **PART 2: GENERAL SAFETY MANAGEMENT ISSUES**

7. ORGANISATION AND MANAGEMENT
8. OPERATING MANUAL
9. HARDWARE AND SYSTEMS ASPECTS
10. SOFTWARE ASPECTS
11. OPERATING INSTRUCTIONS
12. PERSONNEL TRAINING AND QUALIFICATION REQUIREMENTS
13. AOC ASPECTS
14. LEGAL REQUIREMENTS
15. ORGANISATIONAL CAPABILITIES

#### **PART 3: SAFETY MANAGEMENT DEVELOPMENT**

16. DEVELOPMENT OF CONCEPTS
17. SAFETY CASES

#### **ANNEXES**

- |           |   |                           |
|-----------|---|---------------------------|
| ANNEX A   | - | OPERATING MANUAL CONTENTS |
| ANNEX B   | - | SOFTWARE MANAGEMENT       |
| ANNEX C   | - | SAFETY CASE DEVELOPMENT   |
| ANNEX...D |   | GLOSSARY                  |

## **PART 1: PRELIMINARY MATERIAL**

### **1. INTRODUCTION**

- 1.1 The purpose of this document is to provide guidance to flight inspection organisations on the organisational and general issues within the safety management of flight inspection. In so doing, it complements the technical standards and criteria which apply to the provision of flight inspection services.
- 1.2 This document has been written as a safety management handbook for use by operating organisations themselves. Where applicable, however, it may also be used as a basis for safety regulation of such organisations by appropriate regulatory authorities. Its adoption and implementation in this role must remain a matter for National Aviation Authorities in each state.

### **2. SCOPE**

- 2.1 This document relates to organisations undertaking all forms of flight inspection, for airport, en-route and instrument approach procedure purposes. It also includes material on the development of formalised safety management systems, including the use of safety cases and safety analysis techniques. It is recognised that such aspects may not, at present, be generally developed or explicit in flight inspection organisations.

### **3. STRUCTURE**

- 3.1 The main body of this document is generic in nature, applying to all types of flight inspection tasks. Where specific systems or technologies require special safety management provisions, these have been detailed in separate appendices.
- 3.2 In the areas of organisational capabilities, competencies and certification of aircraft operations, application within States can vary according to national frameworks. States may therefore wish to deal with these issues by means of a national supplement to this doc.

### **4. STATUS**

- 4.1 This document is currently at draft discussion stage.

## 5. REFERENCES

- 5.1 Where appropriate, the document relates to relevant agreed standards and practices, with particular reference to ICAO documentation, such as Annex 10 to the Convention and ICAO Document 8071.
- 5.2 In addition, reference has also been made to a wide variety of publicly available safety management and analysis documentation.

## 6. DEFINITIONS, SYMBOLS AND ABBREVIATIONS

- 6.1 A glossary of definitions, symbols and abbreviations has been included at ANNEX D. Wherever applicable, these have been drawn from those agreed within ICAO.

*(A final glossary will be drawn up at the end of the drafting stage of the document, when contents and text are complete, and included at that time)*

## **PART 2: GENERAL SAFETY MANAGEMENT ISSUES**

### **7. ORGANISATION AND MANAGEMENT**

- 7.1 The safety objective of any organisation intending to perform flight inspection, within the scope of para 2 of this document, is that it is qualified and competent, having regard to any relevant experience, equipment, staffing, maintenance and other arrangements, to produce accurate and adequate flight inspection results.
- 7.2 In this respect, the purpose of this document is to examine the aspects of flight inspection work which affect, or have the potential to affect safety, and should therefore be afforded appropriate organisation and management.

### **8. EXPOSITION**

- 8.1 A comprehensive way for flight inspection organisations to commence addressing safety management issues is within an operating manual, covering the overall organisation and its intended operation. A suggested structure and list of contents is given in Annex A, but represents a minimum set of aspects to be covered. Specific operations or national contexts may require additions or enhancements to this list in order to adequately address the relevant safety issues in those cases.
- 8.2 The role of an operating manual is to:
- a) present and deal with safety issues in a complete, common and co-ordinated way
  - b) to act as source of information on these issues for reference by the organisation and its staff
  - c) to act as a source of information on these issues for reference by bodies with whom the organisation has safety interfaces
  - d) to act as the foundation of a formal safety management system

### **9. AIRCRAFT, HARDWARE AND SYSTEM ASPECTS**

- 9.1 **SAFETY OBJECTIVE. The management of aircraft, hardware and system aspects of flight inspection shall ensure that all applicable safety issues are identified and adequately resolved.**
- 9.2 The following are certain general aspects taken from the operating manual. All aspects in the manual should be similarly considered.
- 9.3 The system maintenance infrastructure should be adequate to preserve the specified functionality of the flight inspection system over its lifecycle. This includes documentation, records, programmes, logistics and personnel competence.

- 9.4 Configuration management of the flight inspection system should be maintained throughout its lifecycle. This includes all system aspects such as hardware, software, firmware, documentation and procedures. Change control procedures should be in place which take account of relevant responsibilities in areas such as the operating authority, design authority and quality management.
- 9.5 Total lifecycle support of the system should be adequate, including considerations of responsibilities, design support, review of faults and performance, service level agreements with subcontractors, system modifications and enhancements.
- 9.6 The organisation shall have a formalised quality management system in place. This should exhibit all the characteristics expected of a quality system as detailed in relevant regulatory publications or standards (eg. ISO 9000 series). Formal recognition or accreditation is not essential for the benefits of this approach to be realised.

## 10 SOFTWARE ASPECTS

- 10.1 **SAFETY OBJECTIVE. The management of software aspects and elements of the flight inspection system shall ensure that all applicable safety issues are identified and adequately resolved.**
- 10.2 Software is being used increasingly in technical systems. While this trend offers significant advantages in terms of data handling and presentation, the participation of software in the safety performance of the flight inspection system needs careful attention, and appropriate safety management.
- 10.3 Various international software standards exist, and may be relevant to this application, but do not completely cover the range of tasks and roles undertaken by software in the flight inspection process. Accordingly, the need is identified for a comprehensive approach to the safety management of software, and this is addressed by the additional material contained in Annex B of this report.

## 11. OPERATING INSTRUCTIONS

- 11.1 **SAFETY OBJECTIVE. The operating instructions shall ensure that all measurements are made to defined and documented procedures.**
- 11.2 This documentation should include concise details of:
- (a) The flight profile to be used for each individual measurement.
  - (b) Pre-flight calibration of measuring equipment. (i)
  - (c) Siting of any necessary ground tracking or position fixing equipment
  - (d) Scheduled maintenance and calibration of the measuring equipment. (i)

- (e) Operation of the measuring equipment. (i)
- (f) Production of the flight inspection report
- (g) Certification of both equipment and personnel.
- (h) The method of calculating any results which are not directly output by the measuring equipment.

*Note:* (i) indicates flight inspection aircraft.

## 12. PERSONNEL TRAINING AND QUALIFICATIONS REQUIREMENTS

- 12.1 **SAFETY OBJECTIVE. All personnel concerned with the flight inspection tasks identified in this scope shall be adequately trained and qualified for their job functions.**
- 12.2 The organisation needs to be able to demonstrate that all personnel concerned with the flight inspection are adequately qualified for their job functions.
- 12.3 The organisation should be equipped with CV's/résumé's for all personnel directly concerned with flight inspection, from which each person's experience and suitability can be determined.
- 12.4 The organisation should have a procedure for ensuring the competence of its personnel, both initially and on a continuing basis.
- 12.5 For all flight inspection asks, the flight crew's familiarity with each location to be inspected is considered to be of importance. The organisation's procedures and instructions must therefore include details of appropriate training in this respect.

## 13. AIRCRAFT OPERATING ASPECTS

- 13.1 **SAFETY OBJECTIVE. In respect of aircraft operations, flight inspection organisations shall be adequately qualified to undertake their declared flight inspection tasks.**
- 13.2 Organisations seeking to perform flight calibration may need to hold applicable regulatory approvals certifications (eg. an Operators Certificate). This requirement will be determined by the nature of the organisation's business. In the first instance, advice and/or guidance should be sought from the relevant regulatory body.
- 13.3 Organisations already holding an appropriate regulatory approval/certification may be subject to regulatory oversight by the relevant regulatory body when engaged in calibration work and are advised to contact the relevant regulatory representative for further information.

## 14. LEGAL REQUIREMENTS

14.1 **SAFETY OBJECTIVE. Flight inspection organisations shall operate in accordance and compliance with all applicable legal requirements.**

14.2 Any general legal requirements should be raised in consultation with relevant regulatory legal representatives during the course of any approval action. Organisations are generally bound to comply with all such requirements and any conditions contained within any approvals issued to them.

## 15 ORGANISATIONAL CAPABILITIES

15.1 **SAFETY OBJECTIVE. The safety of flight inspection operations shall be ensured by matching the declared scope of flight inspection tasks with appropriate and adequate organisational capabilities.**

15.2 The operating conditions under which flight inspection is undertaken in the various regions and countries of the world vary a great deal. Where appropriate, therefore, it is necessary for flight inspections to have, and to deploy, operating capabilities which are designed to meet the total range of conditions which can be anticipated within their declared scope of tasks.

15.3 Where this is necessary, it is essential that such capabilities are afforded appropriate safety management. Such capabilities may include:-

- (a) night operations
- (b) operations at busy airports, including handling traffic delays
- (c) operations in poor/restrictive weather
- (d) operations involving long sectors and/or positioning flights

15.4 The provision of any or all such operating capabilities should be analysed from a safety management viewpoint to ensure that they are capable of matching the required demands, and be reflected where necessary in appropriate additional technical and operational systems and procedures.

## **PART 3: SAFETY MANAGEMENT DEVELOPMENT**

### **16 DEVELOPMENT OF CONCEPTS**

- 16.1 The purpose of this section is to consider the role and development of a formal safety management system in flight calibration organisations. The other sections of this document do not elaborate on this concept but do touch on certain aspects such as safety classification and safety reviews of software.
- 16.2 The introduction of a formal safety management system should result in an organisation that pro-actively handles safety. The provisions of this document should ensure to a large extent that this happens, but the handling of safety is not made an explicit function unless a formal safety management system is introduced, together with the production and use of safety assessment/justification documentation such as safety cases.
- 16.3 There are many publications relating to safety management systems but, to summarise these briefly, the organisation should have the following in place:
- (a) Safety policy statements
  - (b) Safety accountabilities of key personnel
  - (c) Safety Management Manual
  - (d) Implementation of safety policy and staff safety training
  - (e) Safety auditing
  - (f) Incident investigation/fault reporting/safety review process
  - (g) Safety cases for all aspects of the organisation and flight inspection system, and changes to either
  - (h) Safety classification and analysis of the flight inspection system, including hardware, software, firmware, procedures and personnel, and changes thereto
  - (i) Communication arrangements in the organisation in respect of safety issues, changes to the system, organisation, operating manual or operating safety case, including (where applicable) communications with relevant regulatory authorities.

### **17 SAFETY CASES**

- 17.1 Within the operation of the organisation's safety management system, it is necessary to have a means of providing appropriate assurance, on a continuing basis, of the organisation's safety performance. Safety cases have been shown to be a flexible, robust and comprehensive method of achieving this aim, and their use is therefore offered as one suggested way of maximising the benefits of safety management.

- 17.2 As a basis for providing a Safety Case applicable to an organisation, an operating manual can be developed into such a document. This entails the inclusion of information as specified in (a) to (i) above, together with arguments for safety adequacy for each topic in the operating manual. Hence, the operating manual would cease to be simply a descriptive document, but would become document giving the case for adequacy (a Safety Case). It is envisaged that the 'safety adequacy' would be related to the requirements for aircraft operation, and for consistently and accurately producing calibration and measurement reports.
- 17.3 The Safety Case would be subject to configuration control and amendment in accordance with changes. Such changes would themselves be subject to a form of safety analysis or safety case, and this would then be used as a basis for updating the above mentioned Safety Case. Where applicable, the regulator would be alerted to changes and would hold an up to date copy of this Safety Case.
- 17.4 Further information on the development of safety cases is given in Annex C to this document.

## ANNEX A

### OPERATING MANUAL CONTENTS

A.1 The following sections give a suggested structure and contents of an operating manual document for an organisation undertaking flight inspection work. The areas outlined below constitute a minimum, and may be enhanced to suit the needs of particular state or flight inspection tasks.

#### A.2 IDENTIFICATION/GENERAL

- (a) Organisation name, document title, reference number.
- (b) Base location.
- (c) Amendment status, issue number, date, amendment record.
- (d) Approval by appropriate manager.
- (e) Distribution list.
- (f) Operating manual administrator.
- (g) Contents list
- (h) Purpose of document.

#### A.3 ORGANISATION

- a) Introduction to and general information on, the organisation.
- b) An organisational chart or organogram.
- c) Interfaces with other organisations and/or departments.
- d) General statements of organisational policy as related to safety.
- e) Past experience in relevant areas.

#### A.4 UNDERTAKING

To define the range and scope of flight inspection tasks to which the operating manual will apply.

#### A.5 PERSONNEL/STAFFING

- a) Personnel responsibilities, qualifications, terms of reference and authority to act.
- b) Staffing arrangements and levels in so far as they affect safety.
- c) Personnel training, competency qualifications and recency checking arrangements.

## A.6 PROCEDURES

- a) Procedures to record and major changes to the organisation.
- b) Procedures to document the latest flight inspection programme, updated on a regular basis.
- c) Procedures to record proposed equipment changes and modifications or change of aircraft type.
- d) Procedures/instructions for all aspects of the flight inspection process, to include calibration of equipment, provision of flight inspection reports as well as operating instructions for inspectors and flight-crew.

## A.7 EQUIPMENT

- a) Details of all aircraft types used for flight inspection.
- b) Function description, technical specification and manufacturers type number for all major items in the flight inspection system. This includes details of the equipment used in equipment calibration and integration testing.
- c) Location, characteristic and type of all measurement details on the aircraft.
- d) Technical description of any parts of the flight inspection system which the operator has designed or built.
- e) For all hardware and software equipment, there should be a statement of
  - i) the Design Authority
  - ii) configuration control responsibility (if applicable)
  - iii) the operating responsibility.
- f) Details of all uses of software and firmware used in the measurement system, including support arrangements of these aspects.
- g) Details of support arrangements for the flight inspection system, including any subcontractors and suppliers, and their qualifications.

## A.8 WORK CONTROL

Details should be provided of:

- a) Log or record system(s) for faults and maintenance of the measurement system.
- b) Arrangements for handling and reporting major events or incidents which affect, or have the potential to effect, the safety performance of the flight inspection system.
- c) Spares holding and control.
- d) Documentation Control, including a list of documents held or produced.
- e) Workshop facilities, both internal and in relation to sub-contractors.
- f) Maintenance arrangements and programmes.
- g) Internal and external auditing systems.
- h) Quality Management system.
- i) Procedures for general control of sub-contractors, including details of agreements/responsibilities.

## A.9 RESULTS

In support of the results generation process, the following should be included:

- a) A typical or test flight inspection report.
- b) A typical or test sample of an ILS structure measurement for both localiser and glidepath.
- c) A statement showing to 95% confidence, the measurement uncertainty which the organisation claims to achieve for each of the measurable parameters.
- d) Details of statistical methods or interpolative techniques which may be applied.

## A.10 CAPABILITIES

Details should be included of specific or additional capabilities with which the flight inspection is equipped in order to undertake specific tasks. Such capabilities could include (where applicable) arrangements, including operating procedures for:-

- a) flight inspection at busy airports, where movement co-ordination and delays may be experience/required.
- b) flight inspection at night.
- c) flight inspection in poor weather.
- d) flight inspection involving long-range sectors and/or positioning.

## A.11 REGULATORY ISSUES (where applicable)

Where the flight inspection organisations is subject to formal safety oversight by a safety regulatory body, the following criteria should also be presented:-

- a) details of any formal or implicit approvals which the organisation has received.
- b) a list of tasks which the organisation regularly undertake under such approvals, to include
  - i) type of facility
  - ii) location of facility
  - iii) category of facility (if applicable)
  - iv) Instrument Approach Procedures related to the above (where applicable)
- c) details of any approvals related to an Operator's Certificate (or similar) held in respect of any aircraft operation related to flight inspection.

## ANNEX B

### SOFTWARE MANAGEMENT

#### Software Safety

B.1 The following sections detail specific requirements relating to the safety of software contained in flight calibration systems.

B.2 *SOFTWARE DESIGN AUTHORITY*

A Software Design Authority should be appointed. The Software Design Authority should be responsible for the safety of all aspects of the design, development, testing and production of software contained in the flight calibration system.

B.3 *SOFTWARE SAFETY CLASSIFICATION*

B.3.1 The Design Authority should ensure that the software safety requirements are properly defined, consistent and complete. Certain components of flight calibration systems are considered 'safety related'. These safety related components should include at least those that are necessary for the correct calculation of:

- measured ILS critical parameters
- positional, tracking and essential timing information relating to those measurements

B.3.2 For safe operation, the continuing approval of an ILS is contingent upon these critical parameters lying within the specified range of values (hence those components of the flight calibration system responsible for the measurement and calculation of these values in space should be considered safety related).

**Note 1:** *The safety requirements should include those necessary for system calibration and self test.*

**Note 2:** *Not all software need be considered safety related but, justification will be required if such a case is to be made.*

**Note 3:** *Display and presentation software may also need special consideration if such software is used to produce flight inspection records in support of a satisfactory flight inspection and continued ILS operation.*

*(depending on the safety significance of the role/function of this software, "special consideration" may involve some or all of the provisions for safety related software detailed below.)*

## B.4 SAFETY RELATED SOFTWARE

B.4.1 Safety related software within Flight Calibration Systems should be subject to appropriate formal analysis in the specification, design, development, coding and testing stages to assure the:

- integrity of input and output data  
(i.e. data required for the calculation of critical parameters)
- correctness of algorithms processing such data
- other safety performance requirements

**Note:** *This formal analysis is an essential part of the argument for the safety of the flight calibration system and will provide specific evidence in support of any approval required.*

B.4.2 Proper account should be taken of other aspects of the system that relate to the integrity, correctness and safety performance requirements such as the physical characteristics of the hardware and its environment and how these are modelled in the software.

## B.5 ANALYSIS OF SAFETY RELATED SOFTWARE

B.5.1 Formal analysis of safety related software in flight calibration systems should include:

- (a) a rigorous specification of the method of measurement of the critical parameters, positional, tracking and timing information, including and justifying any assumptions made.
- (b) formal argument in support of the correctness of design with respect to the specification.
- (c) formal argument in support of the correctness of the implemented code with respect to the design.
- (d) specification and analysis of test coverage to demonstrate the:
- (e) correctness of algorithms
- (f) internal consistency of modules
- (g) adequacy of subsystem interfaces

## B.6 SAFETY REVIEWS

At appropriate intervals, the Design Authority should carry out formal safety reviews of the specification, design, testing and coding. These reviews should be recorded.

# General Software Engineering Considerations

## B.7 *SOFTWARE ENGINEERING PRACTICE*

B.7.1 The Design Authority should prepare a code of software engineering practice for all procedures, methods, techniques and tools used in the development of software, based on software standards that nationally apply.

## B.8 *SOFTWARE LIFECYCLE*

B.8.1 A clearly defined and documented software development process should exist and include the following phases:

- (a) System and software requirements
- (b) System and software design
- (c) Code implementation and unit testing, in both static and airborne dynamic environments.
- (d) System integration and testing
- (e) Software maintenance

B.8.2 Each phase should have clearly established development and performance standards and procedures.

B.8.3 During system development, each phase should have specific input and output requirements and corresponding deliverables which should be fully documented and placed under configuration management.

## B.9 *SOFTWARE TOOLS*

All software tools employed in the production of flight calibration systems should be identified, including the system release and version, options selected and mode of use. Care should be taken in the selection of such tools to assure their safety and integrity. Typically such tools might include:

- (a) development tools and environments
- (b) compilers and linkers
- (c) test and debugging tools
- (d) other verification and validation tools
- (e) configuration management tools
- (f) documentation tools

## B.10 *SOFTWARE CONFIGURATION MANAGEMENT*

B.10.1 The Design Authority should identify personnel responsible for configuration management and the control and release to configuration management of all configurable items.

B.10.2 All configurable items should be held under configuration management control for all phases of the system lifecycle. All configurable items should be traceable to the software requirements.

## B.11 *SOFTWARE CHANGE CONTROL*

B.11.1 Procedures for the control of software changes should exist. Each proposed change should be assessed and details of the nature of the change and its likely effect on the system documented. All relevant documentation should be updated to reflect the change when approved and the change history maintained.

B.11.2 Changes to supplied or supporting software or software tools (e.g. compilers) should be monitored and controlled.

B.11.3 Changes that affect any formal approval of the system should first be notified to the regulator for approval before being introduced into service.

B.11.4 As software changes or updates may be applied independently to individual components making up the total flight inspection system, software change control procedures should also address and ensure the continued compatibility between system components.

## B.12 *SOFTWARE QUALITY ASSURANCE*

B.12.1 The Design Authority should appoint personnel responsible for software quality assurance. Such personnel should be responsible for the identification and evaluation of quality problems and authorised to ensure the necessary corrective actions are taken.

B.12.2 Software quality assurance should ensure that delivered software items conform to requirements. This should be achieved by the construction of a software quality plan covering all phases and aspects of software development. Conformance should be assured by:

- (a) software reviews
- (b) quality audits
- (c) software configuration audits
- (d) problem reporting and corrective actions

B.12.3 Reviews and audits should be scheduled within the software quality assurance plan.

### B.13 *PERSONNEL*

The Design Authority should ensure that the qualifications, experience, responsibility and authority of all personnel engaged in the production of software are appropriate to their tasks.

### B.14 *DOCUMENTATION*

All documentation supporting system software should be adequate, correct, current and under configuration management control throughout the system lifecycle.

#### B.14.1 Software Configuration Document

A top level document should exist identifying all applicable software documentation and for each document, details of its current status, purpose and contents.

### B.15 *SUBCONTRACTORS SOFTWARE*

The Design Authority should ensure that software supplied by subcontractors and other suppliers conforms to the relevant safety requirements where appropriate. Similar assurance should be required for embedded software.

# ANNEX C

## SAFETY CASES

### C.1 *INTRODUCTION*

The purpose of this Annex is to generally present the concept of safety cases, their use, and how they may assist in the management and, where required, the regulation of safety.

### C.2 *DEFINITION AND SCOPE OF SAFETY CASES*

C.2.1 A Safety Case can be defined as:

"A document which clearly and comprehensively presents sufficient arguments and evidence that a facility, an operation or an organisation is adequately safe in defined respects."

C.2.2 The reference to "defined respects" means that the document has specific scope which relates to particular objectives. For example, a safety case can address the safety of personnel at work, the safety of the general public or the safety of specific people such as those carried by aircraft, or a defined combination of these.

C.2.3 Safety cases constructed for air traffic services, for example, address the safety aspects of maintaining aircraft separation from each other and from obstacles. Their prime purpose is therefore aimed at addressing the safety of passengers. Determining the scope needs especially careful consideration when constructing a safety case. Further, it is important that a safety case addresses all relevant aspects relating to safety in the scoped area. In the context of flight inspection, the scope would normally encompass the provision, by an organisation, of a defined flight inspection service.

C.2.4 A safety case is not only a descriptive document, but also includes two other vitally important functions. In addition to the descriptive element, a safety case will:

- (a) examine each topic area and determine the risks and safety issues to be addressed, and
- (b) present arguments which demonstrate how these risks have been dealt with.

C.2.5 The intended overall conclusion of a safety case is that the person responsible for the areas covered by the safety case has done everything that can reasonably be done to ensure the safety of those areas. The person who bears the safety responsibility for the areas within the defined scope is therefore the "owner" of the safety case.

C.2.6 Sometimes safety requirements cannot be easily identified as stand alone items. They are often embedded within technical specifications and standards. In many cases therefore, a Safety Case may simply be expressing how a particular aspect of a system or organisation complies with a required standard or recommended practice.

### C.3 *SAFETY CASES IN THE CONTEXT OF SAFETY MANAGEMENT*

C.3.1 Safety Cases should be considered as part of a safety management system. Such a system has an explicit and pro-active approach to safety. As a basis, safety management systems are founded upon those elements of quality management which provide the fundamentals of documentation control, configuration management, training and ongoing performance analysis and feedback.

C.3.2 The key ingredients of a safety management system are:

- Safety Policy statements.
- Safety Accountabilities of key personnel.
- Safety Management Manual.
- Implementation of Safety Policy and staff safety training.
- Safety auditing.
- Incident investigation/fault reporting/safety review process.
- Safety Cases for the organisation, "systems"\* and changes thereto.
- Safety classification and analysis of 'systems' including hardware, software, firmware, procedures and personnel and changes thereto.
- Communication arrangements in the organisation and with the both the regulator and other bodies or organisations related to service provision.

( \* "systems" meaning equipment, procedures and personnel.)

### C.4 *TYPES OF SAFETY CASE*

C.4.1 There are two main types of safety case. An Operating Safety Case addresses the organisation and systems which are used in order to undertake the current operation. A key feature of this type of safety case is that it must be maintained as fully up-to-date, and will therefore reflect the operation at any given point in time.

C.4.2 The other type, a Change Safety Case, addresses all types of changes to the current operation. For significant changes, Change Safety Cases are often associated with projects, but the scope of these can often encompass not only changes to the flight inspection system itself, but can also include, for instance, changes to aircraft operations, operating procedures and also relevant changes to the flight inspection organisation. A Change Safety Case contains all the information required to address a proposed change from a safety viewpoint, and can therefore readily serve as the means of updating the Operating Safety Case when the change is implemented.

## C.5 CONTENTS OF AN OPERATING SAFETY CASE

As mentioned above, the scope of safety cases has to be carefully considered, and in turn will determine their actual contents. The Operating Safety Case addresses the existing or prevailing operation, and the following are suggested topic areas for inclusion:

### C.5.1 General

- (a) Safety and quality management systems description including policy and procedures. (See above reference to safety management system characteristics including aspects such as safety auditing).
- (b) General organisational description including explanation of interfaces between various areas and the corporate structure.
- (c) Regulatory interfaces including any mandatory reporting arrangements.

### C.5.2 'Operational'

This relates to the services provided by an organisation and how they are provided.

- (a) A description of the service provided.
- (b) The specific organisational structure providing the service.
- (c) The procedures for delivering the service.
- (d) The arrangements for assuring and maintaining service provision personnel competence. Such competence will be broken down into specific tasks making up the service.
- (e) Interfaces both within the specific organisation and external to it. How these are defined, agreements made and controlled.
- (f) How changes are implemented to the service and how they are analysed for their effects and requirements.
- (g) Manning levels (for operational service).
- (h) Service design authorities.
- (i) Service performance monitoring.
- (j) Man machine interfaces and environment.
- (k) Handling of emergencies.
- (l) Service documentation arrangements (controlled by a QMS).

### C.5.3 Operational Support

This relates to arrangements that support service provision. It generally relates to the engineering systems that facilitate the service being provided and covers hardware, software and logistics.

- (a) Functions provided by the support arrangements.
- (b) The specific organisational structure related to the support arrangements.
- (c) Description and analysis of support arrangements e.g. description of equipments and systems detailing features related to safety, failure modes, integrity checking.
- (d) The procedures related to support arrangements.
- (e) The arrangements for assuring and maintaining operational support personnel competence. Such competence will be broken down into specific tasks related to support arrangements, e.g. maintenance tasks.
- (f) Interfaces both within the specific organisation and external to it. How these are defined, agreements made and controlled. An example would be the control of sub-contractors providing maintenance or modification support.
- (g) How changes are implemented to the support arrangements/engineering systems and how they are analysed for their effects on the service provided.
- (h) Manning levels (for operational support)
- (i) Design authorities., e.g. for specific equipments and systems.
- (j) Support arrangement performance monitoring e.g. reliability/integrity of specific equipments and systems against specified requirements.
- (k) Handling of emergencies.
- (l) Support documentation arrangements (controlled by QMS) e.g. equipment/system maintenance manuals.
- (m) Installation arrangements.
- (n) Post design support services.
- (o) Environment.
- (p) Logistics.
- (q) Recording arrangements for post incident analysis.

## C.6 CHANGE SAFETY CASES

C.6.1 As referred to above, if there are any changes to the prevailing situation in any of the above topic areas, then some form of safety analysis should take place to determine the significance of such changes. This analysis may take the form of a Safety Case in its own right (a Change Safety Case), or perhaps simply a document addressing the particular change. In either case, the Operating Safety Case should be updated, if the change is considered significant enough. In a Change Safety Case, it is helpful to approach the analysis in chronological form, following the life-cycle of the change, and addressing the following possible topics:

- (a) Need for change.
- (b) Requirements for new system/arrangements. These would normally be 'operational' requirements related to the service provided. Sometimes it may not be possible to provide quantitative requirements. It may at times only be possible to quote particular standards and recommended practices which have to be adhered to.
- (c) Hazard and risk assessment. This may not always be feasible or possible as certain requirements, especially in pure service terms, human factors, procedures etc., can only be qualitatively expressed.
- (d) Determination of specific performance requirements. This may not always be possible in quantitative terms but generally equipment and systems supporting services will have some reliability and integrity specification to meet.
- (e) Design analysis against specific performance requirements.
- (f) Installation arrangements.
- (g) Testing and integration arrangements.
- (h) Analysis of outstanding issues arising from testing and integration to determine acceptability.
- (i) Arrangements for transition into service including training and de-commissioning of any existing systems.
- (j) Arrangements for supporting and maintaining the systems/new arrangements arising from the change.

C.6.2 The provision of normal project documentation can form the basis of the Change Safety Case. Such a Safety Case could be maintained for each system etc. related to the change, or as indicated above, incorporated into the Operating Safety Case by abridging the appropriate parts.

## *C.7 HAZARD/RISK ASSESSMENT*

C.7.1 As mentioned previously, a safety case should include safety arguments. This may not always be possible in a quantitative sense, but an argument should be presented, to the extent possible, that a particular topic area has been adequately addressed. This may, at times, only be feasible by addressing particular standards and recommended practices that have to be met.

C.7.2 In terms of quantitative analysis there are various techniques available. The most commonly-used process involves the following steps:

- (a) determination of the function or service to be provided
- (b) identification of the hazards associated with that service
- (c) categorisation of the criticality of the hazards
- (d) assignment of acceptable probabilities of occurrence to each hazard category
- (e) derivation of the performance requirements
- (f) failure mode analysis to determine design acceptability and assign performance requirements to sub-system parts.

C.7.3 There are numerous formal techniques available to support the above tasks, such as FMECA, fault tree analysis, and HAZOPS for both quantitative and qualitative analysis.

## *C.8 REGULATORY ARRANGEMENTS*

C.8.1 The regulatory arrangements will depend on the philosophy of each industry sector. Regulatory acceptance or approval can be afforded to the service provider by accepting the arguments in the particular safety cases and endorsing the particular safety management system. The amount of 'freedom' a service provider is allowed will depend upon the particular regulatory philosophy.

C.8.2 A possible scenario is that once initial acceptance or approval is granted by the regulator via a submitted Operating Safety Case, then further approval is not required for each change. Rather, the service provider is required to alert the regulator via an agreed interface and the regulator can 'sample' audit any change as it sees fit. The alerting would be via an agreed arrangement, including notifying the regulator of amendments to the Safety Cases. This has been found to work well in situations where developed safety management systems are in place.

## Annex D-Glossary of Definitions, Symbols and Abbreviations

This Glossary contains terms that have a specific meaning in civil aviation, safety, or regulatory matters.

The definitions annotated 'ICAO' have been taken directly from Annex 2 or PANS/RAC (Document 4444). Terms annotated 'A' have a different interpretation to ICAO and those annotated 'B' are not defined by ICAO but require clarification.

The definitions annotated 'ITU RR' have been taken from the International Telecommunication Union (ITU) Radio Regulations 1990 Edition. Note that terms printed in italics in the text of a definition are also defined by the Radio Regulations.

Those terms not annotated are used frequently and are considered to require clarification or explanation.

### DEFINITIONS

Accuracy	Recommended accuracy requirement for general operational use. The stated value of required accuracy represents the uncertainty of the reported value with respect to the true value and indicates the interval in which the true value lies with a stated probability. The recommended probability level is 95 per cent, which corresponds to the 2's level for a normal (Gaussian) distribution of the variable. The assumption that all known correction are taken into account implies that the errors in the reported values will have a mean value (or bias) close to zero. Any residual bias should be small compared with the stated accuracy requirement. The true value is that value which, under operational conditions, characterizes perfectly the variable to be measured/observed over the representative time, area and/or volume interval required, taking into account siting and exposure. (CIMO definition).
Act (the)	The current version of the Civil Aviation Act.
Aerodrome	Any area of land or water designed, equipped, set apart or commonly used for affording facilities for the landing and departure of aircraft.
Aeronautical Fixed Service	A telecommunication service between specified fixed points provided primarily for the safety of air navigation and for the regular, efficient and economical operation of air transport. [ICAO Annex 11 Chapter 1] Note: The ITU RR1-4 23 3.4 uses wording 'A <i>radiocommunication service</i> ' which is restricted to the utilisation of radio systems, whereas the ICAO definition includes transmissions by wire, optical or other electromagnetic systems. [For the purposes of this publication the ICAO definition will be used
Aeronautical Information Service (AIS)	Publisher of NOTAMs.
Aeronautical Mobile Service	<i>A mobile service between aeronautical stations and aircraft stations, or between aircraft stations, in which survival craft stations may participate; emergency position-indicating radiobeacon stations may also participate in this service on designated distress and emergency frequencies.</i> [ITU RR1-5 34 3 151 [ICAO Annex 11 Chapter 11
Aeronautical Station	A land station in the aeronautical mobile service. In the ANO the term aeronautical radio station is used.
Air-Ground Communication	Two way communications between aircraft and stations or locations on the surface of the earth. (ICAO)
Air Traffic	All aircraft in flight or operating on the manoeuvring areas of aerodromes. (ICAO)



Connection Delay	The time between a request to establish a connection with a system and the corresponding confirmation.
Continuity of Service	The ability of a system to complete its required function.
Controlled Airspace	An airspace of defined dimensions within which air traffic control service is provided to IFR flights.
Critical Equipment Parameter	Means a facility performance parameter that can have a direct effect on the operational integrity of the facility
Data Communications Network	The digital communication equipment, sub-networks and protocols that provide for the transfer of data from one data link end system to another.
Data Communications Service Provider	An organisation that provides the means to transfer data between an ATS facility and aircraft
Data Link Application	The implementation of data link technology to achieve specific Air Traffic Management (ATM) operational functionalities.
Data Link Service	A set of ATM related transactions, both system supported and manual, within a data link application? which have a clearly defined operational goal. Each data link application is a description of its recommended use from an operational point of view.
Data Link Service Provider	The organisation with overall accountability for the data link service. This includes the operational requirements of the data link system.
Data Link System	The total set of equipment that is required to provide the data link service
Dead Band	A term used to describe the cross-over characteristic on a 360° potentiometer or position resolver and optical encoder alignment errors.
Decision Height	A specified height at which a missed approach must be initiated if the required visual reference to continue the approach to land has not been established. (ICAO)
Displayed Gust	This is a wind speed, averaged over a 3 second sample, that has increased from the 2 or 10 minute mean wind speed by 10 kts or more.
Endorse	Wherever the term 'endorse' is used in connection with safety regulation matters this shall be taken to mean acceptance. It is not to be confused with an ANO approval where formal methods have been applied to secure acceptable regulatory confidence in the approval holder
Equipment	A non-specific term used to denote any product (which may be called by a specific name) designed and built to perform a specific function as a self contained unit or to perform a function in conjunction with other units. Units are physical hardware entities, possibly with software and firmware.
Error	A detected event or condition that occurs as a result of a failure state
Error Detection	A process of testing for non valid data, bit error, syntax, and addressing or the event of an error being detected.
Error Rate	A process of testing for non valid data, bit error, syntax, and addressing or the event of an error being detected.



Integrity	That quality which relates to the confidence that can be placed in the validity of the information provided by a system.
Integrity Risk	The probability of an undetected failure, event or occurrence within a given time interval
Intermediate approach	That part of an instrument approach procedure from the first arrival at the first navigational facility or predetermined fix to the beginning of the final approach. (ICAO)
Lines of Communication	A communications link whatever its' function or method of operation. Available lines of communication are those which can be accessed at a particular operating position. Selected lines of communication are those available lines which have been selected by the operator for a mode of operation
Luminance	(L or B, Candela Metre-2) In a given direction at the point on a surface, is the luminous intensity in that direction, of an infinitesimal element of the surface containing the point, by the area of the orthogonal projection of this element on a plane perpendicular to the direction considered
Luminous Flux	(F, Lumen) Quantity relating to a characteristic radiant flux, which expresses its capacity to produce visual sensation, evaluated according to the values of relative luminous efficiency for the light-adapted eye adopted by the CIE. (Commission Internationale De L'Eclairage).
Luminous Intensity	(I, Candela) In a given direction it is the quotient of the luminous flux emitted from a source or from an element of a source containing the point under consideration by the area of this element
May	Optional, alternative, permissive
Maintenance	The preservation or restoration of the required system performance over the system lifecycle
Non-Radar Separation	The separation used when the aircraft position information is derived from sources other than radar. (ICAO)
Obstacle Clearance Limit	The height above aerodrome or threshold elevation for a given final approach direction and instrument approach aid below which the minimum specified vertical clearance above obstacles cannot be maintained either on approach or in the event of a missed approach. (A)
Operational Requirement (OR)	The basic operational need in the aeronautical environment from the air traffic service perspective.
Plan Position Indicator	A cathode ray tube display indicating in plan the positions of objects producing radar echoes
Primary Radar	A radar system that uses reflected radio signals. (ICAO)
Provider (of an air traffic service)	A person, or persons, nominated by an aerodrome or other authority who is competent having regard to the organisation, staffing, equipment maintenance or other arrangements to provide a service which is safe for use by aircraft.
QNH	The pressure to be set on the subscale of an aircraft altimeter that would read the aerodrome elevation if the aircraft were on the ground at that aerodrome. (ICAO Abbreviations and codes DOC 8400/4)
Radar	A radio detection device which provides information on range, azimuth and/or elevation of objects. (ICAO)
Radar Approach	An approach, executed by an aircraft, under the direction of a radar controller. (ICAO)
Radar Blip	A generic term for the visual indication. in non-symbolic form, on a radar display of the position of an aircraft obtained by primary or secondary radar. (ICAO)
Radar Clutter	The visual indication on a radar display of unwanted signals. (ICAO)

Radar Contact	The situation which exists when the radar blip or radar position symbol of a particular aircraft is seen and identified on a radar display. (ICAO)
Radar Control	Term used to indicate that radar-derived information is employed directly in the provision of air traffic control service. (ICAO)
Radar Display	An electronic display of radar derived information depicting the position and movement of aircraft. (ICAO)
Radar Echo	The visual indication on a radar display of a radar signal reflected from an object. (ICAO)
Radar Identification	The process of correlating a particular radar blip or radar position symbol with a specific aircraft. (ICAO)
Radar Map	Information superimposed on a radar display to provide ready indication of selected features. (ICAO)
Radar Monitoring	The use of radar for providing aircraft with information and advice relative to significant deviations from nominal flight path. (ICAO)
Radar Position Symbol	A generic term for the visual indication in a symbolic form on a radar display, of the position of an aircraft obtained after digital computer processing of positional data derived from primary radar, SSR, or both. (ICAO)
Radar Response	The visual indication on a radar display of a radar signal transmitted from an object in reply to an interrogation. Radar Return A generic term meaning variously a radar blip or radar position symbol.
Radar Return	A generic term meaning variously a radar blip or radar position symbol.
Radar Separation	The separation used when aircraft position information is derived from radar sources. (ICAO)
Radar Unit	That element of an air traffic services unit which uses radar equipment to provide one or more services. (ICAO)
Radial	A magnetic bearing extending from a VOR VORTAC/TACAN. (B)
Radiation Shield	A reflective radiation shield housing capable of protecting the internal sensors from direct and reflected solar and terrestrial (long wave) radiation and from precipitation. The shield shall provide adequate ventilation and shall not represent a significant thermal mass.
Reliability	The ability of a system to perform a required function under given conditions for a given time interval.
Reporting Point	A specified geographical location in relation to which the position of an aircraft can be reported. (ICAO)
Requirement	A requirement is an expressed or implied need that is satisfied through appropriate compliance action. A requirement may call for compliance to such standards, codes of practice, or specifications as considered appropriate by the regulator. A requirement may be satisfied by appropriate means actioned by the regulated and as approved by the regulator
Routine Maintenance	Maintenance at regular periodic intervals, identified at the systems design stage of equipments, functions, components etc., which are known to cause or potentially cause degradation to the required system performance
Rule	One of the rules of the ANO.
Runway	A defined rectangular area on a land aerodrome prepared for the landing and take-off run of aircraft along its length

Safety Case	A document which clearly and comprehensively presents sufficient arguments and evidence that a facility, facilities or organisation is/are adequately safe in air traffic service respects
Safety Critical	An item or system the failure of which could lead to, or directly contribute to, the possibility of an accident or serious loss of functionality, integrity, or safety margins will be identified as safety critical
Safety Objective	A safety objective is a planned and considered goal that has been set by a design or project authority. The satisfaction of an objective may be demonstrated by appropriate means to be determined in agreement with the regulator
Safety Policy	A safety policy is a declaration of a general plan of action set by the authority of management
Safety Related	Since the ability to cause a catastrophic incident is often linked to a series of apparently innocuous and seemingly unrelated events all processes are assumed to be safety related. If something or some process is to be excluded from this precept the burden of proof for exclusion lies with the regulated party
Secondary Surveillance Radar	A system of radar using ground interrogators and airborne transponders to determine the position of aircraft in range and azimuth and, when agreed modes and codes are used, height and identity of flight and airframe as well. (A)
Shall (is to, are to, and must)	Means that the requirement or instruction is mandatory
Should	Means that it is strongly advisable that an instruction or action is carried out; it is recommended. It is applied where the more positive 'shall' is unreasonable but nevertheless a provider would need good reason for not complying
Sidetone	A speech signal derived from the transmit path and fed back at a reduced level to the receive path with negligible delay. The level of sidetone approximates to that heard by direct propagation through the air when a person speaks. The absence of sidetone leads to the person speaking too loudly and excessive sidetone leads to the person speaking too softly.
Specification	A specification is a precise technical definition of the required parameters or performance to be achieved
Standard	A standard defines characteristics, methods, principles and practices that can be used to satisfy a requirement. Standards may be international, national or company internal. Standards may be adopted by a regulated organisation in response to a regulatory requirement provided that it is acceptable to the regulator. The regulator may specify a standard to satisfy part or all of a requirement
Station Time Marking	All recorded information requires a time label. The time reference or standard used for this shall be the station clock. This will require the system to be interfaced to the station master clock or station operational procedures put in place to ensure that the system clock is within +5 seconds of the station clock.
Stopway	A defined rectangular area at the end of the take-off run available, prepared and designated as a suitable area in which an aircraft can be stopped in the case of a discontinued take-off
Surface Movement Control Service	An aerodrome control service two way radiotelephony communications facility for the control of vehicles on the MANOEUVRING area
Surveillance Radar	Radar equipment used to determine the position of an aircraft in range and azimuth. (ICAO)
System Failure	The inability of a system to fulfil its operational requirements. Failure may be systematic or due to a physical change.

System Self Test	An automatic test procedure that ensures the system is free from error
Technical Response Time	The time from the issue of a triggering event by the originator user process to the moment a logical system response is received by the originator user process. It therefore includes the technical data extraction, the composition of the data message, the data transmission and processing, the logical checks at the destination, and the transmission and receipt of a response
Terminal Control Area	A control area normally established at the confluence of airways in the vicinity of one or more major aerodromes.
Threshold	The beginning of that portion of the runway useable for landing (ICAO)
Touchdown	The point where the predetermined glide path intercepts the runway
Track	The direction of the path of an aircraft over the ground usually expressed in degrees from north (true magnetic).
Transfer Delay	The time from the issue of a triggering event by the originator user process to the moment the message is received, validated and ready for further treatment at the destination user process. It therefore includes the technical data extraction, the composition of the data message, the data transmission and processing.
Transponder	A receiver/transmitter which will generate a reply signal upon proper interrogation, the interrogation and reply being on different frequencies.
Video Mapping	The electronic superimposing of a map or plan on a radar display.
Visual Approach	An approach by an IFR flight when part or all of an instrument approach procedure is not completed and the approach is executed with visual reference to terrain. (ICAO)
Visibility	The ability, determined by atmospheric conditions and expressed in units of distance, to see and identify prominent unlit objects by day and prominent lighted objects by night. (ICAO) (a) Flight Visibility: The visibility forward from the flight deck of an aircraft in flight (b) Ground Visibility: The horizontal visibility at ground level. (c) RVR: Horizontal visibility along runway.
Visual Meteorological Conditions	Meteorological conditions expressed in terms of visibility, horizontal and vertical distance from cloud. equal to or better than specified minima.
Will	Used for informative and descriptive writing

## **ABBREVIATIONS**

## **UNITS OF MEASUREMENTS**

*Revised 8/12/97*