Safety Regulation Group

Civil Aviation Authority

CAP 760

Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases

www.caa.co.uk

Safety Regulation Group

Civil Aviation Authority

CAP 760

Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases

For Aerodrome Operators and Air Traffic Service Providers

10 December 2010

ISBN 978 0 11792 488 8

First edition 13 January 2006
First edition incorporating amendments to 10 December 2010

Enquiries regarding the content of this publication should be addressed to:
Air Traffic Standards Division, Safety Regulation Group, Civil Aviation Authority, Aviation House, Gatwick Airport South, West Sussex, RH6 0YR.

The latest version of this document is available in electronic format at www.caa.co.uk, where you may also register for e-mail notification of amendments.

Published by TSO (The Stationery Office) on behalf of the UK Civil Aviation Authority.

Printed copy available from:
TSO, PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0844 477 7300
Fax orders: 0870 600 5533
www.tsoshop.co.uk
E-mail: caa@tso.co.uk
Textphone: 0870 240 3701

Amendment Record

Amendment Number	Amendment Date	Incorporated by	Incorporated on
2010/01	10 December 2010	CAA	10 December 2010

Amendment Number	Amendment Date	Incorporated by	Incorporated on

List of Effective Pages

Chapter	Page	Date
	iii	10 December 2010
Contents	1	10 December 2010
Contents	2	10 December 2010
Contents	3	10 December 2010
Revision History	1	10 December 2010
Foreword	1	10 December 2010
Foreword	2	10 December 2010
Introduction	1	10 December 2010
Glossary	1	13 January 2006
Glossary	2	13 January 2006
Glossary	3	13 January 2006
Chapter 1	1	13 January 2006
Chapter 1	2	10 December 2010
Chapter 1	3	13 January 2006
Chapter 1	4	13 January 2006
Chapter 1	5	13 January 2006
Chapter 2	1	13 January 2006
Chapter 2	2	13 January 2006
Chapter 2	3	13 January 2006
Chapter 3	1	13 January 2006
Chapter 3	2	13 January 2006
Chapter 3	3	13 January 2006
Chapter 3	4	13 January 2006
Chapter 3	5	13 January 2006
Chapter 3	6	13 January 2006
Chapter 3	7	13 January 2006
Chapter 3	8	13 January 2006
Chapter 3	9	13 January 2006
Chapter 3	10	13 January 2006
Chapter 3	11	13 January 2006
Chapter 3	12	13 January 2006
Chapter 3	13	13 January 2006
Chapter 3	14	13 January 2006
Chapter 3	15	13 January 2006
Chapter 3	16	13 January 2006
Chapter 3	17	10 December 2010
Chapter 3	18	13 January 2006
Chapter 3	19	13 January 2006
Chapter 3	20	13 January 2006
Appendix A	1	13 January 2006
Appendix A	2	13 January 2006
Appendix A	3	13 January 2006
Appendix A	4	13 January 2006
Appendix A	5	13 January 2006
Appendix A	6	13 January 2006
Appendix B	1	13 January 2006
Appendix B	2	13 January 2006
Appendix B	3	13 January 2006
Appendix B	4	13 January 2006
Appendix B	5	13 January 2006
Appendix B	6	13 January 2006
Appendix B	7	13 January 2006
Appendix C	1	13 January 2006
Appendix C	2	13 January 2006
Appendix C	3	13 January 2006
Appendix C	4	13 January 2006
Appendix C	5	13 January 2006
Appendix C	6	13 January 2006
Appendix C	7	13 January 2006
Appendix D	1	13 January 2006
Appendix D	2	13 January 2006
Appendix D	3	13 January 2006
Appendix D	4	13 January 2006
Appendix D	5	13 January 2006
Appendix D	6	13 January 2006
Appendix E	1	13 January 2006
Appendix E	2	13 January 2006
Appendix E	3	13 January 2006
Appendix E	4	13 January 2006
Appendix E	5	13 January 2006
Appendix F	1	13 January 2006
Appendix F	2	13 January 2006
Appendix F	3	13 January 2006
Appendix G	1	13 January 2006
Appendix G	2	13 January 2006
Appendix G	3	13 January 2006
Appendix G	4	13 January 2006
Appendix G	5	13 January 2006
Appendix G	6	13 January 2006
Appendix G	7	13 January 2006
Appendix G	8	13 January 2006
Appendix G	9	13 January 2006
Appendix G	10	13 January 2006
Appendix G	11	13 January 2006
Appendix G	12	13 January 2006
Appendix G	13	13 January 2006

INTENTIONALLY LEFT BLANK

Contents

Appendix A Hazard Identification using Brainstorming

Appendix B Failure Modes, Effects and Criticality Analysis

Appendix C Hazard and Operability Studies

Appendix D Using Event Trees

Appendix E Diagrammatic Representation of Safety Arguments

Appendix F Hazard Logs

Appendix G Required Level of Confidence in Evidence

INTENTIONALLY LEFT BLANK

Revision History

1st Edition **13 January 2006**

International and European standards have been revised in recent years to require the use of Safety Management Systems and the production of Safety Cases by Air Traffic Management organisations. This first edition of CAP 760 has been produced by the Aerodrome, Air Traffic and Licensing Standards Division of the CAA Safety Regulation Group to assist air traffic service providers and aerodrome operators to develop Safety Cases that meet the relevant international standards thereby enabling them to gain regulatory approval for their services and operations.

1st Edition, Amendment 2010/01 **10 December 2010**

Amended to reflect the change in the regulatory framework brought about by Single European Sky legislation.

INTENTIONALLY LEFT BLANK

Foreword

1 The CAA believes that publishing guidance and acceptable means of compliance, with respect to European Regulations such as EUROCONTROL's Safety Regulatory Requirement number 4 (ESARR 4) and the equivalent Single European Sky (SES) regulation (EC Regulation No 2096/2005 Common Requirements For The Provision Of Air Navigation Services), enhances safety regulation and potentially enhances safety performance, even though there is no requirement for National Supervisory Authorities to do so. In order to fulfil this belief, CAP 760 was published in January 2006 and is an initial guidance document on the conduct of hazard identification, risk assessment, mitigation and the production of safety cases for aerodrome operators and air traffic service providers. However, CAP 760 relates to ESSAR 4, rather than the SES Common Requirements, which were published on 20 December 2005.

2 The SES Common Requirements places responsibilities directly on Air Navigation Service Providers, of which ATS Providers are a sub-set. In particular, they require ATS Providers to conduct risk assessment and mitigation in respect of changes to the ATS system.

3 National Supervisory Authorities, such as the CAA, have a responsibility to oversee ATS Providers with regards to changes to the ATS System but are not ultimately responsible for the adequacy of the risk assessment and mitigation performed by ATS Providers.

4 The CAA has been engaged with various stakeholders, experts and agencies within the UK, the EU and other European States, in refining guidance and identifying acceptable means of compliance to meet the SES Common Requirements in respect of hazard identification, risk assessment, mitigation and the production of safety cases. Recently the European Aviation Safety Agency (EASA) has taken legal competence in the field of ATM and is in the process of adapting the SES regulations to fit within their regulatory framework. This has led to uncertainty over the exact form regulations for the safety assessment of change will take. Consequently, to date, no updates to CAP 760 or related acceptable means of compliance have been produced.

5 In the meantime, the content of CAP 760 broadly addresses subject matter related to risk assessment and mitigation. However, ATS Providers, when using this guidance, must apply caution, as it does not absolve them of their responsibilities to comply with the law as it currently stands e.g. the SES Common Requirements. It is the ATS provider's responsibility to determine the exact requirements of the source legislation and not simply to refer to the guidance in this CAP.

6 If used, this CAP must be related to the risk assessment and mitigation specifics of the current source legislation and users must ensure that the guidance in this CAP is suitably adapted to the particular change. In particular, in the current regulatory circumstances, users must ensure that risk assessment and mitigation is aimed at achieving safety in terms of minimising the likelihood of all accidents that may occur as a result of the change and not to managing a particular hazard's severity and rate. However, if the change does not introduce new hazards, does not increase the rate of already identified hazards and is, for example, a simple one to one change of equipment, then assessment based solely on hazards, may be acceptable.

7 There is, however, a need to carefully consider all changes as, for example, even simple equipment changes may introduce new behaviours that create new hazards or modify the rate of occurrence of existing hazards. In such cases new accidents may be identified or the rate of occurrence of accidents already identified could increase, thus increasing the total accident rate.

8 It should be noted that compliance with other CAPs or prescriptive requirements and processes does not absolve an ATS Provider of responsibilities of meeting current regulations. For example, if a new obstruction on an airfield does not infringe a safeguarding height the ATS Provider still has to ensure that any hazards introduced by the obstruction have been identified and any additional potential for aircraft accidents assessed for acceptability. CAP 738 Safeguarding of Aerodromes does in fact indicate this.

Introduction

1 International regulations and standards[1] require that any change to a system[2] that has an impact on the safety of aerodrome operations or Air Traffic Services (ATS) shall be subject to a risk assessment and mitigation process to support its safe introduction and operation. The result of the assessment should be documented and this is typically achieved by developing a Safety Case. The term 'Safety Case' is used in respect of a set of one or more documents that include claims, arguments and evidence that a system is safe. A Safety Case provides all the documentation and references necessary to demonstrate, both to the operator themselves and to the CAA, that a new system or a change to an existing system is tolerably safe and will meet specified Safety Objectives.

2 This document is a consolidated reference addressing the development of a Safety Case for the purposes of assuring the safety of ATS and aerodrome operations. It should be noted that the concepts associated with a Safety Case are not unique to the aviation environment, and similar requirements may be placed on aerodrome operators and Air Navigation Service Providers (ANSPs) for other purposes by other regulatory bodies (for example by the Health and Safety Executive in relation to the wellbeing of employees and other individuals).

3 This guidance is based on a seven-step safety assessment process defined in 'The Manual of Safety Management for Air Traffic Services' presented at the ICAO 11th Air Navigation Conference (Information Paper No.9). Other approaches may be taken for hazard identification and risk assessment; ultimately, what is important is that the Safety Case presents adequate evidence and argument to demonstrate that the new system or change is tolerably safe.

4 The purpose of this document is to provide guidance to aerodrome operators and ANSPs on the development of a Safety Case and, in particular, on hazard identification, risk assessment and the mitigation techniques that may be used.

5 For conciseness, the terms 'system' and 'project' are used throughout this document and should be considered to include the following constituents:

a) any equipment;

b) any procedure (e.g. operational procedure used by the aerodrome operator or air traffic service provider or, alternatively, a maintenance procedure for related equipment); and

c) the people involved and their organisation.

6 During the life of a system (from design to de-commissioning) there may be several iterations of risk assessment and mitigation and updates to the Safety Case. The Safety Case is, therefore, a 'living document' and should be developed along with the lifecycle of the system. Work on the Safety Case should therefore begin when a project is at its initial concept phase and the content should be added to as the project progresses throughout its lifecycle through to its removal from service.

7 International and nationally recognised standards may be applicable to certain types of systems or equipment. The guidance contained within this document shall not be used in place of any requirements and/or guidance contained in applicable standards. The standards take precedence over the guidance contained within this document.

1. Including ICAO Annex 11 Air Traffic Services, Single European Sky Common Requirements and EUROCONTROL Safety Regulatory Requirements (ESARRs).
2. A change to a system includes the introduction of a new system and the removal of an old system.

INTENTIONALLY LEFT BLANK

Glossary

Term or abbreviation	Meaning
Accident	An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which: a) a person is fatally or seriously injured as a result of: - being in the aircraft; or - direct contact with any part of the aircraft, including parts which have become detached from the aircraft; or - direct exposure to jet blast; except when the injuries are from natural causes, self-inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew; or b) the aircraft sustains damage or structural failure which: - adversely affects the structural strength, performance or flight characteristics of the aircraft; and - would normally require major repair or replacement of the affected component, except for engine failure or damage, when the damage is limited to the engine, its cowlings or accessories; or for damage limited to propellers, wing tips, antennas, tyres, brakes, fairings, small dents or puncture holes in the aircraft skin; or c) the aircraft is missing or is completely inaccessible.
ALARP	**As Low As Reasonably Practical** A risk is low enough that attempting to make it lower, or the cost of assessing the improvement gained in an attempted risk reduction, would actually be more costly than any cost likely to come from the risk itself.
AIS	**Aeronautical Information Service** A service established within a defined area of coverage responsible for the provision of aeronautical information and data necessary for the safety, regulatory, and efficiency of air navigation.
ANSP	**Air Navigation Service Provider** Any provider of: a) Air Traffic Control (ATC) service; b) Flight Information Service (FIS); c) Air Traffic Advisory service; d) Air Traffic Alerting service; e) Aeronautical Information Service (AIS); f) Meteorological service; or g) Communications, Navigation or Surveillance (CNS) services.
ATC	**Air Traffic Control** A service provided for the purpose of preventing collisions between aircraft or between aircraft and obstructions (in the manoeuvring area) and for the purpose of expediting and maintaining an orderly flow of air traffic.
Applicable safety regulatory requirements	The requirements for the provision of aerodrome and air traffic services or facilities, applicable to the specific situation under consideration, concerning, inter alia: a) technical and operational competence and suitability to provide the service or facility; b) systems and processes for safety management; c) technical systems, their constituents and associated procedures.

Term or abbreviation	Meaning
ATS	**Air Traffic Services** The provision of air traffic control, flight information and/or air-ground communications services.
CAE	**Claim Argument Evidence** A graphical method to represent claims, arguments and evidence.
Derived safety requirements	Those Safety Requirements that have been generated by undertaking a hazard identification and risk assessment process (as described in this guidance) on the components of the system.
DRACAS	**Defect Reporting And Corrective Action System** A formal procedure for recording all system defects, analysing them and taking corrective action as necessary.
ESARR	**EUROCONTROL Safety Regulatory Requirement** Material published by EUROCONTROL for adoption by member states, containing safety requirements covering a range of topics.
FIS	**Flight Information Service** Non-radar service for the purpose of providing information useful for the safe and efficient conduct of flights e.g. information concerning weather, serviceability of facilities, conditions at aerodromes, etc.
FISO	**Flight Information Service Officer** Person qualified to provide a discrete FIS (i.e. not in association with an air traffic control service).
FMECA	**Failure Modes Effects and Criticality Analysis** A systematic hazard identification and assessment methodology that sequentially identifies the impact of a range of component failure scenarios on the system function.
GSN	**Goal Structured Notation** A graphical method to represent claims, arguments and evidence.
Hazard	Any condition, event, or circumstance which could induce an accident.
HAZOP	**Hazard and Operability study** A systematic functional hazard identification process that uses an expert group to conduct a structured analysis of a system using a series of guide words to explore potential hazards.
Incident	An occurrence, other than an accident, associated with the operation of an aircraft which affects, or would affect, the safety of operation.
MOR	**Mandatory Occurrence Reporting** Formal scheme for the national recording and reporting of safety-significant incidents.
RFFS	**Rescue and Fire Fighting Service**
Risk	A combination of the likelihood of an hazard occurring and the severity of the accident that could result; e.g. the higher the risk, the more likely the accident will occur and/or the more severe will be the consequence.
Risk assessment	A process that for identified hazards, evaluates their risk in terms of probability and severity of consequences.
Safety barriers	Term used to indicate systems, sub-systems or methods used to reduce the likelihood of a hazard escalating into an incident or accident, and/or reduce their severity.
Safety assessment criteria	The set of quantitative or qualitative criteria to be used in a safety assessment to determine the acceptability of the assessed level of safety.

Term or abbreviation	Meaning
Safety case	A documented body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application and environment over its lifetime.
Safety case report	A report that summarises the arguments and evidence of the Safety Case.
Safety objective	The definition of a hazard together with its target maximum rate of occurrence. A goal or target that, where achieved, demonstrates that a tolerable level of safety is being, or will be achieved for the hazard concerned.
Safety requirement	Specified criteria of a system that are necessary in order to reduce the risk of an accident or incident to an acceptable level. Also a requirement that helps achieve a Safety Objective.
Serious incident	An incident involving circumstances that indicate that an accident nearly occurred. Typical examples include: - A near collision requiring an avoidance manoeuvre, or when an avoiding manoeuvre would have been appropriate to avoid a collision or an unsafe situation. - Controlled flight into terrain (CFIT) only marginally avoided. - An aborted take-off on a closed or engaged runway, or a take-off from such runway with marginal separation from obstacle(s). - A landing or attempted landing on a closed or engaged runway. - Gross failure to achieve predicted performance during take-off or initial climb. - All fires and smoke in the passenger compartment or in cargo compartments, or engine fires, even though such fires are extinguished with extinguishing agents. - Any events which required the emergency use of oxygen by the flight crew. - Aircraft structural failure or engine disintegration which is not classified as an accident. - Multiple malfunctions of one or more aircraft systems that seriously affect the operation of the aircraft. - Any case of flight crew incapacitation in flight. - Any fuel state which would require the declaration of an emergency by the pilot. - Take-off or landing incidents, such as undershooting, overrunning or running off the side of runways. - System failures, weather phenomena, operation outside the approved flight envelope or other occurrences which could have caused difficulties controlling the aircraft. - Failure of more than one system in a redundancy system which is mandatory for flight guidance and navigation.
Statutory safety requirements	Those Safety Requirements applicable to a system that have been specified in Standards or by the CAA.
System	Used to describe the collection of equipment, procedures and/or personnel required to carry out a function.
TLS	**Target Level of Safety** A safety objective defined as a tolerable accident rate in terms of probability of an accident given a certain quantity of activity.
VCRI	**Verification Cross Reference Index** A record detailing the system requirements against the location of the evidence where the requirement is proven to be met or how it is planned to prove the requirement.

INTENTIONALLY LEFT BLANK

Chapter 1 System Lifecycle

1 Introduction

1.1 Aerodrome and ATS projects commonly pass through a variety of phases during their life from initial concept through to decommissioning. Safety needs to be planned for and addressed in all of these phases although the depth of risk assessment will vary depending upon the stage of the project and the degree of risk that exists. Performing risk assessment early in the project can identify hazards that impact on the design of the system. It is better that these hazards and their impact are identified early in a project so that the system can be designed to take account of them, rather than incurring expense trying to change a design or retrospectively to generate safety assurance evidence later in a project. Also failure to update earlier safety analyses with information that subsequently becomes available in later project phases may invalidate the earlier analyses.

2 Planning for Safety

2.1 Planning for safety is as important a part of a project as planning for operational use. Consideration should be given to developing a Safety Plan for a project detailing:

a) the scope of the project or system that is being considered (consider equipment, procedures and people aspects);

b) the safety activities planned to be carried in the different project phases (see the sections below);

c) when or at what stage in the project the safety activities will be carried out;

d) the staff responsible for contributing to the safety activities; and

e) the authority of staff e.g. having the authority to approve safety documentation or having the authority to accept unresolved risks on behalf of the organisation etc.

2.2 Not only can a Safety Plan be used to enable the project to be completed efficiently and without unexpected or unnecessary cost but it can also form a part of the argument in the Safety Case that safety has been adequately managed.

2.3 Early in the planning stage of a project, there may be some benefit in producing an outline of how it is intended to argue the safety of the system e.g. identifying the sort of safety assurance evidence that may be required. This outline can help to identify activities that need to be scheduled in the overall safety plan.

2.4 What follows is an outline of the typical phases of a project that should be planned for. It should be noted, however, that each project is different and you may find that different, fewer or additional phases are more suited to a particular project.

3 Feasibility and Concept - Safety Activities Early in a Project

3.1 The feasibility and concept phase occurs early in a typical project where the project is a developing set of ideas and options but has no detail. Typically a concept of operation or an early draft of operational requirements may be developed. Performing a high-level hazard identification and risk assessment early in the project can identify hazards that impact on the design of the system. It is better that these hazards and their impact are identified early in a project, and suitable measures are taken at that

stage, rather than incurring possible expense or delay having to change a design or provide further safety assurance evidence where the hazards were missed and discovered later.

3.2 Early in the project it is beneficial to identify the Applicable Safety Regulatory Requirements, including National and International Standards and Recommended Practices, local Regulations and guidance material applicable to the intended system. These will influence the design of the system and compliance to these standards and regulations will often mitigate hazards inherent to the project. For example, for Air Traffic Service systems the following may be applicable:

a) ICAO Standards and recommended Practices, e.g. ICAO Annex 10 and Annex 11.

b) Single European Sky Interoperability Rules and Common Requirements.

c) European Standards e.g. Eurocae MOPS (Minimum Operational Performance Specifications); Eurocontrol ESARRS (European Safety Regulatory Requirements).

d) CAA CAPs e.g. CAP 670 Air Traffic Services Safety Requirements.

3.2.1 For aerodrome projects, the following may be applicable:

a) ICAO SARPs e.g. ICAO Annex 14.

b) European Standards, e.g. EUROCONTROL ESARRs.

c) CAP 168 Licensing of Aerodromes.

d) CAP 232 Aerodrome Survey Information.

e) CAP 642 Airside Safety Management.

f) CAP 683 The Assessment of Runway Surface Characteristics.

g) CAP 699 Standards for the Competence of Rescue and Fire Fighting Service (RFFS) Personnel Employed at United Kingdom Licensed Aerodromes.

h) CAP 748 Aircraft Fuelling and Fuel Installation Management.

4 Design and Development

4.1 As a project changes from a concept to a reality, more detailed system design is undertaken and more knowledge of the system and its operational requirement is gained. Performing risk assessment partway through a design phase, building on previous assessments, can help designers focus on the riskiest parts of the system, identifying and implementing mitigations as necessary e.g. equipment back-ups, alternative procedures, increased training, a higher level of software development scrutiny etc. It is not possible to be specific about when a risk assessment should be conducted during system design because this will depend on the size, complexity and speed of development of the project.

4.2 Applicable Safety Regulatory Requirements pertinent to the design must be considered as the system is developed. The generation of compliance matrices against the standards can help ensure that every requirement is satisfactorily addressed. Very often it may not be possible for the ANSP or aerodrome operator to demonstrate compliance with the standards without the assistance of an equipment supplier or developer. This is particularly likely where the standard imparts a requirement covering the processes to be followed when developing the system e.g. as in the case of a software development standard. In such cases the ANSP or aerodrome operator must review the evidence provided to them from their subcontractor or supplier to satisfy themselves that the relevant requirements have been met.

5 Tender and Contract

5.1 Often a project will involve an external company supplying equipment or services under contract. When devising the contract it is important to include those safety aspects that need to be addressed by the supplier. These aspects may include:

a) evidence of good system development practice;

b) evidence of compliance to applicable standards;

c) specific system test requirements required as evidence that safety requirements have been met;

d) conduct of hazard identification;

e) the use of a Hazard Log; and

f) training of operators and maintainers.

5.2 Clearly it is important to identify what safety aspects need to be included in the contract prior to placing the contract. It is important therefore to conduct a risk assessment of the proposed system prior to placing the contract to identify any safety requirements that must be achieved and the types and level of evidence that the system supplier will be expected to provide in order to demonstrate that the requirements have been achieved.

5.3 For some contracts, it may be appropriate to include the conduct of periodic safety reviews or a clause that enables the ANSP or aerodrome operator to withdraw from the contract without penalty if the relevant safety standards are not maintained.

6 System Realisation

6.1 During the realisation of the system, the items listed under 'Tender and Contract' above will be further developed.

6.2 Typically during the realisation of a system, there will be changes to the original design intent as unexpected problems arise and methods are devised to deal with the them. Care must be taken to not only consider the effects of these changes on the functionality of the system, but to consider the safety impact of these changes. The use of a 'change control system', e.g. a formal method of notifying, considering and authorising the changes, will ensure that changes are given due consideration. The review and confirmation of the safety impact should form part of this change control system and may require additional risk assessment and mitigation activity to ensure that any new hazards are identified and assessed (and also to remove any that are no longer applicable).

7 Transition to Service

7.1 Before putting a system into service an acceptable safety case for the system should be in place. This safety case, ideally developed in accordance with the 7-step procedure detailed within this guidance, will identify the safety requirements and present the evidence that these safety requirements have been met along with any shortcomings. Evidence typically required for the transition into service phase may include:

a) Site Acceptance Test (SAT) results;

b) systems integrations test results; and

c) operational trial results.

7.2 It may be necessary to contact the CAA for Approval of the system prior to putting it into service. Also Single European Sky (SES) requirements are being developed that may require additional regulatory action in respect of the system prior to it being put into service. Contact your CAA Inspector for guidance regarding what regulatory action may be required.

7.3 Part of the risk assessment process should examine the impact of the introduction of the new system or variations on existing systems and services. For example, there may need to be a break in the service during the changeover from one system to another; the overall system needs to be able to tolerate this break. There may also be interfaces to other systems within the aerodrome and ATS environment; these interfaces must be assessed both to ensure that the change or new system can be accommodated safely and that there are no impacts on existing systems by the project under consideration. Approval for a break to an existing service may also need to be sought from the CAA.

7.4 The assessment may have identified the provision of reversionary procedures as mitigation should the new system cause initial problems.

8 On-going Operation and Maintenance

8.1 Part of the risk assessment of the system should look at the risks associated with operating and maintaining the system. Typically this will identify safety requirements to ensure that operators and maintainers are appropriately trained and that procedures covering operation and maintenance are produced and used. This should be planned for early in the project especially where training is required to be provided by equipment suppliers.

8.2 As part of a Safety Management System (SMS) operators are required to ensure that operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken (required by ESARR3). Consideration should be given to developing a defect reporting and corrective action system (sometimes known as DRACAS) in order to log and react appropriately to any defects or failures of the system. Records of such faults may be used to help identify persistent areas of failure or trends that may lead to more serious failures. Analysis of the records may identify new hazards that need to be addressed in the safety case, or a failure to meet safety requirements or objectives, which will require mitigation.

8.3 Schemes for recording safety significant events, such as the CAA Mandatory Occurrence Reporting (MOR) scheme[1], should not only be used for the recording of incidents, but should be used to trigger analysis of what caused the incident and what needs to be done to prevent it reoccurring.

8.4 Auditing of procedures to ensure operators and maintainers are properly applying the procedures is another way to provide evidence that safety requirements to do with their application are being met. The written reports of this auditing process can be used as evidence in the safety case. Similarly, audits may be conducted of suppliers to ensure that the supplied services are of a satisfactory standard.

8.5 Periodically revisiting the safety case of a system should be planned for. If a system has been in service for a long period of time, any assumptions about the environment or the conditions that the system is operated under may change e.g. the numbers of aircraft using the aerodrome may increase over time; are the safety requirements still valid and can the systems cope?

1. Or other scheme compliant with the requirements of EUROCONTROL ESARR2 Reporting and Assessment of Safety Occurrences.

8.6 Some assumptions and requirements specified in the safety case may only be able to be fully substantiated after a period of operation of the system. The verification of these should be addressed after an appropriate period of time. In the interim period, it may be necessary to apply additional mitigations until such time as it can be shown that the requirement is satisfied.

9 Changes

9.1 There can be many reasons to make changes to an existing system, for example:

a) to correct defects;

b) to replace or update ageing equipment;

c) to increase functionality;

d) to modify procedures e.g. where there are efficiencies to be gained;

e) where staff changes reduce the level of experience or expertise.

9.2 A change to a system can be considered as a small project, with the lifecycle phases described above being applicable to a variable extent depending on the size of the change. As in the System Realisation section above, the use of a change control system will ensure that changes are given due consideration and include assessing the safety impact of the change.

9.3 The guidance above, covering 'transition to service', may be applicable for the change i.e. the safety case for the system may need updating and approval by the CAA prior to the change being put into service. Contact your CAA Inspector for guidance on whether this is the case.

10 Removing the System from Service/Decommissioning

10.1 Where a decision has been made to remove a system from service, a risk assessment of the impact of removing the system should be conducted. Where the system is being replaced by another system, then this aspect may be covered by the risk assessment associated with putting the new system into service. When a system is being removed but not being replaced, the impact on other systems to which this one relates should be assessed.

10.2 There may also be hazards specifically related to decommissioning the system, for example, disruption to control rooms or interference to manoeuvring area operations, which need to be considered.

10.3 The impacts of decommissioning should be documented in the safety case and the safety case closed and filed for future reference.

INTENTIONALLY LEFT BLANK

Chapter 2 Risk Assessment and Mitigation - Introducing the Seven-Step Process

1 Introduction

1.1 Risk assessment and mitigation is a structured and systematic process for the identification of hazards and the assessment of the risk associated with each hazard, or group of hazards. The acceptability of the risks is determined by comparing the assessed level of risk to the predetermined safety assessment criteria[1] or Safety Objectives.

1.2 ICAO Annex 11 Air Traffic Services (paragraph 2.26.5) requires that any significant safety-related change to the ATC system shall only be implemented after a safety assessment has demonstrated that an acceptable level of safety will be maintained. Therefore, any new system or any change to an existing system should be assessed through a structured risk assessment and mitigation process.

1.3 ICAO Annex 14 Aerodromes (paragraph 1.4) places a similar requirement on licensed aerodromes.

1.4 ICAO published an Information Paper (No.9) for the ICAO 11th Air Navigation Conference containing a draft of 'The Manual on Safety Management for Air Traffic Services'. This was subsequently updated and published as ICAO Doc. 9859. Within this manual is a safety assessment process defined by a seven-step process. The guidance contained here is based upon that process.

2 When Risk Assessment and Mitigation is Required

2.1 Although it is not possible to produce an exhaustive list detailing every circumstance requiring risk assessment the following are some typical examples where such an assessment would be required:

a) Implementation of new, or changes to, communications, surveillance or other safety-significant systems and equipment, including those providing new functionality and/or capabilities.

b) Physical changes to the layout of runways and/or taxiways at an aerodrome.

c) Physical changes to apron road schemes.

d) Introduction of a new aircraft type or class to an aerodrome.

e) Development or modifications of aerodrome procedures, including new procedures to operate at the aerodrome premises, changes to fire and rescue procedures etc.

f) Changes/Establishment of training or re-training of operational and technical staff.

g) A change to separation minimum to be applied within an airspace or at an aerodrome.

h) New operating procedures, including departure and arrival procedures, to be applied within an airspace or at an aerodrome.

1. A tolerability table is reproduced in Step 5 of this guidance, however users should generate their own assessment criteria, but this must be justified.

i) A reorganisation of the ATS route structure.

j) A resectorisation of the airspace.

k) Introduction of a new Safety Management System (SMS) for an organisation, where the SMS requires Risk Assessment of the systems that it covers.

2.2 Confidence in safety is required before any changes to a system are put into service; the risk assessment and mitigation process should therefore start early in the lifecycle of a new system. For a large and complex project, there will be several phases of Risk Assessment and mitigation, each becoming more detailed as the design and development of the system progresses. The final pre-implementation Risk Assessment then forms the basis for the periodic safety reviews of the operational system, which should continue throughout its lifecycle until decomissioning. See the previous chapter for more information on a project lifecycle.

3 Summary of the Seven Steps

3.1 Risk assessment and mitigation requires a systematic approach. The complete process can be divided into seven steps. These are:

Step 1 - System description.

Step 2 - Hazard and consequence identification.

Step 3 - Estimation of the severity of the consequences of the hazard occurring.

Step 4 - Estimation/assessment of the likelihood of the hazard consequences occurring.

Step 5 - Evaluation of the risk.

Step 6 - Risk mitigation and safety requirements.

Step 7 - Claims, arguments and evidence that the safety requirements have been met and documenting this in a safety case.

3.2 Figure 1 illustrates the risk assessment and mitigation process. The process is iterative and there may be a need to perform a number of cycles throughout the project lifecycle in order to assess proposed risk mitigation measures for their effectiveness and impact.

3.3 The following Chapter will examine each of the seven steps in more detail.

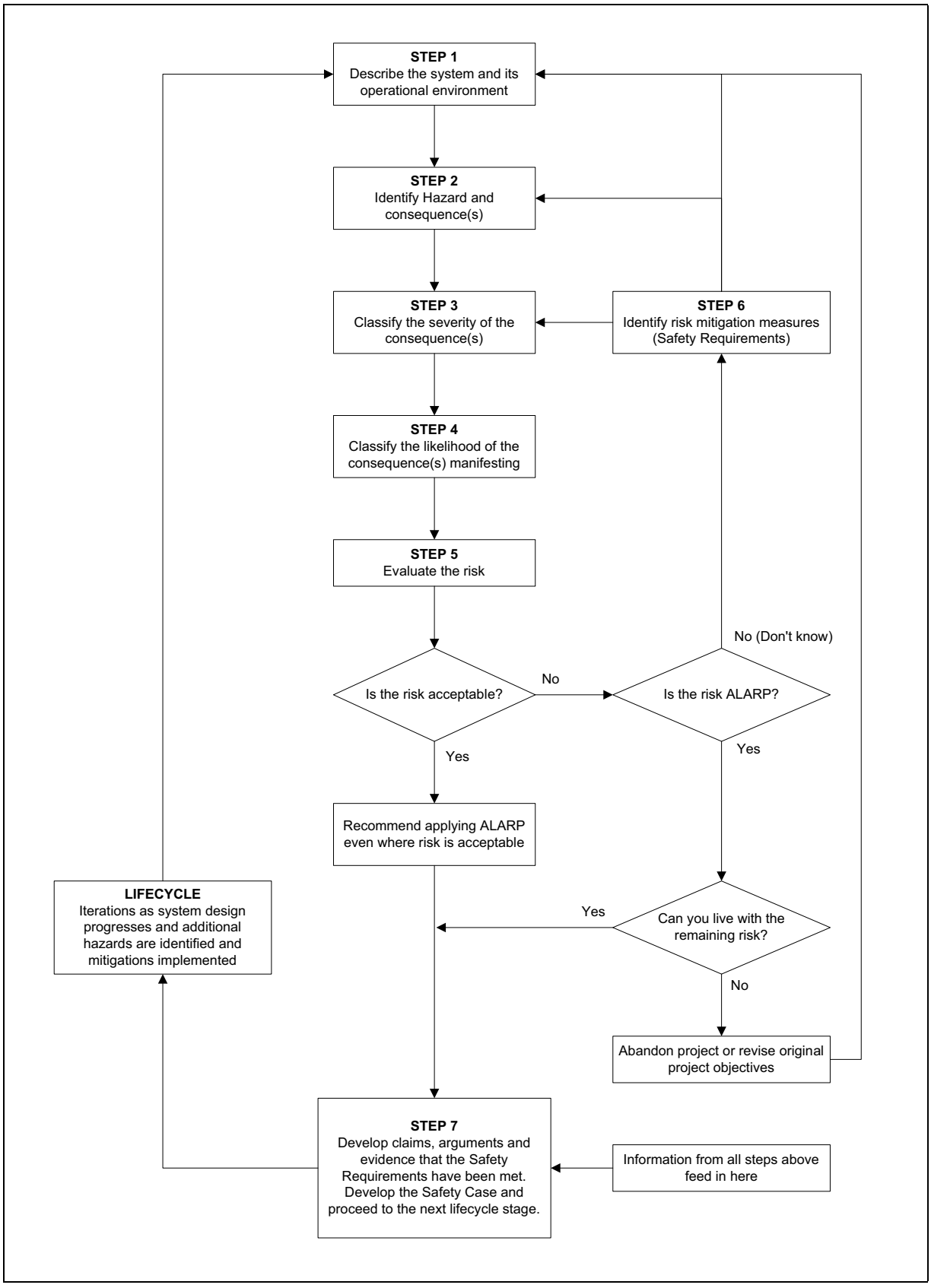

Figure 1 The Seven-Step Approach

INTENTIONALLY LEFT BLANK

Chapter 3 The Seven-Step Risk Assessment and Mitigation Process

1 Step 1 - System Description

1.1 The key activities in Step 1 are to describe:

a) the system/change;

b) the purpose of the system;

c) how the system will be used (concept of operation);

d) the system functions (operational requirements);

e) the boundaries of the system; and

f) the environment including the interface with any larger system.

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

NOTE: The system description and subsequent risk assessment process may be limited to the description of a concept in the early stages of a project (see Chapter 1, System Lifecycle).

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

1.4 A detailed description of the system should include:

a) the purpose of the system;

b) how the system will be used (this may be described as a concept of operation);

c) a description of system functions (this may be achieved, in part, by describing the operational requirements of the system);

d) the system boundaries and the external interfaces;

e) other systems that may be influenced by, or influence this one; and

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

NOTE: To aid readability, long technical descriptions of how individual equipments work should be avoided. Reference to technical documents may be made instead.

1.5 The safety impact of a potential loss, degradation or failure of the system will be determined, in part, by the characteristics of the operational environment in which the system will be integrated. The description of the environment should therefore include any factors that could have a significant effect on safety. These factors will vary from one case to another. They could include, for example:

a) traffic characteristics;

b) aerodrome infrastructure;

c) reliance on space based systems e.g. Communications satellites and Global Navigation Satellite Systems;

d) bird hazard;

e) movement area;

f) hours of operations (day/night);

g) weather, e.g. prevalence of crosswinds or windshear, or duration of Low Visibility Operations;

h) frequency of diversions due to severe weather.

1.6 The description of the system should include any assumptions about interfaces or other systems with which this system interacts. Justification for the assumptions should be included where possible.

1.7 The description of the system should also address pre-existing contingency procedures and other non-normal operations, for example during:

a) failure of ATS equipment;

b) depletion of the Rescue and Fire Fighting Service (RFFS);

c) reduction of the declared distances.

1.8 For many projects it will be appropriate for the system description to address the strategy for transition from the old to the new system. For example, will the existing system be decommissioned and replaced immediately with the new system, or will the two systems be operated in parallel for a period of time?

1.9 There may be several updates to the System Description throughout the Lifecycle of the project. It is important to keep the System Description up to date as design decisions are made and implemented. Without this, there is a risk that Hazard Identification sessions, that may take place at several stages in the life of a project, may not be considering the latest system design.

1.10 The system description will often be best presented using a combination of text and diagrams. The use of diagrams can be an effective means of conveying information, for example:

a) use of flow diagrams to show a system process or the sequence of activities required by a procedure;

b) use of drawings to show the aerodrome layout including taxiways, runway crossing points, RFFS location, fuel stores, ATS equipment location etc.;

c) use of drawings or diagrams showing airspace arrangements including sectors, standard departure and arrivals routes, missed approach routes, radar vectoring area etc.;

d) use of block diagrams to show interactions between system components and the flow of information and data.

2 Step 2 - Hazard and Consequence Identification

2.1 The key activities in Step 2 are:

a) create a hazard log;

b) identify the hazards;

c) identify the consequences of each hazard; and then

d) update the hazard log.

2.2 Hazard Log

2.2.1 A Hazard Log is a formal method used to document hazards identified for a system. The Hazard Log consists of a series of forms where details of each hazard can be recorded. Details of the risks associated with each hazard together with any mitigation measures should also be entered on the forms when the information becomes available. Appendix F shows an example structure of a Hazard Log form.

2.3 When To Perform Hazard Identification

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

2.4 Sources of Hazards

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

a) the equipment (hardware and software);

b) the operating environment (including physical conditions, airspace and air route design, runway hot spots[1] and obstacles);

c) the human operators (pilots, air traffic controllers, maintenance engineers);

d) the human machine interface (HMI);

e) operational procedures;

f) maintenance procedures;

g) external services e.g. electricity, telephone lines;

h) contracted services.

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

2.4.3 Non-standard aerodrome operating configurations should also be considered, if appropriate, for example during Low Visibility Operations or whilst there is 'Work in Progress'.

2.5 Hazard Identification Methods

2.5.1 Hazard identification methods break down into the following 3 generic approaches:

a) **Historical** - Use and analysis of existing hazard logs and accident/incident reports (this may be required as part of a safety management system). Also any hazards identified from other risk assessment processes on other systems that may be similar to this system (for example, has a similar system gained significant in-service history in a comparable mode of operation?);

1. A 'Hot Spot' is the generic term applying to known runway incursion risk location.

b) **Brainstorming** - Planned and organised sessions aimed at encouraging a team of participants of various relevant experience and expertise to explore the system for potential hazards in a creative way. Appendix A gives guidance on a brainstorming process;

c) **Systematic** - Sessions involving a thorough sequential review of a system often using system diagrams and descriptions as prompts together with keywords to help focus the on the types of failures to be assessed. Systematic hazard identification processes include:

- Failure Modes Effects and Criticality Analysis (FMECA) - Appendix B gives guidance on running a FMECA.
- Hazard and Operability Analysis (HAZOP) - Appendix C gives guidance on running a HAZOP process.

NOTE: For maximum effectiveness the Historical and Brainstorming approaches should be used in conjunction with the Systematic processes. The output of the historical analysis can be fed into the Systematic and Brainstorm analysis processes to trigger further exploration of any identified hazards in the new context.

2.5.2 Some of the more complicated hazards identified using the above processes, especially those involving sequences of events, may benefit from further examination using Event Trees. These can be used to explore the range of consequences and available barriers for a particular hazard. Appendix D gives further guidance on how to use Event Trees.

2.5.3 For effective Hazard Identification it is important that the appropriate staff and system experts become involved in the hazard identification processes. Typical of the people who may become involved are:

a) air traffic controllers;

b) pilots;

c) maintenance and design engineers;

d) specialist aerodrome staff such as RFFS staff, security staff and refuelling staff.

NOTE: For efficiency, the staff involved with the Hazard Identification processes above may include the assessment of severity and likelihood (Steps 3 and 4) in the same sessions following the hazard identification process.

2.6 Ad Hoc Hazard Logging

2.6.1 An effective Safety Management System (SMS) should ensure that all staff are encouraged to seek out and report safety issues and potential hazards as part of normal day-to-day working. Relevant hazards identified in this way should be captured within the Hazard Log.

2.6.2 For effective ad-hoc hazard capture, the methods for reporting the hazards should be clearly defined i.e. procedures should be in place that identify how to log a hazard and to whom hazards should be reported.

NOTE: A culture should be developed within the organisation to encourage the reporting of hazards.

2.7 Hazard Consequences

2.7.1 The consequences of the hazard are determined by analysing what could happen if the hazard manifested itself into an accident or incident. Some consequences may be obvious, with there being only one possible outcome as the result of a particular hazard. However other hazards may result in a range of consequences of varying

severity. Using Event Tree analysis (see Appendix D) can help determine the range of consequences. The extent[1] of the effects on the following should be considered:

a) air crew (workload, ability to perform functions);

b) air traffic controllers (workload, ability to perform functions);

c) the functional capabilities of the aircraft;

d) the functional capabilities of the ATS ground systems;

e) the ability to provide safe air traffic management services (e.g. the magnitude of the loss or corruptions of air traffic management services or functions).

f) aerodrome operational staff (workload, ability to perform functions);

g) aerodrome operational procedures (they might be corrupted).

2.7.2 Once all the hazards have been identified they must be entered into the Hazard Log together with their potential consequences.

2.8 Recording the Results of Hazard Identification

2.8.1 All identified hazards should be assigned a hazard number, and recorded in a Hazard Log.

2.8.2 The Hazard Log should eventually contain a description of each hazard, its consequences, the assessed likelihood and severity (steps 3 and 4), and any required mitigation measures (step 6).

2.8.3 Additional Hazard Log entries will need to be made where there is more than one credible consequence of concern.

NOTE: It is not always the most severe consequence that is the highest risk. This is because the most severe consequence may be very unlikely to occur, whilst less severe, yet undesirable consequences may be more likely to occur. It should be remembered that 'risk' is a combination of severity and probability.

2.8.4 The Hazard Log should be updated as new hazards are identified and proposals for mitigation are introduced throughout the project lifecycle.

2.8.5 The hazards recorded in the Hazard Log should be used to feed into the later risk assessment steps of this procedure.

3 Step 3 - Estimation of the Severity of the Hazard Consequences

3.1 The key activities in Step 3 are:

a) assess the severity of each consequence; and

b) record results in the Hazard Log.

3.2 Prior to the commencement of this step, the consequences of each hazard identified in Step 2 should have been recorded in the hazard log. Step 3 involves the assessment of the severity of each of these consequences.

3.3 The same group that performed the hazard identification may assess the severity of the consequences.

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

1. Consider the quantity of aircraft, pilots and air traffic controllers affected and the geographical extent of the problem.

3.5 Table 1 contains a Severity Classification Scheme that may be used. The severity classification for all credible consequences of a hazard should be determined from the table. If an alternative scheme is used it should be clearly defined.

3.6 Once the assessment of severity has been completed for all the identified hazards and consequences, the results, including the rationale for the severity classification chosen, should be recorded in the Hazard Log.

Table 1 Example Severity Classification Scheme

Accidents	Accident - as defined in Council directive 94/56/EC[1] for air traffic services. Also includes loss of or substantial damage to major aerodrome facilities. Serious injury or death of multiple staff/ members of public at the aerodrome.
Serious Incidents	Serious Incident - as defined in Council directive 94/56/EC[1] for air traffic services. For the aerodrome, an event where an accident nearly occurs. No safety barriers remaining. The outcome is not under control and could very likely lead to an accident. Damage to major aerodrome facilities. Serious injury to staff/members of public at the aerodrome.
Major Incidents	A major incident associated with the operation of an aircraft, in which safety of aircraft may have been compromised, having led to a near collision between aircraft, with ground or obstacles. A large reduction in safety margins. The outcome is controllable by use of existing emergency or non-normal procedures and/or emergency equipment. The safety barriers are very few approaching none. Minor injury to occupants of the aircraft or staff/members of public at the aerodrome. Minor damage to aircraft or major aerodrome facilities may occur.
Significant Incidents	Significant incident involving circumstances indicating that an accident, a serious or major incident could have occurred, if the risk had not been managed within safety margins, or if another aircraft had been in the vicinity. A significant reduction in safety margins but several safety barriers remain to prevent an accident. Reduced ability of the flight crew or air traffic control to cope with the increase in workload as a result of the conditions impairing their efficiency. Only on rare occasions can the occurrence develop into an accident. Nuisance to occupants of the aircraft or staff/members of public at the aerodrome.
No Effect Immediately	No immediate effect on safety No direct or low safety impact. Existing safety barriers come into play to avoid the event turning into a significant incident or accident.

1. As defined in Council directive 94/56/EC of 21 November 1994 establishing the fundamental principles governing the investigation of civil aviation accidents and incidents, OJ L 319 of 12 December 1994, p. 14-19. See the Glossary for definitions of Accident and Serious Incident taken from the Council directive reference. Major Aerodrome Facilities may include: Aerodrome buildings and hangars, fuel installations, air traffic service equipment installations, the runway and lighting system, principle taxiways, rescue service vehicles, service vehicles etc.

4 Step 4 - Estimation/Assessment of the Likelihood of the Hazard Consequences Occurring

4.1 The key activities in Step 4 are:

a) estimate the likelihood of hazard consequences occurring; and

b) record the details in the Hazard Log.

4.2 The estimation of the likelihood of the consequences of a hazard occurring uses a similar approach to that adopted in Steps 2 and 3; that is, by means of structured discussions using a standard likelihood classification scheme as a guide. Table 2 shows an example of a classification scheme for this purpose.

4.3 Table 2 specifies the likelihood as qualitative categories e.g. 'remote', 'frequent' etc. but also includes numerical values for the probabilities associated with each category. In some cases, data may be available which will allow direct numerical estimates of the likelihood of failure to be made. For example, for the hardware elements of a system, data is often available on historical component failure rates. Evidence gained from in-service experience of failure rates of existing similar systems may also give an indication of the likelihood of failure.

4.4 The estimation of the likelihood of occurrence of incidents associated with human error will generally involve a greater degree of subjective assessment (and it should be borne in mind that even when assessing hardware, there is always the possibility of failures due to human error such as incorrect maintenance procedures).

4.5 Early in the project lifecycle there may not be much information on which to base an estimate or assessment. However, the use of structured group discussions with participants who have extensive experience in their respective fields, and the adoption of a standard likelihood classification scheme, should ensure that the outcome will be an informed judgement.

4.6 Later on in the project lifecycle, for example after this 7-step procedure has been run through more than once, evidence will start to be amassed that can be used to improve the credibility of the likelihood assessment. This evidence will be needed later in step 7 to help build the argument that the Safety Objectives (i.e. the objective to ensure that all hazards are tolerable) have been met.

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

NOTE: An alternative to estimating the probability of an accident/incident occurring at this stage in the process is to establish the tolerable probability of an accident/incident occurring for a hazard. This would then become a Safety Objective that could be passed on to the system designers in order for them to have a safety target to design to. Setting the Safety Objectives involves using Table 3 in Step 5 to identify the maximum acceptable probability for a particular hazard consequence severity taking the accumulation of hazards that lead to the same consequence severity into account.

Table 2 Probability or Likelihood Classifications

	Probability of Occurrence Definitions				
	Extremely improbable	**Extremely remote**	**Remote**	**Reasonably probable**	**Frequent**
Qualitative definition	Should virtually never occur	Very unlikely to occur	Unlikely to occur during the total operational life of the system	May occur once during total operational life of the system	May occur several times during operational life
Quantitative numerical definition	$< 10^{-9}$ per hour	10^{-7} to 10^{-9} per hour	10^{-5} to 10^{-7} per hour	10^{-3} to 10^{-5} per hour	1 to 10^{-3} per hour
Quantitative annual/daily equivalent (approximate)	Never	Once in 1000 years to once in 100,000 years	Once in 10 years to once in 1000 years	Once per 40 days to once in 10 years	Once per hour to once in 40 days

5 Step 5 - Evaluation of the Risk

5.1 The key activities in Step 5 are:

a) decide whether the risk is acceptable or not; and

b) record the details in Hazard Log.

5.2 The acceptability of a risk is dependent on both the likelihood of it occurring and the severity of its consequences. Acceptability is therefore usually based on comparison with a severity/probability matrix, sometimes called a Tolerability Matrix. It is therefore necessary to generate a Tolerability Matrix in order to set and evaluate the Risk.

5.3 An example Risk Classification/Tolerability Matrix is shown in Table 3[1]. The Safety Objective is to ensure that all risks associated with hazards fall in the 'Acceptable' cells of the matrix.

5.4 Air Traffic Service Providers and Aerodrome Operators may devise their own Risk Tolerability Matrix, however justification for the figures used in the matrix must be provided to the CAA.

1. The Safety Objective for the tolerable level of accidents in European Controlled Airspace has been set in ESARR4 as 1.55×10^{-8} accidents per flight hour (or 2.31×10^{-8} per flight). Table 3 is loosely based on this.

Table 3 Risk Classification/Tolerability Matrix

		Probability of Occurrence (Likelihood)				
		Extremely improbable	**Extremely remote**	**Remote**	**Reasonably probable**	**Frequent**
		< 10^{-9} per hour	10^{-7} to 10^{-9} per hour	10^{-5} to 10^{-7} per hour	10^{-3} to 10^{-5} per hour	1 to 10^{-3} per hour
ESARR 4 Severity	Accidents	Review	Unacceptable	Unacceptable	Unacceptable	Unacceptable
	Serious Incidents	Acceptable	Review	Unacceptable	Unacceptable	Unacceptable
	Major Incidents	Acceptable	Acceptable	Review	Unacceptable	Unacceptable
	Significant Incidents	Acceptable	Acceptable	Acceptable	Review	Unacceptable
	No Effect Immediately	Acceptable	Acceptable	Acceptable	Acceptable	Review

5.6 Each consequence should be checked against the above table for tolerability by placing the consequence in the correct Table Cell that lines up the Likelihood and Severity. The consequence will fall in one of the three regions:

a) **Acceptable** - the consequence is so unlikely or not severe enough to be of concern. The risk is tolerable and the Safety Objective has been met. However, consideration should be given to reducing the risk further to As Low As Reasonably Practical (ALARP - see later) in order to further minimise the risk of an accident or incident.

b) **Review** - the consequence and/or likelihood is of concern; measures to mitigate the risk to ALARP should be sought. Where the risk still lies within the 'Review' region after ALARP risk reduction has been undertaken, then the risk may be accepted provided that the risk is understood and has the endorsement of the individual ultimately accountable for safety within the organisation.

c) **Unacceptable** - the likelihood and/or severity of the consequence is intolerable. Major mitigation or redesign of the system may be necessary to reduce the likelihood or severity of the consequences associated with the hazard.

5.7 Several different hazards may all lead to the same consequence (accident/incident). Where this is the case it is not sufficient to assess the tolerability of each hazard independently because this may be misleading. For example there may be fifty hazards that all lead to the same undesirable consequence, where each hazard has a very low probability of occurring e.g. 'extremely remote' in Table 3 above. When considering the tolerability of each individual hazard and consequence, it may be found that each one sits in the 'ACCEPTABLE' region of the Tolerability Matrix. However when all fifty hazards are considered together there will be an increase in the probability of the consequence occurring that may move the consequence from the 'ACCEPTABLE' region to the 'REVIEW' or 'UNACCEPTABLE' region of the Table. It is therefore important to identify those hazards that contribute to the same consequence and add the probabilities together to get an overall probability of the consequence occurring. It is this overall probability for the consequence occurring that is used to identify where the consequence sits in Table 3 above.

5.8 Summation of probabilities is not straightforward where qualitative probability estimates have been used because there are no numbers to add together. Where this is the case the following simple assumptions may be made:

a) More than 50 'Extremely Improbable' hazard consequences are required to move the overall consequence probability into the 'Extremely Remote' category.

b) More than 50 'Extremely Remote' hazard consequences are required to move the overall consequence probability into the 'Remote' category.

c) More than 50 'Remote' hazard consequences are required to move the overall consequence probability into the 'Reasonably Probable' category.

d) More than 50 'Reasonably Probable' hazard consequences are required to move the overall consequence probability into the 'Frequent' category.

5.9 Where several hazards all contribute to the same consequence and risk reduction is required due to where the consequence sits in the tolerability matrix, the matrix can be used to prioritise the most significant hazards to attempt to mitigate first. This is achieved by placing all the individual hazard consequence probabilities in the matrix to see which lie within, or close to the intolerable regions. These hazards are the highest risk and should be mitigated first where practical. This may enable the overall risk to fall into an acceptable category more quickly through addressing the most significant hazards first rather than dealing with a number of less significant hazards of less impact.

5.10 ALARP means a risk is low enough that attempting to make it lower, or the cost of assessing the improvement gained in an attempted risk reduction, would actually be more costly than any cost likely to come from the risk itself. This does not automatically mean the risk is acceptable though; a judgement will need to be made and justified.

5.11 Once the assessment of acceptability of the risk has been completed for all the identified hazard consequences, the results should be recorded in the hazard log. It is particularly important that all cases where the risk falls in the 'REVIEW' region of the Table but has been accepted as ALARP and tolerable are well documented and that the justification for the decision is clearly stated.

6 Step 6 - Risk Mitigation and Safety Requirements

6.1 The key activities in Step 6 are:

a) mitigate those risks identified as Unacceptable;

b) apply ALARP principles generally; and

c) generate Safety Requirements.

6.2 As already noted in Step 5, if the consequence does not meet the predetermined acceptability criteria, an attempt should always be made to reduce the risk to a level which is acceptable, or if this is not possible, to ALARP using appropriate mitigation measures.

6.3 It is recommended to apply the ALARP principle to all identified risks, even where the risks fall in the 'Acceptable' region of the tolerability matrix. This is in order to support the goal of constant safety improvement whenever practicable.

6.4 The identification of appropriate risk mitigation measures requires a good understanding of why the hazard is likely to manifest and the factors contributing to the severity of its consequences, since any mechanism that will be effective in reducing risk will have to modify one or more of these factors.

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

6.6 Risk mitigation strategies include:

a) revision of the system design;

b) modification of operational procedures;

c) changes to staffing arrangements; and

d) training of personnel to deal with the hazard;

e) development of emergency and/or contingency arrangements and plans; and

f) ultimately, ceasing operation.

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

6.8 The effectiveness of any proposed risk mitigation measures must be assessed by first examining closely whether the implementation of the mitigation measures might introduce any new hazards or whether they change the basis on which other assessments have been made. Having decided that a simple mitigation measure may be suitable it will often be necessary to repeat steps 3, 4 and 5 in order to evaluate the acceptability of the risk with that proposed mitigation measure in place. If the proposed mitigation measure can affect other parts of the system - or, perhaps, even the suitability of the system to achieve its intended function - it may be necessary to repeat step 2 or even step 1. Unfortunately it is not possible to give any more specific guidance on when it might be necessary to reassess the system as a whole because this judgement can only be made by those who fully understand the system.

6.9 Mitigation measures that are necessary for the system to meet the safety criteria are referred to as Safety Requirements and must be clearly documented. Putting the system into operational service cannot proceed until all these Safety Requirements are met. Step 7 of this process addresses the arguments and evidence required to show that each Safety Requirement has been satisfied.

7 Step 7 - Claims, Arguments and Evidence that the Safety Objectives and Safety Requirements Have Been Met and Documenting this in a Safety Case

7.1 The key activities in Step 7 are:

a) identifying all applicable Safety Objectives and Safety Requirements;

b) developing Claim, Argument and Evidence statements; and

c) documenting the results in a logical and complete manner.

7.2 Introduction

7.2.1 The documenting of claims, arguments and evidence that a system meets its Safety Requirements is part of the Safety Case (or Safety Case Report) and may be presented as a stand-alone document for the system.

7.2.2 Safety Objectives and Requirements will have been identified in the previous steps of this procedure, however further Safety Objectives and Safety Requirements may be applicable from regulatory material and other standards, including those internationally adopted.

NOTE 1: For conciseness in section 7 the term 'Safety Requirement' is used to mean both 'Safety Objective' and 'Safety Requirement' as appropriate.

NOTE 2: Reference to Safety Requirements in the section below refers to those identified in the hazard analysis process (steps 1 to 6) and those applicable from regulatory material and other standards.

7.2.3 Safety Requirements that relate to the performance of software within air traffic service related systems are subject to extra scrutiny due to the additional problems that software has historically shown to manifest. Software related Safety Requirements must comply with the arguments and evidence requirements described in CAP670 Part B Section 3 SW01; guidance within SW01 shows how this can be achieved.

7.2.4 Evidence can vary in quality, depth and quantity and it is important that the level of evidence provided to demonstrate that a Safety Requirement has been achieved is commensurate with the criticality of the Safety Requirement. It is not always obvious when this is the case therefore guidance is provided to show the level of evidence expected for various criticality levels (see Appendix G).

7.2.5 Evidence can come from a variety of sources and guidance is provided in this section on the sources of evidence.

7.2.6 Presentation of evidence alone is not sufficient to demonstrate that a Safety Requirement has been satisfied. The evidence must be associated with a claim being made and an argument that explains how the evidence demonstrates that the Safety Requirement has been met.

7.2.7 Some Safety Requirements have to be broken down into a smaller set of Safety Requirements which when combined demonstrate the higher-level requirement. Accordingly, claims, arguments and evidence that prove the full set of lower level requirements can be used as evidence of satisfaction of the top-level requirements. Guidance on methods of representing a hierarchical structure of claim, argument and evidence is provided later in this section.

7.2.8 In some cases it may not be possible to fully demonstrate achievement of a Safety Requirement, or it may be necessary to make assumptions when demonstrating achievement of Safety Requirements where there is no supporting evidence. Where this is the case, then the shortfall in evidence must be clearly documented so that any residual risk due to any uncertainty may be considered and either accepted, or worked on further to reduce the risk.

7.2.9 The Safety Requirements, claims, arguments, evidence and any shortfalls identified need to be documented in a coherent manner to allow easy understanding and to facilitate future review and update. It should be remembered that Safety Cases are living documents that develop along with the lifecycle of the project (see Chapter 1, Lifecycle). Guidance is provided on the structure and content of a Safety Case (or Safety Case Report) in the following paragraphs.

7.3 Safety Case (or Safety Case Report) Presentation and Structure

7.3.1 A Safety Case is the key document that demonstrates that a system is safe. It (or a summarised version of it in the form of a Safety Case Report) is the document that the Regulator may audit to ensure that the ANSP or aerodrome operator has satisfied themselves that the system has been fully analysed and demonstrated to be safe. It is also a key document likely to be called up as evidence for any legal action involving a failure of safe operations. It is therefore important that the following are considered to ensure that the document is concise, clearly presents the information and is complete:

a) Provide a title page clearly stating the system under consideration and at what stage in the project this Safety Case covers.

b) Provide an Amendment Record that logs the history of the document e.g. the various drafts and formal issues with a short note of what has changed at each up-issue.

c) Provide a Contents Page stating what each section of the document covers and any tables, figures, diagrams or appendices that are included.

d) Write in plain English. Avoid overly long sentences; use well-understood terms rather than the obscure.

e) Use figures and diagrams to support the text e.g. one well-labelled radar coverage diagram can convey more information quickly than a long textual description of the coverage.

f) Adopt a logical and sequential structure to the document (more on this follows).

g) Use page numbering.

7.3.2 Modern information technology (IT) systems can be employed to make finding your way around a Safety Case and supporting information easier. For example it may be possible to burn a safety case and supporting evidence to a Compact Disk (CD) and use hyperlinks within the Safety Case text to call up the evidence documents.

7.4 Safety Case Structure

7.4.1 Table 4 shows a suggested Safety Case structure. It is recommended that this be followed, although other logical structures may be used. Note also that depending on the stage in the lifecycle that the project is, not all sections in the table may be applicable.

NOTE: Some complex organisations with separate departments responsible for different aspects of a Safety Case may choose to divide the Safety Case into multiple parts. This is not necessary and the documentation can be provided in whatever form is most suitable.

Table 4 Suggested Structure of a Safety Case

Part or Section	Description
Title Page	Include: the name of the organisation to which the Safety Case is relevant; the system being covered; stage in the project; issue status; date of issue; author(s). An 'Authorised By' sign-off table may be included where this is a Quality Management requirement for the organisation.
Configuration Control Page	A table showing the version history of the document including a brief description of what changed between versions
Executive Summary	A brief description of the Safety Case including: a short introduction to the system, where the Safety Requirements have come from, whether they have been met, key outstanding activities, residual risks and the conclusions drawn.
Acronyms and Abbreviations	Include a list explaining any acronyms or abbreviations used in the safety case.
Contents Page	Include chapters or sections, tables, diagrams, figures, appendices and page numbering for these.
Scope	Include: The overall role of the system, why it is needed, where it fits in with other systems and the limits to what this Safety Case covers.
Functional Description	Include a description of the functions of the system; include the operational requirements; use diagrams and figures; show where this system fits in with others including any interfaces to other systems.
System Description	Describe the components of the system, interfaces between them; use diagrams and figures; describe the different allowable configurations of the system. Record here the version number, build state or procedure issue for which this Safety Case is applicable.
System Operation	Describe how the system will, or does operate; include the concept of operation; describe the flow of information or data; inputs and outputs (e.g. human machine interface [HMI] aspects); what processes are carried out or what decisions are being made.
System Design	Describe how the system was designed; who designed it; any design standards used. **Note:** This section can be expanded to act as supporting (backing) evidence where Safety Requirements call for evidence of good design practice.
Design Dependencies	Include any systems or inputs that this system depends upon for safe operation. Be brief where these have already been described in the previous sections of the document.
Assumptions	Include any assumptions about interfaces or other systems with which this system interacts and any other assumptions; include justification for the assumptions where possible. **Note:** These assumptions are likely to have been made during the hazard identification and risk assessment processes.
Safety Objectives	Where Safety Objectives have been set for individual hazards, then these should be stated. Where the tolerable probability for a set of hazards sharing the same consequence severity has been used (as in the case of using a risk matrix to set Safety Objectives) then the tolerable probability for each severity level should be stated, along with a list of hazards associated with each severity level.

Table 4 Suggested Structure of a Safety Case (continued)

Safety Requirement Derivation	State how the Safety Requirements came about, referencing out to related documentation e.g. reports from brainstorming, HAZOPs or FMECA.
Safety Requirements	State the derived Safety Requirements for the system i.e. the safety requirements derived by this procedure. Where available/applicable, include the Required Level of Confidence for each Safety Requirement i.e. High, Medium or Low (See Appendix G).
Statutory Safety Objectives and Requirements	Reference out to regulatory material containing Safety Objectives and Requirements applicable to this system; only restate them if compact (See paragraph 7.5 - Safety Requirements below).
System Assurance	Address each Safety Objective and Safety Requirement; include the claim(s), associated argument(s) and reference the evidence that supports each argument; reference to diagrammatic representations of arguments if used (See Appendix E for more information). Identify the status of the Requirement i.e. is it met, not yet met or only partially proven? State whether any further work to prove that the Requirement is met is planned e.g. at later stages of the project (See paragraph 7.6 - Claims, Arguments and Evidence below).
Limitations and Shortcomings	Identify any deficiencies found with the system. Identify any Safety Objectives or Requirements that have only partially been proven, have failed to be proven or have insufficient evidence to provide the required level of confidence (except those Requirements where further validation work is already planned). Identify any counter evidence for the system i.e. any evidence that demonstrates that a Requirement is not met. Reiterate any assumptions for the system for which there is no, or insufficient validation or rationale.
Ongoing Monitoring	Identify any Safety Objectives or Requirements that require ongoing monitoring in order to accrue evidence that the Requirement continues to be met.
Conclusion	Draw a conclusion on the Safety Case. State whether your organisation believes the system is safe to be put into service or what additional work is necessary in order for this to be the case; or state whether you believe that the planned work will lead to system being safely put into operational service. State any limitations and shortcomings that your organisation is prepared to live with and any that are unacceptable, including any actions to rectify the situation.
References	Where applicable, include the following references: a) Standards; b) Supporting hazard identification and risk assessment documentation; c) Sources of evidence.
Appendices	Appendices should be used to store text, diagrams, tables etc., that if contained in the main body of the Safety Case, may distract from the main flow of the document. Typically, appendices should contain: a) Extracts from MATS Pt 2/Aerodrome Manual e.g. where they form part of the system description; b) Compact items of evidence (reference should be made to larger documents rather than reproducing them); c) Standards Compliance matrices; d) Verification Cross Reference Indices (VCRI).

7.5 Safety Requirements (including Safety Objectives)

7.5.1 The purpose of the Safety Case is to demonstrate that all Safety Requirements for the system under consideration have been addressed and that the system is tolerably safe. It is necessary, therefore, to clearly state the Safety Requirements being addressed early in the Safety Case.

7.5.2 Safety Requirements to be stated come from several sources:

a) Those generated by the risk assessment process (Steps 1 to 6 of this procedure). These are called 'Derived Safety Requirements';

b) Those applicable from regulatory material and/or standards, called 'Statutory Safety Objectives and Requirements', for example:

- ICAO Annexes e.g. Annex 10 technical requirements for communications, navigation and radio (including radar and ADS-B) systems;
- Single European Sky Common Requirements, Implementing Rules and Community Specifications;
- CAP 168 Licensing of Aerodromes for aerodrome requirements;
- CAP 670 ATS Safety Requirements for technical and resource requirements (including software Safety Requirements);
- CAP 744 Air Traffic Controllers - Licensing for training and competence requirements;
- CAP 700 Operational Safety Competences - A UK Code of Practice for aerodrome management competence requirements.

7.5.3 Identifying Safety Requirements from the many interoperability and other requirements contained in international standards (such as those identified in 7.5.2 b) above) is not always straightforward. One of the simplest ways to identify whether any particular Requirement is a Safety Requirement is to pose the question, 'if this requirement fails to be met, or is only partially met, will it increase the safety risk of the system under consideration?' If it does increase the probability of an incident, or the likely severity of an incident to an intolerable level, then it should be considered a Safety Requirement that will need to be addressed in a Safety Case.

7.5.4 Requirements found in International Standards that are not explicit Safety Requirements are often concerned with interoperability and will still need to be complied with where the standard has been endorsed by the UK CAA or Europe as a whole. Therefore consideration should be given to demonstrating compliance to all requirements within the standards and documenting the results in the Safety Case. This saves having to go through the process of differentiating between safety and non-safety requirements with the possibility of making errors leading to some safety requirements being overlooked. It is acceptable for a Safety Case to include such aviation-related requirements.

7.5.5 Where it is practical to do so, then the safety requirements should be restated within the safety case e.g. The Derived Safety Requirements generated from the Risk Assessment process (steps 1 to 6) would normally be restated.

7.5.6 Where impractical to restate the Safety Requirements e.g. where International Standards documents are involved with many detailed Requirements, then references to the documents and sections where the Safety Requirements can be found needs to be made in this part of the Safety Case.

7.5.7 A compliance matrix or verification cross-reference index (VCRI) can be useful in documenting compliance to referred standards. These consist of tables listing the paragraph numbers from the standard, a shortened form of the requirement, where the requirement is proven to be met e.g. test specification reference, analysis report etc. (or how it is intended to be proven where not yet proven) and any deviation or limitation in meeting the requirement that has been identified. Spreadsheet or Database software can be used to manage these tables.

NOTE: It is often impractical for ANSPs or aerodrome operators to demonstrate compliance to detailed sets of technical requirements, such as those found in ICAO SARPs, themselves. They are therefore advised to place the requirement to provide evidence of compliance to these standards on the suppliers of the equipment or services at the contract stage. It is then up to the ANSP or aerodrome operator to satisfy themselves that the evidence provided is acceptable.

7.6 Claims, Arguments and Evidence

7.6.1 It is not enough to merely state that a Safety Objective or Requirement has been satisfied; it must be proven. This can be achieved through statements linked to evidence clearly showing that a Requirement has been met. The statements take the form of a claim, justified by an argument supported by evidence.

7.7 Claim

7.7.1 A claim is a simple statement typically used to indicate that a safety objective or requirement has been met as demonstrated by the associated argument and evidence. It may be the case that a complete claim can not be made due to incomplete or weak evidence being available, in which case the deficiency in the claim should be clearly stated and addressed later in the 'limitations and shortcomings' section.

7.7.2 A claim may be sub-divided into a number of smaller sub-claims which when combined meet the overall higher-level claim. If representing this in text, then this needs careful structuring to avoid confusing or losing the reader. The following may help:

a) Use of a hierarchical numbering system e.g. 1.1, 1.2, 1.2.1, 1.2.2, 1.3 etc.;

b) Use of paragraph indents (as often used in software programming) where the indented text may be sub-claims of the preceding non-indented text;

c) Tabulation of the text, with separate tables for each top-level claim and its sub-claims.

7.7.3 Alternatively, the hierarchy of claims, arguments and evidence can be represented diagrammatically using one of a number of notation systems (typically associated with software tools). See Appendix E for more information.

7.8 Arguments

7.8.1 Arguments are statements justifying why a claim is valid and point to the supporting evidence. Depending of the amount of evidence available supporting a claim being made, more than one argument per claim or sub-claim may be required to encompass all of the evidence.

7.9 Evidence

7.9.1 Evidence is used to support an argument that a Safety Objective or Requirement has been met as associated with claim-argument-evidence statements or diagrammatic representation of arguments. There can be many sources of evidence, however it is important to think about two key types of evidence:

a) **Direct Evidence** - This is evidence clearly linked to the Requirement itself e.g. a test result showing that a safety critical parameter is within tolerance.

b) **Backing Evidence** - This is evidence that supports the Direct Evidence, thus giving Direct Evidence more credibility e.g. a qualified test engineer using certified test equipment carried out the testing or that an approved designer designed an instrument flight procedure.

7.9.2 In general, Direct evidence comes from three sources:

a) **Test Evidence** - the running of test procedures and simulations designed to exercise the equipment or operational procedures and to measure the performance against predefined criteria. This also includes inspection against checklists derived from standards e.g. ICAO Standards and Recommended Practices (SARPs), Eurocae Minimum Operational Performance Standards (MOPS), CAA Publications (CAPs) etc.

b) **Field Service Evidence** - using records of satisfactory performance of identical or similar systems as evidence for the new system.

c) **Analytical Evidence** - predictions of performance based on design information or analysis of a limited amount of testing or field service evidence.

7.9.3 It is important that the evidence presented in support of an argument is appropriate and credible. When recording evidence the following factors should be considered:

a) **Scope** - The evidence should cover the full extent of the Requirement(s) concerned. Where it does not, further evidence may be required to extend its scope.

b) **Completeness** - There should be no gaps in the evidence. Where there are gaps, then further evidence to fill the gaps may be required.

c) **Accuracy** - Where tests, simulations or field evidence is used, these should be based on an accurate representation of the system being considered. Also, where tests or simulations are used, then the test equipment used should be shown to have the precision required to accurately measure the performance.

d) **People** - The people involved in obtaining or developing the evidence should be qualified or have the necessary experience to do this well.

e) **Configuration Control and Traceability** - Good configuration control i.e. the ability clearly link the evidence to a documented system build state or procedure issue, provides credibility that the evidence is applicable to the system being considered.

f) **Quality Management** - The credibility of evidence is improved where it is demonstrated that it was developed under a good Quality Management regime e.g. review and sign-off procedures are in place and are used; test equipment is certified and internal quality and safety reviews take place etc.

g) **Scrutiny** - The credibility of evidence increases where it has been subjected to independent scrutiny e.g. by inspection by internal or external qualified or experienced inspectors.

h) **Quantity and Diversity** - The more corroborating evidence there is, particularly from different and diverse sources, the more confidence there will be in the evidence to support a Safety Requirement.

i) **Depth** - Evidence can vary in depth e.g.:

- Evidence could cover default operation, operation within expected limits or operation to extreme limits.
- It could be at a system level or go down to component level.

The greater the depth of the evidence then the more confidence there will be in that evidence.

j) **Presentation** - Evidence, along with claims and arguments, should be presented in a manner that is straightforward to understand and follow. Poorly presented evidence erodes its credibility.

7.9.4 An area of difficulty arises when deciding the quality and level of evidence required to provide reasonable assurance that, for example, a Safety Objective or Requirement has been met. This often comes down to a judgement call by those involved. However, what is perceived to be a reasonable level of evidence by a ANSP or aerodrome operator may not be seen as acceptable by the Regulator. Where this is a problem a method has been devised to define the quantity, type and diversity of evidence required to achieve a certain level of confidence. Appendix G provides details on this method.

Appendix A Hazard Identification using Brainstorming

1 Introduction

1.1 This guidance on brainstorming has been derived from the Eurocontrol Safety Assessment Methodology guidance on Identification of Hazards (Ref: SAF.ET1.ST03.1000-MAN-01-01-03-B2 FHA V2 Ch3 GUI B2).

1.2 Hazard identification using brainstorming is complimentary to systematic functional hazard identification e.g. HAZOPs, FMECA etc. The brainstorming method can reveal hazards not identified in the systematic approach.

1.3 Ideally hazard identification using brainstorming should be conducted prior to the systematic approach. This is due to participants in both methods being more open and less focussed on design issues during the brainstorming if they have not been made aware of the detail of the project as required by the systematic approach.

1.4 Table 1 provides an overview of the complete brainstorming process, from initial planning and preparation through to evaluating the results. The remainder of this document expands upon each point made in the table.

2 Initial Planning

2.1 Hazard identification using brainstorming can be undertaken at several stages in the lifecycle of a project. Early in a project, brainstorming may be undertaken once a concept of operation or proposed system description has been drafted. This is necessary to enable the brainstorming group to have an overview of the project and some material to work from. As the project develops and more detail becomes available, the brainstorming exercise may be repeated.

2.2 Due to other commitments e.g. staff rosters, some experts who are valuable to a brainstorming session may need considerable notice to ensure their availability. Depending on the nature and scope of the system under consideration, these may include:

a) Air Traffic Controllers.

b) Pilots.

c) RFFS Staff.

d) Aerodrome Operations Staff.

e) Security Staff.

f) Refuelling Staff.

Table 1 The Complete Brainstorming Process

Plan	• Align risk assessment (including Hazard Identification) activities with the project plans • Involve the Aerodrome Operator, ATC service provider and airline for participating controllers, pilots etc. early in the project due to their limited availability.

Prepare	• Arrange participants which may include:
	  • Relevant Operational Experts e.g. controllers, pilots etc. (ideally NOT involved in the project development or previous systematic hazard identification)
	  • Moderator
	  • Note taker
	  • Expert on operation or system (e.g. senior ATCO, project manager, Aerodrome Operations Manager, senior system engineer)
	  • Safety analyst
	• Prepare how to brainstorm
	• Prepare hazards and categorizations using:
	  • Preliminary scoping brainstorms
	  • Literature, hazard logs and incident/ accident databases
	• Make presentations of:
	  • What a hazard is, how to brainstorm and rules
	  • General background of the project and operation
	• Make a schedule for the brainstorming session
	• Arrange practical issues:
	  • Room free from distractions
	  • Flipchart
	  • Laptop PC and Projector
	  • Availability of refreshments

Brainstorm	• Introduce using prepared presentations
	• Brainstorm:
	  • Take care that basic rules are respected:
	  • As many hazards as possible
	  • No criticism, No dismissals and No analysis
	  • Make short notes of hazards on flipchart
	  • Steer the meeting using prepared hazards and categories
	  • Apply short breaks before productivity drops significantly
	• Close the session

Evaluate	• Distribute minutes of brainstorm with hazard log, requesting corrections
	• Evaluate the effectiveness of the brainstorm:
	  • Are all categories covered?
	  • Are there any suspect categories lacking hazards?
	• Decide whether and when another brainstorming session is needed

3 Preliminary Brainstorming (Scoping Brainstorm)

3.1 The purpose of the preliminary brainstorming activity is to establish a set of Hazard Categories and Issues that can be later used to guide the full brainstorming activity. Typically the Moderator of the brainstorm group can undertake the preliminary brainstorm on their own or with the help of others e.g. a Safety Analyst. This activity should take place before the full brainstorm.

3.2 Input to the preliminary brainstorm can be historical hazard data on similar systems e.g. incident / accident databases, reporting schemes or hazard logs.

3.3 The output of the preliminary brainstorm should be a list of hazard categories and issues, typically:

a) Operational Aspects.

b) Technical Aspects.

c) Potential Conflicts: departures; taxiways.

d) Flight Phases.

3.4 Since the preliminary brainstorming activity is a one or two person exercise, and the purpose of it is not to produce any detail, the conduct of the exercise can be left to the choice of the participants. The guidance that follows for full brainstorming does not necessarily apply to the preliminary brainstorm.

4 Preparation for Full Brainstorming

4.1 Participants

4.1.1 The number of participants at a brainstorming session should be limited to a maximum of 6 people. More than this becomes unproductive and special arrangements should be made to regain some efficiency:

a) Dividing the larger group up into working pairs;

b) Participants undertaking individual note taking followed by group discussion of the findings of each person.

4.2 Participants with Administrative Roles

4.2.1 All participants take part in the brainstorming ideas generation activities, however some participants also have an administrative role:

a) **Moderator:** Controls the flow and timing of the meeting; states the rules of conduct and introduces material and hazard categories to consider. The principle goal of the moderator is to ensure the brainstorming activity is productive;

b) **Safety Analyst:** Should be familiar with hazard, cause and effect and help the group with safety terminology and structuring the record of hazards;

c) **Note Taker:** Somebody noting down the detail of the hazards; this may be on a laptop PC connected to a projector so that the participants can correct any misunderstandings (however the correction of notes should take a lower priority than the generation of ideas);

d) **Operation/System Expert:** This should be somebody familiar with the planned project such that they can answer any clarification questions about the project by participants. Typically this may be the Project Manager, Senior Air Traffic Controller

or Senior Systems Engineer. They would normally present the project overview at the beginning of the session.

NOTE: The Moderator and Safety Analyst may be the same person. The Note Taker may be the Safety Analyst (where not also the Moderator) thus enabling the definition of hazards using correct safety terminology.

4.3 Creative Participants

4.3.1 The above participants have an administrative role to play in the brainstorming process. However the principle role of the remaining participants is to creatively identify hazards with the planned system or project. Key to this is the inclusion of Operational Staff:

a) **Air Traffic Controller:** Where possible this person should not be familiar with the planned project prior to the brainstorming session, but should be familiar with the type of ATC functions planned to be performed e.g. approach control, area control etc.

b) **Pilot:** Where possible this person should not be familiar with the planned project prior to the brainstorming session, but should be familiar with the types of aircraft and operations that may be involved in the planned project.

c) **Relevant Aerodrome Personnel:** Where possible this person should not be familiar with the planned project prior to the brainstorming session.

5 Preparing a Brainstorming Session

5.1 Session Logistics

5.1.1 Brainstorming sessions can be taxing on participants, therefore the following should be considered when arranging the logistics of a session:

a) A meeting room protected from distractions e.g. no calls to be taken.

b) The preparation of a meeting schedule that divides the allocated time up into manageable chucks with frequent refreshment breaks e.g. several half hour sessions split by 10 minute breaks.

NOTE: Participants are normally more pro-active in morning sessions than afternoon sessions.

c) Easy availability of refreshments.

5.2 Introductory Brainstorming Presentation

5.2.1 Some participants to a brainstorming session may not be familiar with the process or what is expected of them. It is therefore important to explain this, ideally in the form of a short presentation covering:

a) Definition of a hazard.

b) How the brainstorm will be managed i.e. the rules:

- No contradiction or dismissals allowed.
- How participants should inform the group of their hazard ideas e.g. open free-for-all discussion; notes on post-its to be stuck on a board; hands raised awaiting moderator attention.

NOTE: Participants are advised to have notepaper and pens to jot down hazards as they occur to them just in case hazards start 'queuing' to be discussed or recorded.

5.2.2 The Moderator would normally undertake the above presentation lasting no longer than 10 minutes.

5.3 **Project or System Presentation**

5.3.1 The brainstorm participants need material to work off, therefore an overview of the project should be presented:

a) This should last no longer than half an hour.

b) It should not be very detailed, but typically cover:

- The objective of the project.
- Concept of Operation e.g. Airspace Configuration and Interfaces; Aerodrome Layout; traffic characteristics; timeframe.
- Human Roles (from an ATC, Pilot or Aerodrome Personnel point of view).
- Policies and Procedures.
- Technical Systems.

c) It should be biased towards pictures and diagrams.

NOTE: The pictures and diagrams e.g. airport layout, airways structure and charts, should be made into posters and stuck around the room where the brainstorming activity takes place to promote their constant consideration and easy reference.

5.3.2 The Operation/System Expert would normally undertake the above presentation.

6 Conduct of the Brainstorming Session

6.1 After the Introductory Brainstorming Presentation and the Project or System Presentation (see above) have been delivered, the Moderator would take control of proceedings by directing the group to consider the hazard categories and issues previously identified at the preliminary brainstorming stage.

6.2 All participants would explore each of the categories and issues and feel free to raise any safety related issues that occur to them. Hazards raised should be quickly noted down on a flipchart to be discussed and expanded further (although not analysed in detail at this stage).

6.3 The Safety Analyst would help formulate any identified Hazards into appropriate wording and the Note Taker would ensure that these are correctly recorded.

6.4 If using a laptop PC and projector, the note taker can ensure that the correct understanding of the hazard as raised by the participant has been recorded.

6.5 This continues, according to the planned schedule, until all the categories and issues identified from the preliminary brainstorm have been exhausted. However, if during the brainstorm activity, further issues and general hazard categories have been identified in addition to those identified during the preliminary work, then these should be explored until exhausted.

7 After the Brainstorming Session

7.1 The minutes or notes of the brainstorming session, which should be sectioned into the hazard categories raised at the meeting, should be supplied to the participants within a few days for error checking.

7.2 The results of the Hazard Identification process should be reviewed and a judgement made as to the how successful the process has been. If, for example, it appears that a particular hazard category has not raised the expected number of hazards, then consideration should be given to arranging further brainstorming sessions (in the lifecycle of a project, there may already be several iterations of Hazard Identification planned providing the opportunity to focus up on any particular issue at a later stage).

7.3 The hazards identified from the Brainstorming Session, together with other Hazards identified by other methods feed in to the next steps of the Hazard Analysis process to ascertain the severity and likelihood of their consequences.

7.4 The hazards identified from the Brainstorming Session should be entered in the Hazard Log where this is being maintained (see Appendix F).

NOTE: The brainstorming group may consist of the same team conducting the risk assessment; therefore the group may allocate initial severity and likelihood information to the hazard consequences immediately after the brainstorming process to aid the later assessment.

Appendix B Failure Modes, Effects and Criticality Analysis

1 Introduction

1.1 Failure Mode Effects and Criticality Analysis (FMECA) is a popular method used for identifying hazards for risk assessment. It is a systematic analysis method used to identify hazards at a functional overview level that can be developed further as more system detail becomes available.

1.2 Although the FMECA process itself is simple, it can be time consuming and the quantity of data assessed and recorded can make it appear complicated. A methodical and disciplined approach to undertaking FMECA work is essential if the full benefit of the FMECA analysis is to be delivered.

1.3 Generic guidance on the FMECA and FMEA (Failure Modes and Effects Analysis) can be found in:

a) International Standard IEC 812 - Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis.

b) Mil-Std 1629A - Procedure for Performing A Failure Modes and Effects Criticality Analysis (although withdrawn from publication the FMECA process in this standard is commonly used).

1.4 This document provides more specific guidance on performing FMECA analysis to identify and categorize hazards when considering Air Traffic Service and Aerodrome operations.

2 The FMECA Process

2.1 Figure 1 shows a flow diagram of the FMECA process.

2.2 The FMECA process can be undertaken at several points in the life cycle of a project, typically:

a) At the initial Concept of Operations or Project Intentions/Ideas stage - where system functions have been defined, but not necessarily the equipment, people or procedures. Running a FMECA at this early stage will identify the most critical functions or constituents of a system that may influence later design choices.

b) At initial system design or initial project definition - where functions are now associated with equipment types and more information on the people and procedures involved is available. Running a FMECA at this stage can help in the final selection of equipment.

c) At the final stage on the actual equipment, procedures and people that will be used. Running a FMECA at this stage will identify any equipment/procedure specific failure consequences that may not have been apparent at the less detailed stages and confirm or update the findings, estimates and assumptions of any earlier FMECA activities.

2.3 Performing a FMECA at the earliest practical point in a project may reduce the amount of work required later on. It may be found that some top-level functions do not pose significant hazards if they fail; as such, further detailed FMECA analysis on lower level system design supporting this function may not be required. Any decision to limit later analysis based on this should be justified and recorded.

2.4 An individual or a team of people may undertake the FMECA. Depending on the level at which the FMECA is being performed and its scope, the individual or team should:

a) Have good knowledge of the Concept of Operation or Project Intentions.

b) Have good knowledge of the environment in which the system will operate.

c) Have experience of Operational Procedures, where these are being analysed.

d) Have good knowledge of the equipment functions and failure modes.

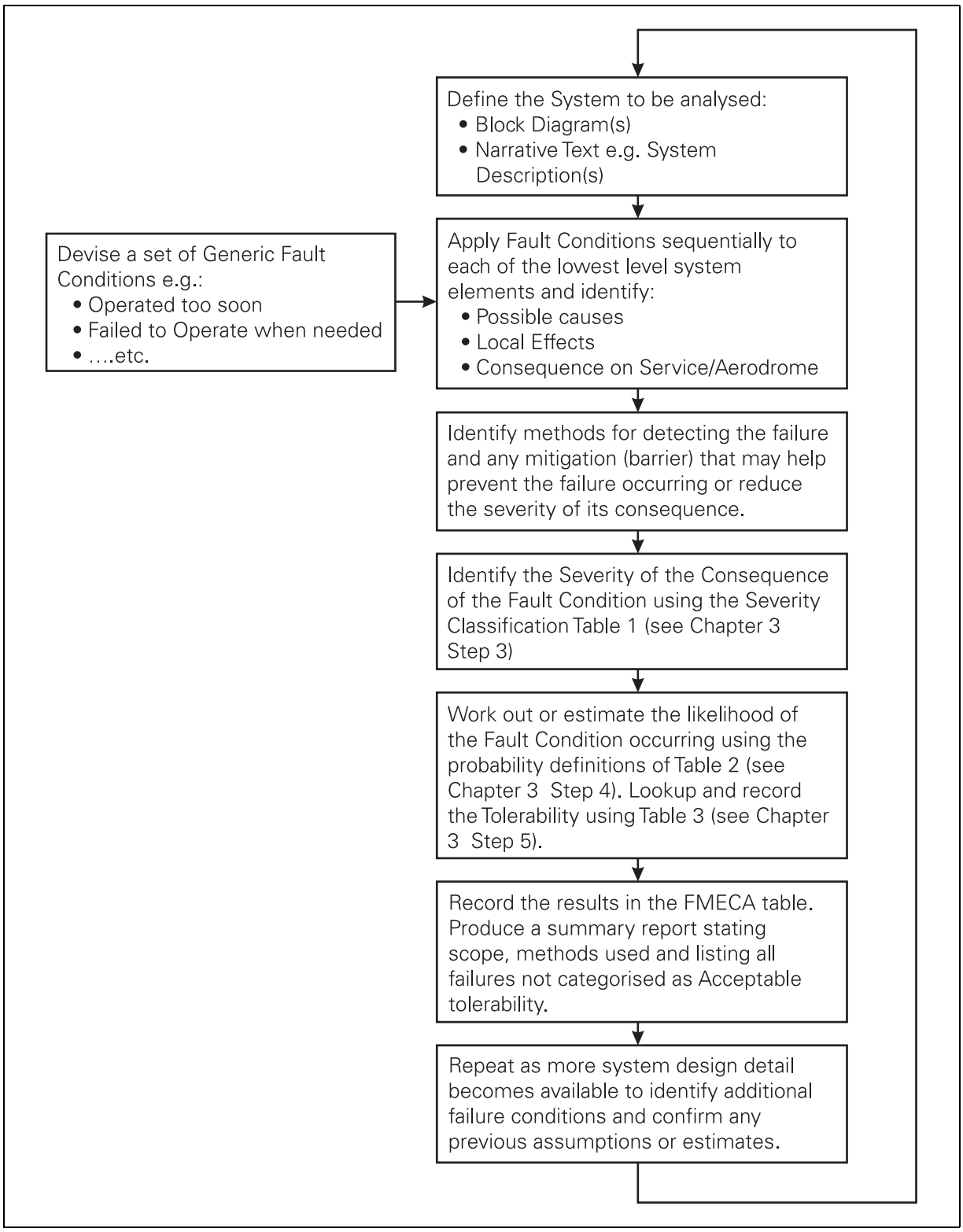

Figure 1 The FMECA Process

3 Defining the System to be Analysed

3.1 A FMECA can be scoped to run at any level, from complete integrated systems to individual equipments. Typically the following applications of FMECA may apply:

a) Running a top-level functional FMECA on an entire Air Traffic or Aerodrome operation. This will help define the top-level interactions and critical functions and help define the structure in which lower level FMECA analysis will sit.

b) Running a medium level FMECA on a set of sub-systems supporting one overall function e.g. a Surveillance System, combining Radar Sensor, Data Transmission and Display systems or an Aerodrome Refuelling operation involving people, equipment and procedures etc.

c) Running a detailed FMECA on an individual equipment or procedure. This may be the case where new or replacement equipment is being installed in an existing system, or where a procedure has been modified or replaced with a new one.

NOTE: It is recommended that Air Traffic Service providers and Aerodrome Operators who identify a requirement for a detailed individual equipment level FMECA consider passing this requirement on to the sub-contractor or equipment supplier i.e. where the detailed design expertise on the equipment resides.

3.2 At whatever level the FMECA is being performed, it is essential that the system to be analysed be clearly defined. Typically this will entail the development of Block Diagrams and supporting narrative text.

4 Block Diagrams

4.1 The purpose of a block diagram is to give a pictorial representation of the system components, what they do and how they relate to each other. Depending on the level of the FMECA, blocks and links between blocks may contain different information.

4.2 Blocks may contain: Function Titles; System Elements (Equipment, People and Procedures), Sub-Systems (e.g. part of an equipment or procedure) down to component level. These should be labelled within the blocks. It is recommended to number the blocks for easier reference during any discussions and for easier text referencing in the narrative description.

4.3 Links between blocks are generally directional i.e. inputs and outputs (or more generally influences on the block and influences the block has on other blocks). The lines between the blocks should be labelled with the influence it has.

NOTE: If using a FMECA process to analyse Procedures, then the block diagram may take the form of a series of steps shown as a sequence of operations.

5 Narrative Text

5.1 The purpose of the narrative text is to provide a description of the system. Typically this relates to the block diagram, expanding on functions and influences where necessary. Any assumptions about the system can be stated here. Text relating to system elements shown in the block diagram can be related through reference to the numbering of the blocks.

6 Defining Failure Modes

6.1 Rather than randomly think up failure conditions for each element of the system, it is recommended to identify a set of failure conditions that can be sequentially applied to each system element. Top-level failure modes are common across many systems and typically include:

a) Operated too soon or unexpectedly.

b) Failed to stop operating at the correct time.

c) Failed to operate when required.

d) Operated, but with errors.

e) Failed during operation.

6.2 Depending of the level of the FMECA analysis and the system elements being considered, a set of more specific failure modes can be defined. For ATS equipment these may include:

a) Failed to transmit.

b) Stuck in transmit.

c) Intermittent Transmit.

d) Data lost.

e) Partial Data lost.

f) Total Data Corruption.

g) Partial Data Corruption.

6.3 For Aerodrome Functions these may include:

a) Fuel Spillage.

b) Manoeuvring Area surface damage.

6.4 For Procedures these may include:

a) Failed to undertake a step.

b) Skipped a step.

c) Undertook steps in wrong order.

d) Partially completed a step.

7 Performing the Analysis

7.1 With the block diagram of the system, associated narrative text and list of possible failure modes it is now possible to start the analysis. The results of the analysis need to be recorded and Figure 2 gives an example of construction of a table suitable for this purpose.

7.2 The analysis process can be a long one, with many failure modes being analysed that are very unlikely to occur or have insignificant consequence. However it is important to systematically run through all of these to record the fact that they were considered. Many sheets for recording the results may be required. Industry has produced FMECA Software to run on a PC to help record and present results.

7.3 The analysis process involves addressing each element shown in the block diagram in turn, applying the failure modes to the inputs and outputs or the function itself and recording the following in the Table:

a) The system element being considered, including its identity number (where numbered in the block diagram).

b) The Failure Mode being applied.

c) The possible causes of the failure - at the higher-level analysis this can be limited to generic failure causes, rather than a long list of specific causes. At the lower level analysis, specific causes can be listed.

d) The local effect of the failure - this can be limited to the effect on output to the next system element, describing the characteristics of the effect.

e) The end effect of the failure - this is the overall effect on the Air Traffic Service or Aerodrome Operation. Here it may be expeditious to indicate the Severity Level according to Table 1 (see Chapter 3 - Step 3).

f) The Failure Detection Methods - record any mechanisms for identifying the failure condition e.g. Control and Monitoring Systems, ATCO Detection on the Display.

g) Barriers and Mitigations - record any existing mechanisms for reducing the probability of the failure occurring or reducing its severity (consequence). This is only for existing mechanisms, and not for defining new barriers or mitigations - this comes later in Step 6 of the 7 Step process. Also see Appendix D on Event Trees to see whether event tree analysis will help identify any barriers.

h) The Probability of the Failure occurring - data may be available from equipment suppliers or field service history of similar equipment. Estimates from experienced Operational Staff and Engineers may be the best alternative.

i) The Tolerability of the Failure - Use Table 3 (see Chapter 3 - Step 5) with the recorded severity and probability figures to identify and record the Tolerability criteria e.g. Acceptable, Review or Unacceptable.

NOTE: This is a slight deviation from the traditional FMECA process, but makes sense where following the 7 Step process.

j) Any other Comments - here record anything of significance not recorded in the other sections of the table e.g. any additional assumptions or the rationale for difficult decisions made.

8 Common Mode Failures

8.1 Environmental effects and some system failures may have an impact on more than one system. Consideration should be given to these, for example:

a) Failure of the outside electricity supply.

b) Adverse weather.

c) Failure of air conditioning.

d) Fire.

9 The FMECA Report

9.1 Due to the volume of analysis material likely to be produced as a result of the FMECA process, it is important to summarise the process and results in a FMECA report. The purpose of the FMECA process described above is to identify and categorise hazards in order that they may be considered further in the later steps of the 7 Step process.

9.2 It may be that several FMECA processes have been undertaken to analyse a complicated or large system. The FMECA report is a place to bring together the results of these analyses.

9.3 The report should contain:

a) The scope of the report i.e. what systems have been analysed.

b) Summary of how the analysis was performed: who, when and how the analysis was conducted.

c) A summary of all the failure conditions other than those found to be inconsequential.

10 Updating the Hazard Log

10.1 The hazards identified by the FMECA process should be entered in the Hazard Log where this is being maintained (see Appendix F).

System element	I/D no.	Failure mode	Cause	Local effect	End effect	Severity	Detection method	Barriers/ mitigation	Probability	Comment

Figure 2 Example Structure of FMECA Table

INTENTIONALLY LEFT BLANK

Appendix C Hazard and Operability Studies

1 Introduction

1.1 A Hazard and Operability Study (HAZOP) is a systematic functional hazard identification process that uses an expert group to conduct a structured analysis of a system using a series of guide words to explore potential hazards.

1.2 The HAZOP systematic approach to Hazard Analysis is complimentary to non-systematic approaches such as the brainstorming method.

1.3 Table 1 provides an overview of the complete HAZOP process, from initial planning and preparation through to evaluating the results. The remainder of this document expands upon each point made in the table.

2 Initial Planning

2.1 HAZOP can be undertaken at several stages in the life cycle of a project. Early in a project, HAZOP may be undertaken once a concept of operation has been drafted. As the project develops and more detail becomes available, the HAZOP process should be repeated typically at the Detailed Design stage, and once the System has been implemented. Therefore performing HAZOP studies should be programmed into project and safety plans from the outset.

2.2 Operational staff, e.g. Air Traffic Control Officers (ATCO), System Engineers, Pilots and various Aerodrome Staff are normally key participants in a HAZOP group. However operational commitments may limit their availability. Therefore advanced planning and notification of HAZOP activity is required to enable the Air Traffic Service Provider (ATSP), the Airline and the Aerodrome Manager to plan the release of these staff.

Table 1 The Complete HAZOP Process

Plan	• Align risk assessment (including Hazard Identification) plans to the project plans • Involve ATC service provider, the airline and the Aerodrome Manager for participating Operational Staff early in the project due to their limited availability.

Prepare	• Arrange participants
	  • Study Leader - who plans and controls the meetings
	  • A Recorder (Note Taker) who assists the Study Leader with administration
	  • System Expert or Designer - must be able to explain the design intent of the system components
	  • Users of the System e.g. ATCOs, Engineers, Pilots and Aerodrome Staff.
	  • Other Experts, particularly those knowledgeable about hazards with similar systems

Table 1 The Complete HAZOP Process (continued)

	• Prepare the HAZOP
	  • Prepare System Representations: Components, Entities and Attributes
	  • Prepare Guide Word lists
	• Make presentations of
	  • The HAZOP process and rules of conduct
	  • General System introduction
	• Make a schedule for the HAZOP session
	• Arrange practical issues:
	  • Room free from distractions
	  • Flipchart
	  • Laptop PC and Projector
	  • Availability of refreshments

HAZOP	• Introduce using prepared presentations
	• HAZOPS
	  • Conduct sequential analysis of the system
	  • Make short notes of hazards on flipchart
	  • Agree causes and consequences for credible hazards and record them
	  • Apply short breaks before productivity drops significantly
	• Close the session

Evaluate	• Distribute records of HAZOP with hazard log, requesting corrections • Evaluate the effectiveness of the HAZOP: • Any unanswered questions? • Decide whether and when another HAZOP session is needed

3 Preparation for the HAZOP Study

3.1 Participants

3.1.1 The number of participants at a HAZOP study should be limited to between 5 and 7 people.

3.1.2 The following participants should be involved in a HAZOP study session:

a) **Study Leader:** Controls the flow and timing of the meeting; states the rules of conduct of the meeting. The Study Leader should lead the meeting through the analysis by postulating possible deviations from design intent by applying the HAZOP guide words sequentially to the system design. The Study Leader should be:

- Independent of the project, but knowledgeable of the design representations (block diagrams etc) and knowledgeable in the technical/ operational field of the system.
- Ideally familiar with, or trained in leading a HAZOP study.
- A competent chairperson, maintaining harmonious control over proceedings.

b) **Recorder (Note Taker):** Somebody noting down the detail of the hazards; this may be on a laptop PC connected to a projector so that the participants can correct any misunderstandings.

c) **Operation/System Expert:** This should be somebody directly involved with the planned project. They will need to explain the design role of each part of the system under consideration. Typically this may be the Project Manager, Senior Air Traffic Controller or Senior Systems Engineer. They may also present a project overview at the beginning of the session.

d) **Users of the System:** Typically these will be Operational Staff such as:

- Air Traffic Controller (or FISO): where possible this person should be familiar with the planned project or should be familiar with the type of ATC functions planned to be performed e.g. Approach, Area etc.
- Pilot: where possible this person should be familiar with the planned project or should be familiar with the types of aircraft that may be involved in the planned project.
- Engineer: where possible this person should be familiar with the planned project or have experience operating or maintaining similar systems.
- Aerodrome Staff: depending on the nature of the system, these could be RFFS staff, security staff, refuelling staff etc. Where possibly these people should be familiar with the planned project and the type of functions to be performed.

e) **Other Experts:** Other Operational or System experts familiar with the system or who can add value to the HAZOP process e.g. a Safety Analysis expert may be present who could help the group with Safety terminology and structuring the record of hazards (this role may be combined with the role of Recorder to more efficiently facilitate the meeting).

4 Planning a HAZOP Session

4.1 Session Logistics

4.1.1 HAZOP sessions can be taxing on participants, therefore the following should be considered when arranging the logistics of a session:

a) A meeting room protected from distractions e.g. no calls to be taken.

b) The preparation of a meeting schedule that divides the allocated time up into manageable chucks with frequent refreshment breaks e.g. several half hour sessions split by 10 minute breaks.

NOTE: Participants are normally more pro-active in morning sessions than afternoon sessions;

c) Easy availability of refreshments.

4.2 Introductory HAZOP Presentation

4.2.1 Some participants to a HAZOP session may not be familiar with the process or what is expected of them. It is therefore important to explain this, ideally in the form of a short presentation covering:

a) Definition of a hazard.

b) How the HAZOP will be managed i.e. the rules.

4.2.2 The Study Leader would normally undertake the above presentation lasting no longer than 10 minutes.

4.3 Project or System Presentation

4.3.1 Although many of the HAZOP participants may already be familiar with the project, some may not be, therefore an overview of the project should be presented:

a) This should last no longer than half an hour.

b) It should not be very detailed, but typically cover:

- The objective of the project.
- Concept of Operation e.g. Airspace Configuration and Interfaces; Aerodrome Layout; traffic characteristics; timeframe.
- Human Roles (e.g. from an ATC, Pilot etc. point of view).
- Procedures.
- Technical Systems.

c) It should be biased towards pictures and diagrams.

NOTE: The pictures and diagrams e.g. airport layout, airways structure and charts, should be made into posters and pinned or placed around the room where the HAZOP activity takes place for easy reference.

4.3.2 The Operation/System Expert would normally undertake the above presentation.

5 Breakdown of the HAZOP process

5.1 Documented Representation of the System

5.1.1 One of the key requirements of the HAZOP session is a clear and complete representation of the system being analysed. This is necessary in order to allow the Study Leader to sequentially select the components or interconnections to be analysed.

5.1.2 The system representation would normally take the form of a block diagram showing system components and their interconnections. These can be at the physical level or logical level.

5.1.3 More than one diagram may be required to represent the complete system.

5.1.4 The system representation should show the system as a set of:

a) **Components:** Discrete structures within the total system e.g. a radio transceiver as used to communicate with aircraft or between ground staff.

b) **Interconnections between components:** e.g. linking a radio transceiver output to an airborne receiver in an aircraft or other receivers at the aerodrome.

c) **Entities:** These relate directly to a component or an interconnection between components. They take the form of nouns that describe the sub-components of the main component and/or describe the content of the interconnections e.g. an entity of the radio transceiver would be the microphone. Typical entities of interconnections are 'data' and 'control data'.

d) **Attributes:** These are words that describe the properties of an entity. They normally involve mechanical or electrical properties that can have values associated with them e.g. voltage, level, bit rate and throughput. The attributes of an entity are the items against which the HAZOP guide words are applied e.g. for

the radio transceiver microphone, attributes include transformation (audio to electrical) and dynamic range.

NOTE: The above sounds more complicated than it is in practice. In general terms the system is broken down to a component, then sub-component level with interconnections and then labelled with physical or electrical attributes relating to the function the component, sub-component or interconnection performs.

5.1.5 It is important to take care in putting the system representation together as it forms the starting point of the HAZOP study.

5.2 Guide Words

5.2.1 A set of generic guide words is shown in Table 2.

5.2.2 More specific guide words may be generated relating more explicitly to the system under consideration.

Table 2 Generic HAZOP Guide Words

Generic Guide Words	
NO	No part of the design intention is achieved e.g. No Power
MORE	An increase above the design intention is present e.g. Too much power
LESS	A decrease below the design intention is present e.g. Too little power
AS WELL AS	The design intention is achieved, but something else is present e.g. electrical noise on the power
PART OF	Only some of the design intention is achieved e.g. intermittent power
REVERSE	The design intention is the opposite of what happens e.g. no power, but shorted to earth or current reversed
OTHER THAN	The design intention is substituted by something different e.g. DC Power expected, but AC Power presented instead
EARLY	Something happens earlier in time than expected
LATE	Something happens later in time than expected
BEFORE	Relating to a sequence or order, something happens before it is expected
AFTER	Relating to a sequence or order, something happens after it is expected

5.3 Conduct of the HAZOP Session

5.3.1 The Study Leader will make use of the System Representation to sequentially run through all attributes associated with components, sub-components and interconnections (entities).

5.3.2 Initially the Study Leader will identify a System Component or Interconnection from the Design Representation. The Operational/System Expert then explains the intended function of the choice made.

5.3.3 The Study Leader will then sequentially run through the entities and attributes associated with the component or interconnection applying each of the Attribute Guide Words (see Table 2) in turn.

5.3.4 The group will consider whether the deviation from intended function as understood from the guide word is credible or not. If not credible, the decision should be recorded

for completeness and for ease of future reference. If credible, the following should be recorded:

a) Details of the hazard identified including any detection mechanisms.

b) Recommendations for mitigating the hazard or its effects.

c) Recommendations for further study where there is uncertainty about any aspects of the hazard, cause or consequences.

d) Any questions to be answered due to uncertainties.

e) Cross reference to any other relevant studies and documents.

5.3.5 Figure 1 shows a recommended method for recording the results of the HAZOP study.

NOTE: The presence of protection or monitoring mechanisms must not stop the hazard being explored. Their effectiveness in reducing the probability or mitigating the consequences of the hazard may be assessed and the results recorded in the HAZOP documentation.

5.3.6 The Study Leader concludes the analysis of the chosen attribute-guide-word by summarising the findings, which are documented by the Recorder.

5.3.7 If using a laptop PC and projector, the Recorder can ensure that the correct understanding of the hazard, causes and consequences as discussed by the participants have been recorded.

5.3.8 This continues, according to the planned schedule, until all system components, entities, attributes and guide words have been exhausted.

6 After the HAZOP Session

6.1 The record of the HAZOP session should be supplied to the participants within a few days for error checking.

6.2 The results of the Hazard Identification process should be reviewed and a judgement made as to the how successful the process has been. If, for example, unanswered questions were raised at the HAZOP session, then answers to these need to be found and consideration given to whether a further HAZOP session is required to address any new information.

6.3 The hazards identified from the HAZOP Session, together with other Hazards Identified by other methods feed in to the next steps of the Hazard Analysis process to ascertain the severity and likelihood of their consequences.

6.4 The hazards identified using the HAZOPs process should be entered in the Hazard Log where this is being maintained (see Appendix F).

NOTE: The HAZOP group may consist of the same team conducting the risk assessment; therefore the group may allocate initial severity and likelihood information to the hazard consequences immediately after the HAZOP process to aid the later assessment.

Title of System Under Analysis: System description:

Figures/Diagrams Used:

Date:

Study Leader:

Recorder:

Team Members:

HAZOP item	Entity (sub-component/ interconnections)	Attribute	Guide word	Cause	Consequence	Indication or protection	Questions/ Recommendations	Comments

Figure 1 Example HAZOP Record Sheet

INTENTIONALLY LEFT BLANK

Appendix D Using Event Trees

1 Introduction

1.1 Event Tree analysis is used to analyse sequences of events that lead to incidents or accidents. It should not be used for hazard identification. It is used to support hazard identification and risk assessment by providing further insight into hazardous events by examining the coincidental circumstances that need to be in place, and the barriers that need to be breached, in order for a hazard to manifest into an accident or incident. Event Trees can therefore be used on hazards to identify a more realistic likelihood of an accident or incident occurring.

1.2 Event Trees can be used to determine the likelihood and severity of a range of consequences given different sequences of events. This is best illustrated by an example.

2 Example use of an Event Tree

2.1 Consider the erroneous plotting of an aircraft position on a radar display. This may have been identified as a hazard during a systematic hazard identification session, however it is not clear what the consequence of the plot error is without considering other related factors e.g.:

a) Is the error persistent or just a one off glitch?

b) Does the air traffic controller believe the error, i.e. is the displayed position of the plot in error credible?

c) Will the controller take action to redirect aircraft based on the erroneous plot data?

d) Will there be another aircraft nearby with the potential to cause a conflict? i.e. if the erroneously plotted aircraft is the only aircraft in the area, then there will be no conflict with other aircraft;

e) Will the pilots notice the potential conflict and resolve it?

f) Will the safety nets e.g. Short Term Conflict Alert and Traffic Collision Avoidance System alert to the potential conflict leading to it being resolved?

g) Will the aircraft actually touch as they pass each other?

2.2 The above sequence of events can be shown diagrammatically as an Event Tree as shown in Figure 1, where the erroneous plot on the radar screen is the 'initiating event' i.e. the first triggering event of the sequence. The subsequent links in the tree are often called 'lines of assurance' and consist of the protective systems, human actions or other coincidental events that have some association with the initiating event.

2.3 Each branch of the tree can have a probability associated with it (shown in the brackets of Figure 1). The product of the paths through the trees to each consequence can be calculated. It can be seen from the above sequence that even where the erroneous plotting of an aircraft on a radar display is a common event i.e. 1 in 10, the other coincidences that have to occur and the barriers (e.g. the controller, the pilot and the safety nets) that help prevent the critical incident occurring will mean the probability of the aircraft colliding is low. However it can also be seen that the above sequence may produce a range of incidents of differing severity and probability e.g. loss of controller situational awareness and loss of separation are both more likely than the aircraft colliding, but also of less severity.

3 Identifying Barriers and Mitigations Using Event Trees

3.1 Modelling hazards using event trees can help identify all of the barriers and coincidences that need to occur in order for an incident to occur. This helps produce more realistic and reduced probabilities for incidents occurring. This can help reduce the amount of arguments and evidence work required in the later stages of the risk assessment and mitigation process.

3.2 The event tree process can help in the design of the system, identifying where best to place barriers or mitigations that help prevent incidents occurring.

NOTE: These barriers and mitigations become Safety Requirements i.e. without them in place, the risk of an incident increases.

3.3 Event trees can be used after an incident has occurred to help find out the causes, likelihood of the event re-occurring and where best to put barriers to help prevent the event occurring again.

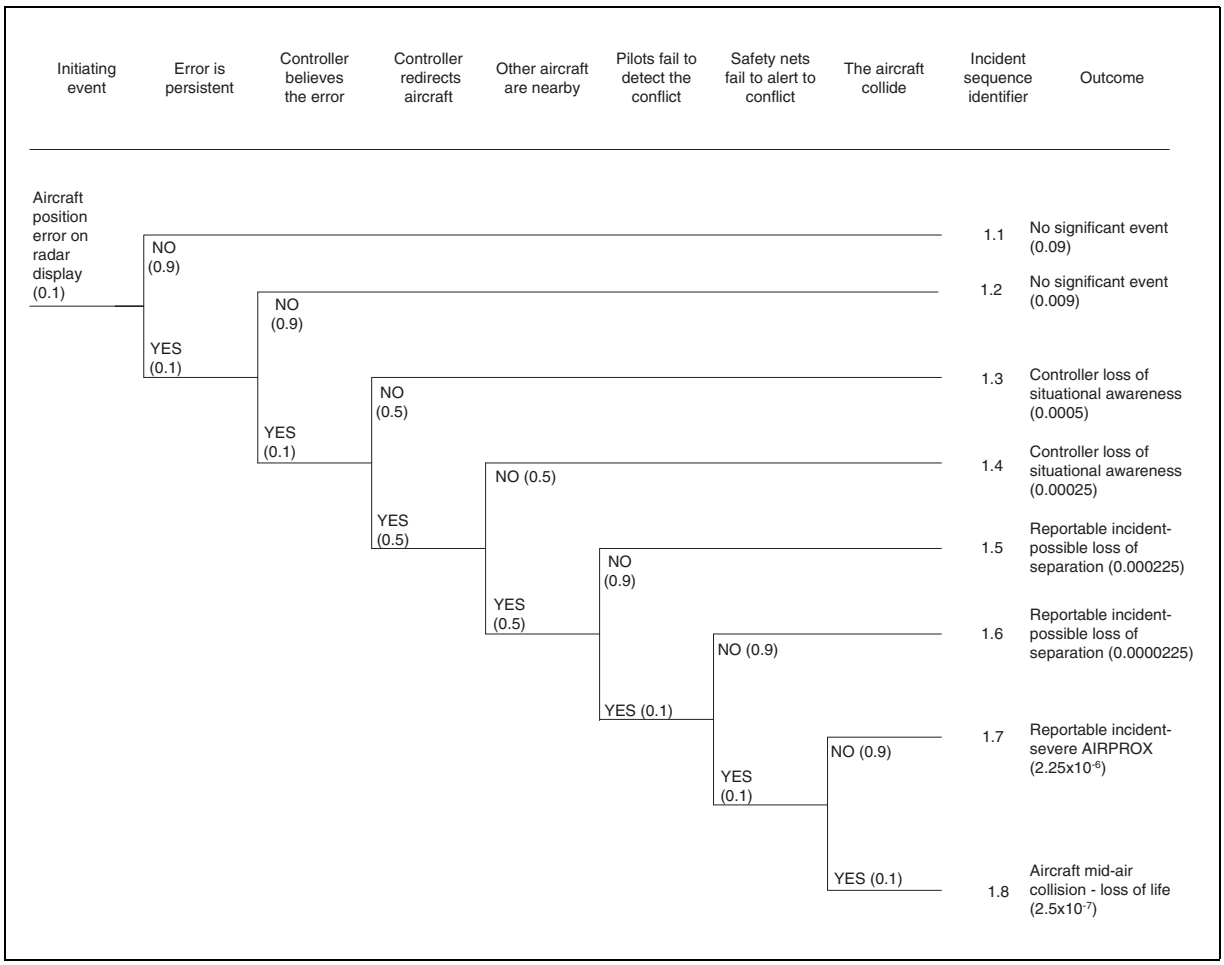

Figure 1 Event Tree for Erroneous Plot Position

4 Procedure for Event Tree Analysis

4.1 The procedure for performing Event Tree analysis consists of the following six steps:

a) Identify or Define the system or procedure of interest.

b) Identify the initiating events of interest.

c) Identify Lines of Assurance, Other Related or Coincidental Events or Other Influencing Factors.

d) Define the incident and accident scenarios - the event trees.

e) Analyse incident sequence outcomes.

f) Summarise and present the results.

4.2 Each step is covered in more detail below.

4.3 **Step 1 - Identify or Define the System or Procedure of Interest**

4.3.1 Where using event tree analysis to support other systematic hazard analysis processes (e.g. HAZOPs and FMECA), then it is likely that the systematic processes will have already defined the system or procedure to be analysed. Where this is the case, the event tree analysis can re-use this information.

4.3.2 Where no previous systematic analysis has been conducted, then it will be necessary to define the system or procedure on which the event tree analysis is to be based. The following should be considered:

a) The functions intended to be performed.

b) The equipment and people involved.

c) The boundaries of the system.

d) Interfaces between different sub-systems and interactions between people.

e) Different initial conditions of the system or procedures e.g. is the equipment in operational or stand-by mode?

4.3.3 The system description, covering the above, can be presented in the form of narrative text with supporting diagrams (e.g. system block diagrams).

4.4 **Step 2 - Identify the Initiating Events of Interest**

4.4.1 Event tree analysis may be performed on a sub-set of hazards that have been selected from a larger set of hazards. The larger set of hazards should have been developed from a systematic hazard identification process such as HAZOP or FMECA or other broad hazard identification technique. The larger set of hazards needs to be reviewed to identify those hazards of a more complex or interactive nature that warrant further analysis using event trees. This review should be conducted by experts in the system and may form part of the systematic hazard identification process.

4.4.2 When performing event tree analysis, it may be more expeditious to eliminate certain categories of events from the analysis that could impact on all event trees e.g. acts of sabotage and wide scale natural disasters. Other common mode failure points such as power supplies may also be excluded from event trees being used to explore in detail particular problem areas. The failure of the power supplies may be modelled at a more generic level. The limitations should be stated.

4.4.3 Often the types of hazard identified may be grouped into sets of similar events and dealt with generically, which may help limit the number of Event Trees needed to be produced.

4.5 Step 3 - Identify Lines of Assurance, Other Related or Coincidental Events or Other Influencing Factors

4.5.1 This step involves identifying a pool of factors from which the branches of the event tree will be later formed.

4.5.2 There are various factors that affect whether an initiating event will lead to an incident. These factors need to be identified and can include:

a) Barriers, safeguards and mitigations. These are equipment and procedures purposefully designed to prevent the initiating event manifesting into a serious incident. In the example of Figure 1 these would be the Safety Nets that alert the air traffic controller or pilots to the potential conflict.

b) Administrative or Personnel Systems such as the fire brigade or other emergency response. These can limit the severity of an incident.

c) Human detection and intervention. This is where humans in the chain of events detect the hazard and take steps mitigate it. In the example of Figure 1 both the Air Traffic Controller dismissing the plot error as incredible and the pilots seeing the potential conflict are examples of human detection.

d) Coincidental Events. These are events that need to occur at the same time, or in sequence with the initiating event in order for the incident chain to propagate. They are chance events. In the example of Figure 1 'other aircraft are nearby' and 'the aircraft touch' can be considered coincidental or chance events.

e) Other Influencing Factors. These are other phenomena that may affect the probability or severity of an incident. They include the weather and time of day. The example at Figure 1 does not include weather, but it can be seen that low visibility weather conditions may affect the ability of the pilots to detect the conflict situation.

4.5.3 At the end of this step a pool of factors should be defined from which the event tree can be constructed.

4.6 Step 4 - Define the Incident and Accident Scenarios - the Event Trees

4.6.1 This step defines the structure of the Event Tree by starting with the initiating event and selecting related factors from the pool developed in the step above and putting them in the sequence they are likely to occur.

4.6.2 There is a logical progression to an incident sequence that moves forward from the time the initiating event occurs. As the incident sequence progresses and becomes more severe or less probable, different systems respond in different ways. Understanding the progression and timing of the system, physical and human responses is essential in developing the logic of the event tree.

4.6.3 Care must be taken when constructing the tree to consider the following:

a) System Dependencies - Most systems interact with other machines and processes in some way. These interactions may influence or degrade the level of protection offered by redundant equipment and fallback systems. For example the failure of the air conditioning system in a control tower may not only cause some electronic equipment to overheat and fail, but also place air traffic controllers trying to cope with the failing equipment under physical duress that may hamper their performance.

b) Conditional Responses - The probability of success for a line of assurance (i.e. a mitigation or barrier) may be conditioned on the success or failure of the lines of assurance that precede it. For example the ability of pilots to be able to visually

detect a potential conflict may be conditioned on the preceding weather conditions or time of day. It is therefore not unusual for the same line of assurance factor to have different probabilities associated with it in different event trees or parts of the same tree depending on what the preceding events or factors are.

c) Allocating the correct probabilities - Where possible, probabilities of event tree branch outcomes should be shown in the event tree. However obtaining confident probability data for the effectiveness of barriers can be difficult e.g. the probability that a human will act in a particular way is difficult to predict. The following may help provide more confident probability estimates:
   - Modelling the particular protection device, procedure or human e.g. by using Human Reliability Analysis (a technique for predicting human performance - not covered in this guidance document).
   - Using field evidence of other system performance to estimate this system performance.
   - The judgement of experts in the systems concerned.

4.7 Step 5 - Constructing the Event Tree Logic

4.7.1 Event tree construction consists of the following steps:

a) List the initiating event on the left side of the tree.

b) List the lines of assurance, barriers and other influencing factors or conditions across the top of the tree in sequential order.

c) Identify success and failure branches at each branch point (the point below a listed line of assurance etc.) and add probabilities if known. Consider the following:
   - Some branch points may have more than two outcomes.
   - Some branch points may have only one outcome where its conditional probability is 1 or 0 i.e. as a result of a preceding event, the outcome of this event is 100% certain.

d) Keep positive or high probability branches of branch pairs or groups at the top of each branch point to aid later sorting of priority items i.e. if highest probability outcomes are always kept to the top, then the topmost outcome will be the most probable.

e) Continue developing the branches and branch points to the right until the sequence of factors is exhausted.

4.7.2 Figure 1 is an example of what an Event Tree can look like.

4.8 Step 6 - Analyse the Incident Sequence Outcomes

4.8.1 The final outcome for each combination of branches is listed at the right hand side of the event tree. It may also be beneficial to label each of the branch combinations with a sequence identifier number or letter to aid any later reference to specific sequences in the event tree.

4.8.2 The final consequence of each sequence of events may be obvious and can be easily appended to the Event Tree in the final column. However, for some sequences of events it is not immediately clear what the consequences may be. Where this is the case, then further work modelling the event sequence or using expert judgement may be necessary to determine the consequence before entering this in the event tree.

4.8.3 Where probabilities have been used in the event tree branches, then the probability for each sequence of events leading to an outcome can be calculated by multiplying all of the probabilities in a sequence together.

4.8.4 A qualitative assessment of the likelihood of an outcome can be based on counting the number of branches (barriers, mitigations and coincidences) between the initiating event and the outcome i.e. counting the number of events that have to come together in order to cause the outcome. A low number means an outcome is likely, whilst a high number equates to an unlikely outcome. A judgement call will be needed to assess just how likely or unlikely the outcome is from the knowledge of how effective the protective systems or procedures forming the event tree branches are.

4.9 Step 7 - Summarise The Results

4.9.1 Where large sets of Event Trees have been produced a practical way of presenting the information from the trees is required. This can be achieved through tabulating the following:

a) Initiating event.

b) Event sequence number (for traceability back to the event tree).

c) The probability or likelihood.

d) The outcome or consequence.

4.9.2 Table 1 shows the summary table for the event tree of Figure 1.

Table 1 Event Tree Summary Table

Initiating Event: Aircraft Position Error on Radar Display		
Incident Sequence Number	**Probability**	**Consequence**
1.1	0.09	No significant Event
1.2	0.009	No significant Event
1.3	0.0005	Controller Loss of Situational Awareness
1.4	0.00025	Controller Loss of Situational Awareness
1.5	0.000225	Reportable incident - possible separation loss
1.6	0.0000225	Reportable incident - possible separation loss
1.7	2.25×10^{-6}	Reportable incident - severe Airprox
1.8	2.5×10^{-7}	Aircraft mid-air collision - loss of life

Appendix E Diagrammatic Representation of Safety Arguments

1 Introduction

1.1 There are a number of diagrammatic ways to represent safety arguments. For example, the University of York[1] developed Goal Structured Notation (GSN) in the 1990s and Adelard[2] developed Claim Argument Evidence (CAE) notation around the same time.

1.2 For illustrative purposes this Appendix concentrates on GSN and its use.

1.3 GSN uses a top-down block diagram approach to representing safety arguments that is simple to understand. It is the way in which GSN diagrams are intuitively understood by a wide range of people who may need to understand the safety arguments for a system that makes it valuable.

1.4 GSN diagrams may also grow with the development of the safety case through different parts of the project lifecycle.

1.5 This Appendix gives a basic explanation of the GSN symbols and an example of their use.

NOTE: The inclusion of this Appendix on GSN is not CAA endorsement of the GSN system over any other diagrammatic way to represent safety arguments. Users are free to use any diagrammatic notation that meets their requirements.

2 Goal Structured Notation - GSN

2.1 GSN uses a set of block diagram shapes filled with text to represent different parts of a safety argument. Each block should be numbered. The block diagram shapes are shown in Figure 1 and their uses are explained as follows.

2.1.1 **The Goal** - (a rectangle) the goal is the ambition that the safety argument or arguments are trying to satisfy. Goals can take the form of Safety Requirements or Safety Objectives. A Goal would normally appear at the top of the GSN diagram and there may be further sub-goals at a lower level that contribute to meeting the top-level goal. Number using G1, G2, G3 etc for top-level goals and G1.1, G1.2 etc for sub-goals.

2.1.2 **The Strategy** - (a rhombus) the strategy would normally appear just below a Goal and will explain how the Goal will be demonstrated to be met. It is optional. A typical strategy will be to divide the goal up into a set of smaller safety requirements and address each one in turn. More than one strategy can be attached to the goal above i.e. there may be multiple ways to demonstrate, or partially demonstrate a goal, that combine to create a more credible proof. Note that High and Medium Required Level of Confidence for safety requirements specify that diverse sources of evidence are required (see Appendix G). Number using S1, S2, S3 etc.

2.1.3 **The Context** - (a curved sided rectangle) the context can be attached to any other shape and contains the operational environment for which this argument is valid. Number using C1, C2, C3 etc.

1. www.cs.york.ac.uk
2. www.adelard.co.uk

2.1.4 **The Assumptions** - (an oval with an 'A' to the bottom right) the assumptions can be attached to any other shape and contain anything that has to be assumed for this argument to be valid. Number using A1, A2, A3 etc.

2.1.5 **The Justifications** - (an oval with a 'J' to the bottom right) the justifications can be attached to any other shape and contain the reasoning behind the content of the associated shape. For example the justification for a Target Level of Safety figure used in a safety requirement may be that a regulatory body mandates it. Number using J1, J2, J3 etc.

2.1.6 **The Solutions** - (a circle) the solution normally equates to items or sets of evidence that demonstrate that the goal or sub-goal above is being met. Number using S1, S2, S3 etc.

2.1.7 **Linking Arrows** - these take two forms:

a) Links with solid arrowheads generally flow in the direction top to bottom and represent the words 'is solved by'.

b) Links with hollow arrowheads generally flow horizontally and are associated with context, assumption and justification shapes and represent the words 'in the context of'.

2.1.8 **To be developed** - (a diamond) this symbol found at the bottom of a goal, sub-goal or strategy indicates that further work to demonstrate this goal is required. Typically this is found in safety cases early in the lifecycle of a project i.e. before the system has been implemented and evidence amassed.

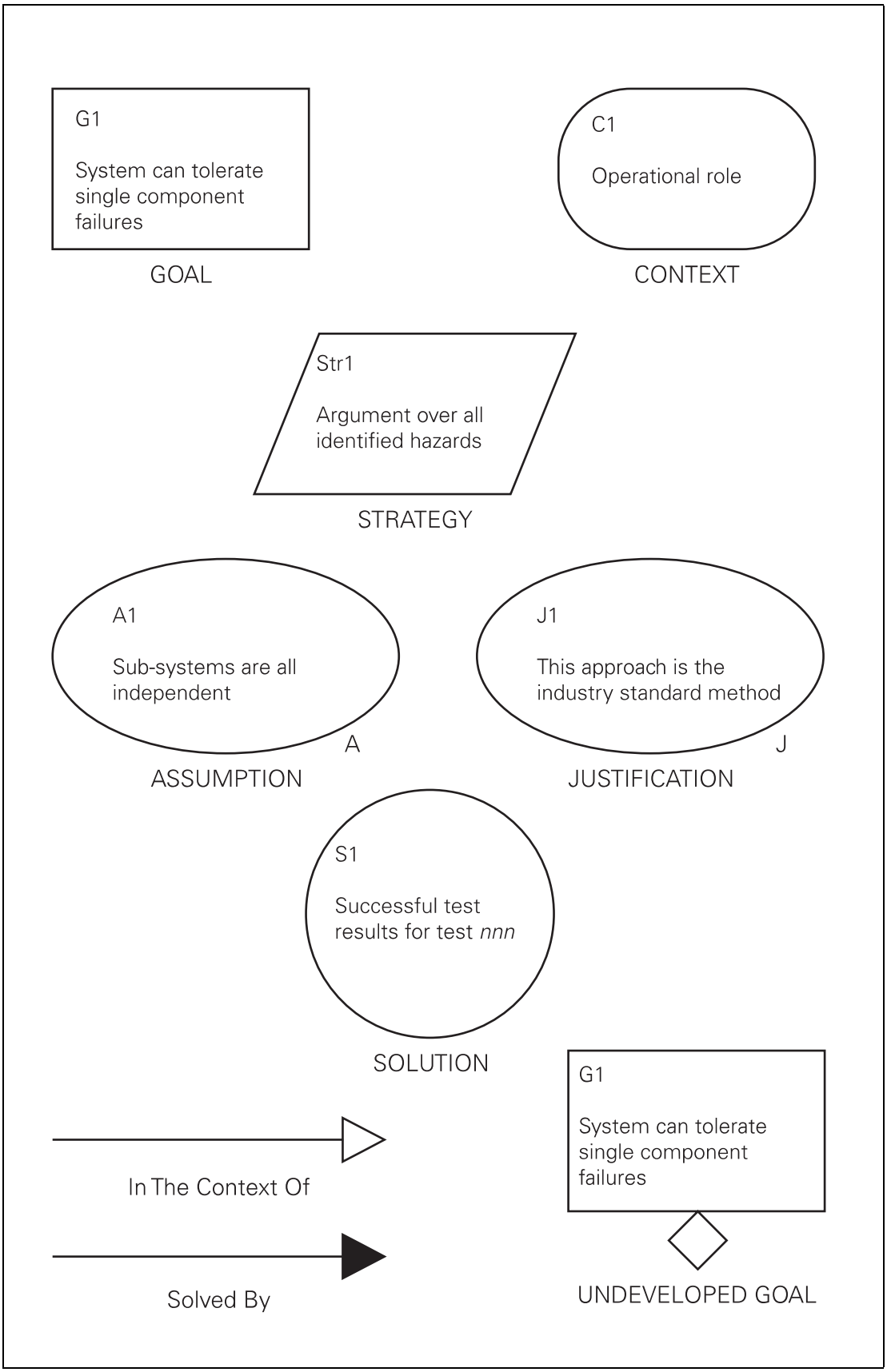
G1
System can tolerate single component failures
GOAL
C1
Operational role
CONTEXT
Str1
Argument over all identified hazards
STRATEGY
A1
Sub-systems are all independent
A
ASSUMPTION
J1
This approach is the industry standard method
J
JUSTIFICATION
S1
Successful test results for test nnn
SOLUTION
G1
System can tolerate single component failures
UNDEVELOPED GOAL
In The Context Of
Solved By

Figure 1

3 Example of Goal Structured Notation

3.1 Consider a surveillance system designed to provide a service suitable for a minimum of 3NM separation within a defined volume of airspace. In this example we will assume that a hazard identification and risk assessment process has been conducted on the surveillance system and that a number of safety requirements concerning the system have been generated. We will assume that one such safety requirement is as follows: *'The accuracy of the displayed position of aircraft within the surveillance system shall be sufficient to operate safely using 3NM separation'*.

3.2 We can consider this safety requirement as a top-level goal within a GSN structure as shown in Figure 2 (although in practice this requirement is likely to be one of several sub-goals of a higher level goal e.g. 'the performance of the surveillance system shall meet the operational requirements').

3.3 Associated with this top-level goal is the context for which the GSN structure is valid i.e. within the desired coverage volume as defined in the Operational Requirement.

3.4 Leading down from the top-level goal is a strategy. This sets out how it is intended to prove that the goal has been satisfied. In this case the strategy is to examine each of the surveillance sub-systems for the characteristics of their errors, combine them into one probability distribution, separate 2 such distributions by the desired separation i.e. 3NM and integrate the area where the tails overlap to obtain a probability of collision due to surveillance system position error.

3.5 Below this strategy are a series of sub-goals that consider each of the surveillance sub-systems in turn and below these are solutions in the form of sources of evidence that demonstrate the sub-goals are met.

3.6 Shown in the middle at a lower level is the important sub-goal G1.5. This goal is that the combination of the various sub-system errors and the analysis of the overlapping tails of the probability distributions should be tolerably safe. Associated with this goal is an assumption of what a tolerably safe overlap (or probability of collision) is and a justification for the figure shown in the assumption i.e. it appears in a regulatory standard.

3.7 Below this is the final solution in the form of evidence that the analysis shows that a tolerably safe figure can be achieved.

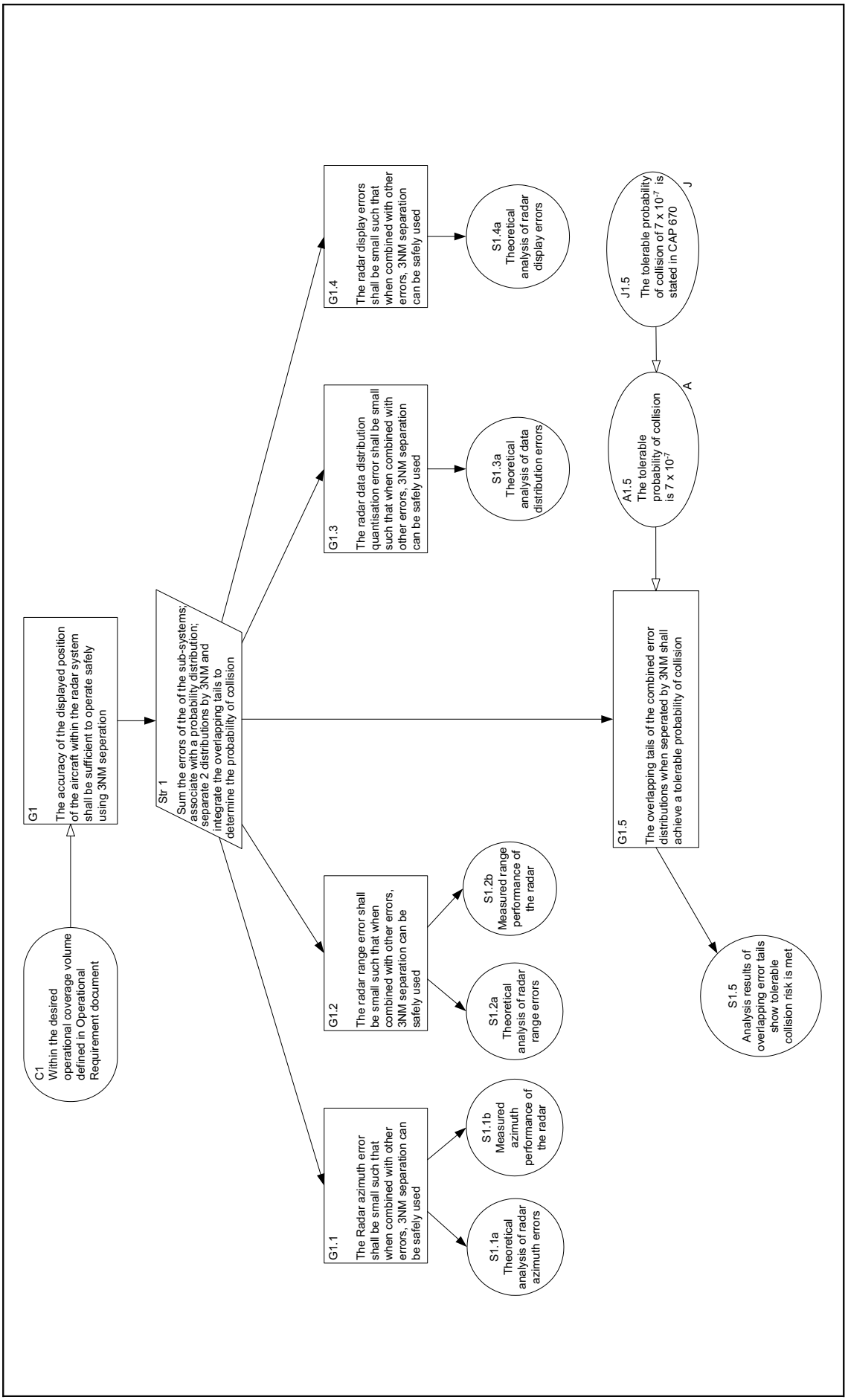

Figure 2 Goal Structured Notation Example

INTENTIONALLY LEFT BLANK

Appendix F Hazard Logs

1 Introduction

1.1 Hazard Logs are a structured way to record the hazards identified pertaining to a project or system and to record the actions that are planned or have taken place to address the hazards registered.

1.2 The Hazard Log should be used at the very beginning of a project and be kept up to date as a living document throughout the lifecycle of the project.

1.3 Early in the life of a Hazard Log, the information logged for each hazard may be limited. As the project develops and further risk assessment and mitigation processes are undertaken, more detail can be added to the Log.

1.4 At milestones of a project, for example just before putting a new system into operational service, the Hazard Log can be reviewed to see the status of the associated hazards i.e. to ensure that all hazards have been addressed (mitigated) or accepted and prove to be a tolerable risk.

1.5 The Hazard Log can be used to log the outcome of the Hazard Identification processes e.g. Brainstorming, FMECA, HAZOPs etc.

2 Developing a Hazard Log

2.1 The Hazard Log normally takes the form of a series of forms, where each form filled in represents one hazard or one of several possible consequences of a hazard. Figure 1 shows the typical composition of a Hazard Log. Within the form are a series of headings that are explained further in the following text.

2.2 **Project or System:** State the project or system to which the hazard identified is applicable.

2.3 **Hazard Log ID:** Use this entry to uniquely number this hazard log entry for document control purposes.

2.4 **Hazard ID:** Copy any Hazard Identity (ID) number allocated during the Hazard Identification process.

2.5 **Identified by:** Name the person or group that identified the hazard and/or the hazard identification process used.

2.6 **Date Created:** Enter the date that this Hazard Log form was first used.

2.7 **Last Update Action:** State the last fields on this form that were updated.

2.8 **Date of Last Update:** Enter the date the last time this form was updated.

2.9 **Hazard Description:** Describe the hazard. This may take the form of how the hazard was recorded during a hazard identification process.

2.10 **Hazard Category:** Use this field to enter categories for sorting hazards e.g. Technical, Operational, Training, and Procedural etc.

2.11 **Hazard Consequence:** Enter the consequence that the hazard could manifest.

NOTE: A single hazard may have more than one consequence. Use multiple sheets where other significant consequences need to be logged.

2.12 **This Hazard Probability (Qualitative and/or Quantitative):** Enter the probability of the hazard manifesting into the consequence. Enter a probability value if available, or qualitative description (see Table 2 from Chapter 3 Step 4).

2.13 **Cumulative Hazards Probability (Qualitative and/or Quantitative):** Where it has been identified that more than one hazard leads to the same consequence, enter the summation of the probabilities of the contributing hazards to identify the total likelihood of the consequence manifesting.

2.14 **Severity:** Enter the severity (see Table 1 from Chapter 3 Step 3).

2.15 **Proposed Action/Mitigation:** Enter the action or mitigation that has been devised to deal with this hazard.

2.16 **Proposed By:** Name the person or team that proposed the action or mitigation.

2.17 **Actionee:** Name the person, team or organisation that will be carrying out the action or mitigation.

2.18 **Planned Date:** Enter the date when the Proposed Action/Mitigation is intended to be implemented.

2.19 **Mitigation/Action Taken:** State the action actually taken (this may be as proposed above).

2.20 **Date of Action:** Enter the date the action was taken.

2.21 **Action Status:** State whether the Action is ongoing, partially complete or complete.

2.22 **Status of this Hazard Log Entry:** Enter whether this Hazard Log entry is awaiting any further input, is awaiting closure etc.

2.23 **Date Closed:** Enter the date when it was agreed that no further action would be taken with respect to this Hazard Log entry.

2.24 **Continuation Sheet? (Y/N):** Enter 'Y' where there is further information relevant to this Hazard Log entry contained on an additional sheet of paper.

Project or system		Hazard Log ID
Hazard ID	Identified by	Date created
Last update action		Date of last update
Hazard Description		
Hazard Category		
Hazard Consequence		
This hazard probability (Qualitative and/or quantitative)	Severity	
Cumulative hazards probability (Qualitative and/or quantitative)		
Proposed action/mitigation		
Proposed by	Actionee	Planned date
Mitigation/action taken		
Date of action	Action status	
State of this hazard log entry		Date closed
Continuation sheet? (Y/N)		

Figure 1 Hazard Log Form

INTENTIONALLY LEFT BLANK

Appendix G Required Level of Confidence in Evidence

1 Introduction

1.1 The more critical a Safety Requirement is i.e. the more likely and more severe the consequences of failure to meet that Safety Requirement are, then a higher level of assurance is required to provide confidence that the Safety Requirement is met.

1.2 An increased level of confidence comes from an increased quantity, quality and diversity of evidence (see Chapter 3 paragraph 7.9). Conversely, a low criticality or low probability hazard does not require large quantities of evidence to prove that the associated Safety Requirement has been met.

1.3 The concept of Required Level of Confidence has been developed to provide a measure of the quantity, quality and diversity of evidence necessary to adequately prove that a safety requirement has been met.

NOTE: Reference to Safety Requirements throughout this Appendix applies equally to Safety Objectives.

2 Determining the Required Level of Confidence for Derived Safety Requirements

2.1 The Required Level of Confidence can be determined by identifying the criticality of the Safety Requirement being considered. The criticality of the Safety Requirement can be determined by analysing the effect of removing the safety requirement to see what severity of consequence manifests and with what likelihood. For Safety Requirements generated by this procedure this information should already be available at Step 5 where the consequence has been categorised in terms of severity and likelihood. Table 1 can then be used to look up the Required Level of Confidence for the hazard by locating the cell in the table where the probability and severity are aligned.

NOTE: Several hazards may all lead to the same consequence. It is the severity and overall probability of the consequence that is important, not the individual hazard threads[1]. It may therefore be necessary to sum the probabilities of the contributing hazard threads and use this total to identify where the overall consequence sits in the Required Level of Confidence table (for more on summing probabilities, see Chapter 3 Step 5). The Safety Requirement(s) of each contributing hazard thread will then inherit the Required Level of Confidence for the consequence.

3 Determining the Required Level of Confidence for Statutory Safety Requirements

3.1 Externally applicable requirements found in International Standards and other mandatory requirements documentation such as CAA CAPs and European Common Requirements may contain large numbers of detailed requirements, many of which are also Safety Requirements i.e. where the requirement is not complied with, there is an increase in the likelihood of an incident occurring, or the severity of the incident. Ideally, the Required Level of Confidence for each identified safety requirement should be established. However due to the large quantity of requirements,

1. A hazard thread consists of the hazard, consequence, likelihood, severity, mitigation and safety requirement.

categorising the hazards by assessing what would happen if each one was not complied with may not be practical. An acceptable approach to this is to consider sets of requirements as contributing to an overall function of a system e.g. a set of technical requirements for a system may contribute to a system working correctly. This top-level function can then be assessed in terms of its failure or corruption to determine the criticality of the incidents that manifest themselves. This criticality can then be adopted by the set of requirements that contribute to the overall function. It is likely that the criticality of the top-level function under consideration will have already been established as part of this hazard identification and risk assessment process of this procedure e.g. during brainstorming, HAZOP or FMECA analysis. From the criticality determined for the top-level function and hence the set of requirements, the Required Level of Confidence can be looked up from Table 1 below.

3.2 The Risk Classification/Tolerability Table of Step 5 has been copied here as Table 1 and modified to show the Required Level of Confidence *(within brackets)* for each cell of table as either:

a) HIGH.

b) MEDIUM.

c) LOW.

3.3 Where the user has defined their own risk classification matrix at step 5, then the following will apply:

a) Any cells marked 'Unacceptable' will take on the required level of confidence value 'HIGH'.

b) Any cells marked 'Review' will take on the required level of confidence value 'MEDIUM'.

c) Any cells marked 'Acceptable' will take on the required level of confidence value 'LOW'.

		Probability of Occurrence				
		Extremely improbable	**Extremely remote**	**Remote**	**Reasonably probable**	**Frequent**
		$< 10^{-9}$ per hour	10^{-7} to 10^{-9} per hour	10^{-5} to 10^{-7} per hour	10^{-3} to 10^{-5} per hour	1 to 10^{-3} per hour
ESARR 4 Severity (Required Level of Confidence)	Accidents	Review (MEDIUM)	Unacceptable (HIGH)	Unacceptable (HIGH)	Unacceptable (HIGH)	Unacceptable (HIGH)
	Serious Incidents	Acceptable (LOW)	Review (MEDIUM)	Unacceptable (HIGH)	Unacceptable (HIGH)	Unacceptable (HIGH)
	Major Incidents	Acceptable (LOW)	Acceptable (LOW)	Review (MEDIUM)	Unacceptable (HIGH)	Unacceptable (HIGH)
	Significant Incidents	Acceptable (LOW)	Acceptable (LOW)	Acceptable (LOW)	Review (MEDIUM)	Unacceptable (HIGH)
	No Effect Immediately	Acceptable (LOW)	Acceptable (LOW)	Acceptable (LOW)	Acceptable (LOW)	Review (MEDIUM)

Table 1 Risk Classification and Required Level of Confidence

4 Accepted Evidence Levels and Sources

4.1 Each of the Required Levels of Confidence is expanded upon in the text and tables that follow showing the expected level and depth of evidence required for each of the three categories: HIGH, MEDIUM and LOW. This is further broken down into suggested Direct and Backing evidence for three types of evidence: Test, Field Service and Analytical.

5 HIGH - Required Level of Confidence General Requirements

5.1 High confidence evidence is where any uncertainties or assumptions are minimised or err on the side of pessimism i.e. the worst is assumed. For high confidence the quantity of evidence should be substantial and diverse forms of evidence should be used i.e. Testing, Field Service and Analytical evidence.

5.2 For equipment and systems supplied by third parties, the cooperation of the supplier is essential because design specifications, manufacturing specifications, design test results and quality assurance data is typically required to support claims and arguments.

5.3 Where possible evidence should be subjected to independent scrutiny through rigorous internal or external quality assurance inspection or audit.

6 MEDIUM - Required Level of Confidence General Requirements

6.1 Medium confidence evidence is where any uncertainties or assumptions are minimised or err on the side of optimism i.e. the worst may not be assumed. For Medium confidence the quantity of evidence should be balanced to the risk. At least two diverse forms of evidence should be used i.e. Testing, and Field Service or Testing and Analytical evidence etc.

6.2 For equipment and systems supplied by third parties, the cooperation of the supplier may be required because design specifications, manufacturing specifications, design test results and quality assurance data may be required to support claims and arguments.

6.3 Where possible, evidence should be subjected to independent scrutiny through internal or external quality assurance inspection or audit, however a sampling approach to the audit may be used.

7 LOW - Required Level of Confidence General Requirements

7.1 Low confidence evidence is where any uncertainties or assumptions are minimised or err on the side of optimism i.e. the worst may not be assumed. For Low confidence the quantity of evidence may be low. Only one form of evidence may be required. However it is recommended to use more than one form of evidence.

7.2 For equipment and systems supplied by third parties, design and manufacturing evidence may not be required, unless it can be provided cost effectively. However good working practice will still need to be demonstrated so some information from the supplier organizations may be required.

7.3 The evidence should be subjected to scrutiny through inspection or audit, however a sampling approach may be used.

8 Required Level of Confidence Tables

8.1 Tables 2 to 10 suggest various forms of evidence at different levels according to the Required Level of Confidence as follows:

- Table 2 - HIGH Confidence Test Evidence
- Table 3 - MEDIUM Confidence Test Evidence
- Table 4 - LOW Confidence Test Evidence
- Table 5 - HIGH Confidence Field Service Evidence
- Table 6 - MEDIUM Confidence Field Service Evidence
- Table 7 - LOW Confidence Field Service Evidence
- Table 8 - HIGH Confidence Analytical Evidence
- Table 9 - MEDIUM Confidence Analytical Evidence
- Table 10 - LOW Confidence Analytical Evidence

Table 2 HIGH Confidence Test Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
TEST	HIGH	Direct evidence	a) Tests and acceptance criteria are specified for all relevant behavioural characteristics for each safety requirement. b) Testing was carried out that shows that the acceptance criteria for each characteristic tested has been met. c) Test Specifications, Acceptance Criteria, Test Results, Analysis of Test Results and Analysis of Faults discovered during testing should all be documented and available. d) All faults discovered during testing have been analysed and their existence does not adversely affect safety.
		Backing evidence	a) Tools used in testing have been validated. For example where simulators are used, these should have been tested and found acceptable; where specific test equipment is used, it should be within calibration and certificates should be available. b) Test procedures and the tests themselves are sufficiently thorough and are representative of the demands that will be made on the system when it is in service. For example evidence showing how the test procedure was derived, the reason for each test and why it is considered an appropriate test should be provided; a Verification Cross Reference Index (VCRI) may be useful in this respect, linking source requirements to tests. All safety requirements should be covered by testing where possible and practical. Any safety requirements not covered by testing must be covered by analytical and/or field service evidence. c) The test specifications were generated independently of the design e.g. the staff or organisation developing the test specifications were not the same as those that designed the system. d) The testing was performed independently from the design e.g. the staff or organisation carrying out the testing were not the same as those that designed the system. e) The test specifications and testing should be subject to audit and scrutiny during testing by Quality Assurance representatives within the organisation or from an external organisation; audit and test observation reports should be available.

Table 3 MEDIUM Confidence Test Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
TEST	MEDIUM	Direct evidence	a) Tests are specified for all relevant behavioural characteristics for each safety requirement. b) Testing was carried out that shows that the acceptance criteria for each characteristic tested has been met. c) Test Specifications, Acceptance Criteria, Test Results, Analysis of Test Results and Analysis of Faults discovered during testing should all be documented and available. d) All faults discovered during testing have been analysed and their existence does not adversely affect safety.
		Backing evidence	a) Tools used in testing have been validated. For example where simulators are used, these should have been tested and found acceptable; where specific test equipment is used, it should be within calibration and certificates should be available. b) Test procedures and the tests themselves are sufficiently thorough and are representative of the demands that will be made on the system when it is in service. For example evidence showing how the test procedure was derived, the reason for each test and why it is considered an appropriate test should be provided; a Verification Cross Reference Index (VCRI) may be useful in this respect, linking source requirements to tests. c) The test specifications and testing should be subject to scrutiny during testing by Quality Assurance or other customer representatives within the organisation or from an external organisation.

Table 4 LOW Confidence Test Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
TEST	LOW	Direct evidence	a) Tests are specified for a sample of behavioural characteristics of the safety requirements. b) Testing was carried out that shows that the acceptance criteria for the sample of characteristics tested has been met. c) Test Specifications, Acceptance Criteria, Test Results and Analysis of Faults discovered during testing should all be documented and available. d) All faults discovered during testing have been analysed and their existence does not adversely affect safety.
		Backing evidence	a) None required - however it is recommended to provide the backing evidence applicable for the Medium Evidence Level where available.

Table 5 HIGH Confidence Field Service Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
FIELD SERVICE	HIGH	Direct evidence	a) An analysis process specifying pass/fail criteria was specified for each characteristic of the system safety requirement that is being justified from Field Service experience. b) The analysis of Field Service records show that the pass criteria for each characteristic of the safety requirement being justified from Field Service experience has been satisfied. c) For credible Field Service Experience the following should be available as evidence: length of service; history of modifications; list of users.
		Backing evidence	a) The proposed system and the system from which Field Service evidence is being claimed should be identical; where differences exist, then the affect on the applicability of the evidence should be analysed and recorded. b) The proposed operational environment and the operational environment from which Field Service evidence is being claimed should be identical; where differences exist, then the affect of on the applicability of the evidence should be analysed and recorded. c) All functions and characteristics of the system safety requirements being justified from Field Service experience should be shown to be exercised in the deployed system. d) A Defect Reporting, Analysis and Corrective Action System (DRACAS) is in place for the deployed system, and is operated in a reliable manner, adequate to support the claims made for the system. A Mandatory Occurrence Reporting (MOR) scheme can be considered a Defect Reporting scheme for Operating Procedures. e) The Reporting schemes should be subject to periodic audit by Quality Assurance representatives in the organisation or from an external organisation. f) For all failures of the system recorded the cause of the failure has been identified, corrected, or that the failure is not relevant because it has no safety impact. g) The Field Service records are correct and complete. h) The procedures and any tools used to support the analysis of the Field Service experience were verified and validated; these may have been subject to audit by Quality Assurance representatives.

Table 6 MEDIUM Confidence Field Service Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
FIELD SERVICE	MEDIUM	Direct evidence	a) An analysis process specifying pass/fail criteria was specified for each characteristic of the system safety requirement that is being justified from field service experience. b) The analysis of Field Service records show that the pass criteria for each characteristic of the safety requirement being justified from Field Service experience has been satisfied. c) For credible Field Service Experience the following should be available as evidence: length of service; history of modifications; list of users.
		Backing evidence	a) The proposed system and the system from which Field Service evidence is being claimed should be identical; where differences exist, then the affect on the applicability of the evidence should be analysed and recorded. b) The proposed operational environment and the operational environment from which Field Service evidence is being claimed should be identical; where differences exist, then the affect of on the applicability of the evidence should be analysed and recorded. c) All functions and characteristics of the system safety requirements being justified from Field Service experience should be shown to be exercised in the deployed system. d) A Defect Reporting, Analysis and Corrective Action System (DRACAS) is in place for the deployed system, and is operated in a reliable manner, adequate to support the claims made for the system. A Mandatory Occurrence Reporting (MOR) scheme can be considered a Defect Reporting scheme for Operating Procedures. e) The Reporting schemes should be subject to periodic review or audit. f) For all failures of the system recorded the cause of the failure has been identified, corrected, or that the failure is not relevant because it has no safety impact. g) The Field Service records are correct and complete.

Table 7 LOW Confidence Field Service Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
FIELD SERVICE	LOW	Direct evidence	a) An analysis process specifying pass/fail criteria was specified for a sample of characteristics of the system safety requirement that is being justified from field service experience. b) The analysis of Field Service records show that the pass criteria for the sample of characteristics of the safety requirement being justified from Field Service experience has been satisfied. c) For credible Field Service Experience the following should be available as evidence: length of service; history of modifications; list of users.
		Backing evidence	a) The proposed system and the system from which Field Service evidence is being claimed should be similar; where differences exist, then the affect on the applicability of the evidence should be analysed and recorded. b) The proposed operational environment and the operational environment from which Field Service evidence is being claimed should be similar; where differences exist, then the affect of on the applicability of the evidence should be analysed and recorded. c) A sample of functions and characteristics of the system safety requirements being justified from Field Service experience should be shown to be exercised in the deployed system. d) For all failures of the system recorded the cause of the failure has been identified. e) The Field Service records are correct and complete.

Table 8 HIGH Confidence Analytical Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
ANALYTICAL	HIGH	Direct evidence	a) An analysis process with pass/fail criteria was specified for each attribute of the safety requirement that is being justified by analysis of the design. b) The specified acceptance criteria for each attribute of the safety requirement being justified by analysis of the design have been satisfied.
		Backing evidence	a) The design documentation is capable of supporting the identification of the appropriate safety requirements and their attributes. b) The design documentation is a sufficient representation of the system allowing adequate analysis of the design (more than one design notation may be used as part of the design documentation at any given design level). c) The analytic methods and techniques used are appropriate for the attributes of the safety requirement. d) The analysis techniques have been applied by adequately qualified and experienced staff (Staff are deemed to be appropriately qualified and experienced if they understand the design documentation, are experienced in using it, and understand the analysis approach, the required attributes and the system context). e) Assumptions used in the analysis (e.g. about the environment, hardware, software, operating system and other interfaces) have been validated. f) The formal proofs or arguments submitted are logically correct. This may be shown either by manual inspection or by tool-based checking, g) Any procedures and tools used to support the analysis have been verified and validated. h) Any analysis tools or procedures used do not corrupt or cause the system to deviate from its design intent such that the integrity of the results are compromised. i) Evidence of the analytical process and results of the analysis have been subjected to inspection or audit by independent external qualified personnel. Audit and/or inspection reports should be available.

Table 9 MEDIUM Confidence Analytical Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
ANALYTICAL	MEDIUM	Direct evidence	a) An analysis process with pass/fail criteria was specified for each attribute of the safety requirement that is being justified by analysis of the design. b) The specified acceptance criteria for each attribute of the safety requirement being justified by analysis of the design have been satisfied.
		Backing evidence	a) The design documentation is capable of supporting the identification of the appropriate safety requirements and their attributes. b) The design documentation is a sufficient representation of the system allowing adequate analysis of the design (more than one design notation may be used as part of the design documentation at any given design level). c) The analytic methods and techniques used are appropriate for the attributes of the safety requirement. d) The analysis techniques have been applied by adequately qualified and experienced staff (Staff are deemed to be appropriately qualified and experienced if they understand the design documentation, are experienced in using it, and understand the analysis approach, the required attributes and the system context). e) Assumptions used in the analysis (e.g. about the environment, hardware, software, operating system and other interfaces) have been validated. f) The formal proofs or arguments submitted are logically correct. This may be shown either by manual inspection or by tool-based checking, g) Evidence of the analytical process and results of the analysis have been subjected to inspection or audit.

Table 10 LOW Confidence Analytical Evidence

Evidence form	Evidence level	Direct or Backing evidence	Required evidence
ANALYTICAL	LOW	Direct evidence	a) An analysis process with pass/fail criteria was specified for a sample of attributes of the safety requirement that is being justified by analysis of the design. b) The specified acceptance criteria for the sample of attributes of the safety requirement being justified by analysis of the design have been satisfied.
		Backing evidence	a) The design documentation is a sufficient representation of the system allowing adequate analysis of the design b) The analytic methods and techniques used are appropriate for the attributes of the safety requirement. c) The analysis techniques have been applied by competent staff.

INTENTIONALLY LEFT BLANK